



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Diseño e Implementación de una Plataforma Web para la
Gestión de Incidentes de Seguridad de la Información*

**Máster en Gestión y Dirección de Sistemas y Tecnologías de la Información y
las Comunicaciones y de Seguridad de la Información**

ALUMNO: Blas Chica Martos

DIRECTORES: Javier Vales Alonso

CURSO ACADÉMICO: 2017-2018



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Diseño e Implementación de una Plataforma Web para la
Gestión de Incidentes de Seguridad de la Información*

**Máster en Gestión y Dirección de Sistemas y Tecnologías de la Información y
las Comunicaciones y de Seguridad de la Información**

RESUMEN

Mediante el presente Trabajo de Fin de Máster se pretende cubrir el reto de implementar una plataforma de Gestión de Incidentes de Seguridad de la Información.

La plataforma ofrecerá los siguientes servicios específicos de Gestión de Incidentes de Seguridad de la Información:

- Recogida de incidentes de Seguridad de la Información, catalogación y registro.
- Gestión de Equipos de Respuesta ante Incidentes de Seguridad de la Información.
- Consulta de medidas de protección recogidas en la guía CCN-STIC 804, de Implantación del Esquema Nacional de Seguridad (en adelante, ENS).
- Gestión de personal responsable de seguridad.
- Cuadro de mandos con estadísticas y gráficas para el apoyo a la toma de decisiones.
- Consolidación de una base de datos de Errores Conocidos (Conocimiento), a partir del histórico de incidencias cerradas y la experiencia acumulada en su resolución.
- Información específica de apoyo a la gestión de la Seguridad de la Información.

La plataforma está pensada para su uso en el entorno de las Administraciones Públicas, mediante la aplicación del ENS.

Así mismo, ofrecerá acceso web multiusuario para el personal responsable de seguridad, empleando doble factor de autenticación.

La Seguridad y la Eficiencia serán los dos aspectos clave que marquen el diseño e implementación de la plataforma web.

PALABRAS CLAVE

Incidentes, Seguridad, Información, ENS, CSIRT

AGRADECIMIENTOS

El desarrollo del presente trabajo ha supuesto un gran esfuerzo para el autor, pero también una gran prueba de paciencia para familiares y amigos. Felicitar en primer lugar a todos aquellos que supieron estar ahí y creyeron en mí.

Destacar especialmente el papel de mi novia Alina y de mis padres, conscientes de que era un gran sacrificio, pero que al final merecería la pena.

Mención especial para el Comandante y compañero José Carlos Vizoso Grande, gracias al cual he podido acceder al presente Máster. Creo que a estas alturas todo el mundo que me conoce sabe lo importante que es este Máster para mí y porqué me lo tomo tan en serio, por lo que es fácil imaginar lo agradecido que le estaré siempre.

No quisiera dejar de incluir al profesorado del Máster, con sus aportaciones siempre interesantes y necesarias, y sabiendo valorar el esfuerzo, la dedicación y la calidad de los resultados.

CONTENIDO

Contenido	1
Índice de Figuras	4
Índice de Tablas.....	9
1 Introducción y objetivos	11
1.1 Introducción y contexto	11
1.2 Motivación	24
1.3 Objetivos y alcance	26
1.4 Organización de la documentación	30
1.5 Fuentes de información	30
2 Estado del arte	31
2.1 Introducción	31
2.2 Aplicaciones de similares características	31
2.2.1 En el Sector Privado	32
2.2.2 En el Sector Público.....	33
2.3 Tecnologías y estándares existentes.....	33
2.3.1 Sistema SIEM	35
2.3.2 Equipos de Respuesta (CSIRT)	38
2.3.3 Plataforma Soteria	39
2.3.4 Resto de recursos	47
2.4 Datos de interés para la gestión de incidencias de Seguridad de la Información	48
2.5 Normativa y legislación	54
2.6 Seguridad de la Información	60
2.6.1 Cumplimiento del ENS.....	60
2.6.2 Cumplimiento del RGPD.....	62
2.6.3 Acceso web seguro multiusuario.	63
3 Desarrollo del TFM.....	65
3.1 Introducción y contexto del desarrollo.....	65
3.2 Servicios propuestos	65
3.2.1 Recogida de incidentes de seguridad de la información, catalogación y registro	65
3.2.2 Gestión de Equipos de Respuesta (CSIRT) y de personal.....	65
3.2.3 Cuadro de mandos con estadísticas y gráficas (Análisis).....	66
3.2.4 Gestión de Conocimiento	66
3.2.5 Acceso web seguro y multiusuario para personal de seguridad	66
3.2.6 Servicio de notificaciones.....	67

3.3 Diseño e implementación de la base de datos.....	70
3.3.1 Especificación de requisitos	70
3.3.2 Diseño conceptual.....	79
3.3.3 Diseño lógico	80
3.3.4 Normalización e Integridad	82
3.3.5 Diseño físico	84
3.4 Diseño de la interfaz web.....	86
3.5 Generación dinámica de las páginas web y tareas automatizadas.	88
3.5.1 Plataforma de generación dinámica de páginas web.	88
3.5.2 Tareas automatizadas.....	89
3.5.3 Implementación del servicio de notificaciones.....	90
3.6 Integración y puesta en marcha de la plataforma web.	92
3.7 Acceso mediante computación en la nube.	94
3.7.1 Contratación de un servicio de máquina virtual en la nube.....	94
3.7.2 Contratación de un dominio de Internet propio	97
3.8 Seguridad.	97
3.8.1 Acceso autenticado y gestión de usuarios	98
3.8.2 Confidencialidad.....	106
3.9 Funcionalidades adicionales y problemáticas encontradas	110
4 Verificación.....	114
4.1 Descripción del apartado.....	114
4.2 Servicio de gestión de incidencias	115
4.3 Servicio de gestión de Equipos de Respuesta (CSIRT)	135
4.4 Servicio de consulta del ENS.....	137
4.5 Servicio de gestión de personal responsable de Seguridad de la Información	138
4.6 Servicio de Análisis	143
4.7 Servicio de gestión de Conocimiento.....	153
4.8 Servicio de Información.....	155
4.9 Servicio de simulación del sistema SIEM.....	156
4.10 Servicio de Notificaciones	157
4.11 Servicio de validación de la entrada	160
5 Conclusiones y líneas futuras	161
5.1 Conclusiones de interés.....	161
5.2 Logro de objetivos	163
5.3 Líneas futuras de trabajo	163
5.4 Clausura del documento.....	166

6 Bibliografía.....	167
Anexo I: Glosario	169
Anexo II: Scripts	175
Anexo III: Instalación del Software esencial.	178

ÍNDICE DE FIGURAS

Figura 1-1. Tendencia búsqueda de la palabra <i>ciberseguridad</i> durante los últimos 5 años.....	11
Figura 1-2. La Ciberseguridad en el ámbito global de la Seguridad de la Información.	12
Figura 1-3. Perspectivas fundamentales de la Seguridad de la Información.....	12
Figura 1-4. Tríada CIA: Confidentiality, Integrity and Availability.....	13
Figura 1-5. Seguridad de la Información como Proceso: Actividades.....	15
Figura 1-6. Esquema Nacional de Seguridad: Medidas de Seguridad.	16
Figura 1-7. Nueva estructura de Seguridad Digital Global de Telefónica.	18
Figura 1-8. Escenario de aplicación de un sistema SIEM.....	19
Figura 1-9. Estructura funcional de un sistema SIEM.	20
Figura 1-10. Esquema general de aplicación de la plataforma Soteria.	22
Figura 2-1. Ámbito del COS.	34
Figura 2-2. Interfaz SIEM ↔ Soteria.	35
Figura 2-3. Relación SIEM-Soteria: aproximación 1ª.....	37
Figura 2-4. Relación SIEM-Soteria: aproximación 2ª.....	38
Figura 2-5. Gestión de Equipos de Respuesta (CSIRT).....	39
Figura 2-6. Ranking Top500 de supercomputadores.	40
Figura 2-7. Sistemas de Gestión de BBDD más populares.....	42
Figura 2-8. Lista TIOBE: extensión principales lenguajes de programación. Octubre 2018.	44
Figura 2-9. Ranking de lenguajes de programación para diversos criterios.	45
Figura 2-10. Encuestas stackoverflow sobre sistemas de desarrollo software 2018.....	46
Figura 2-11. Ciclo de vida de las incidencias en Soteria.....	49
Figura 2-12. Atención de la incidencia en órgano superior.	50
Figura 2-13. Datos de interés.	53
Figura 2-14. RGPD: artículo 33 notificación violación seguridad personales.....	57
Figura 2-15. RGPD: artículo 34 comunicación al interesado.	58
Figura 2-16. Tabla ENS.....	61
Figura 2-17. Extracto de la guía CCN-STIC 804, de Implantación del ENS.....	61
Figura 3-1. Escalado de la Notificación hasta remitirse a la Autoridad de Control (AEPD).....	68
Figura 3-2. Escalado de la Notificación hasta remitirse a las personas físicas afectadas.	69
Figura 3-3. Diagrama E-R.....	80
Figura 3-4. Modelo Relacional.....	81
Figura 3-5. Interfaz web general de acceso a los servicios de la plataforma Soteria.....	86
Figura 3-6. Estructura de directorios recomendada.....	92
Figura 3-7. Fichero de configuración Soteria.wsgi.	93

Figura 3-8. Despliegue de una instancia EC2 de AWS (A).	94
Figura 3-9. Despliegue de una instancia EC2 de AWS (B).	95
Figura 3-10. Despliegue de una instancia EC2 de AWS (C).	95
Figura 3-11. Despliegue de una instancia EC2 de AWS (D).	95
Figura 3-12. Despliegue de una instancia EC2 de AWS (E).	95
Figura 3-13. Despliegue de una instancia EC2 de AWS (F).	96
Figura 3-14. Despliegue de una instancia EC2 de AWS (G).	96
Figura 3-15. Despliegue de una instancia EC2 de AWS (H).	96
Figura 3-16. Despliegue de una instancia EC2 de AWS (I).	97
Figura 3-17. Esquema de Autenticación.	99
Figura 3-18. Código QR y Clave Secreta Google Authenticator de una cuenta de usuario.	103
Figura 3-19. Autenticación mediante usuario y contraseña.	105
Figura 3-20. Autenticación mediante PIN.	106
Figura 3-21. Usuario autenticado.	106
Figura 3-22. Certificado SSL asociado al dominio <i>soteria.es</i> .	107
Figura 3-23. Test de seguridad aplicado sobre <i>soteria.es</i> .	110
Figura 3-24. Estadísticas de uso de los navegadores más populares.	111
Figura 4-1. Interfaz inicial de acceso a la plataforma Soteria.	114
Figura 4-2. Menú superior y lateral de acceso a los servicios de la plataforma.	115
Figura 4-3. Interfaz de búsqueda y alta de incidencias.	115
Figura 4-4. Búsqueda de incidencia por su IDentificación.	116
Figura 4-5. Búsqueda por fecha de Detección.	117
Figura 4-6. Búsqueda por Estado.	117
Figura 4-7. Búsqueda por Severidad.	118
Figura 4-8. Búsqueda mediante Dimensiones de Seguridad. Selector AND.	118
Figura 4-9. Búsqueda mediante Dimensiones de Seguridad. Selector OR.	119
Figura 4-10. Búsqueda por Originador.	119
Figura 4-11. Búsqueda por Responsable.	120
Figura 4-12. Búsqueda por Tipo de incidencia (Clasificación del ENS).	120
Figura 4-13. Búsqueda por Área afectada.	121
Figura 4-14. Búsqueda según tenga asignado o no un Equipo de Respuesta la incidencia.	121
Figura 4-15. Búsqueda por IDentificación de Equipo de Respuesta.	122
Figura 4-16. Búsqueda de falsos positivos.	122
Figura 4-17. Búsqueda de falsos negativos.	123
Figura 4-18. Consulta compuesta: fecha de Detección + Estado.	123
Figura 4-19. Consulta compuesta: Estado + Severidad + Dimensiones.	124

Figura 4-20. Consulta compuesta: fecha Detección + Originador + Tipo.	124
Figura 4-21. Consulta compuesta: Responsable + Área + CSIRT.	124
Figura 4-22. Consulta compuesta: Severidad + Dimensiones + Falso positivo.	125
Figura 4-23. Consulta compuesta: Originador + Responsable + Falso negativo.	125
Figura 4-24. Consulta compuesta desde línea de comandos.	125
Figura 4-25. Servicio de consulta detallada y edición de incidencias.	126
Figura 4-26. Ventana emergente de aviso de la edición correcta de una incidencia.	126
Figura 4-27. Incidencia tras la modificación de todos sus campos editables.	127
Figura 4-28. Verificación del contenido de los campos modificados.	127
Figura 4-29. Inserción automática del registro del escalado de la incidencia.	128
Figura 4-30. Verificación de inserción automática del escalado en el campo <i>details</i>	128
Figura 4-31. Incidencia marcada como falso negativo.	128
Figura 4-32. Verificación del marcado como falso negativo.	129
Figura 4-33. Incidencia marcada como falso positivo y Cierre de la misma.	129
Figura 4-34. Verificación del marcado como falso positivo y cierre de la incidencia.	129
Figura 4-35. Acceso al servicio de alta manual de nuevas incidencias.	130
Figura 4-36. Interfaz para el alta manual de incidencias.	130
Figura 4-37. Mensaje de aviso en caso de no cumplimentar todos los datos necesarios.	131
Figura 4-38. Mensaje de aviso en caso de insertar caracteres no permitidos.	131
Figura 4-39. Deshabilitados CSIRT y CSIRT_ID hasta seleccionar severidad Crítica.	132
Figura 4-40. Se habilitan CSIRT y CSIRT_ID al seleccionar severidad Crítica.	132
Figura 4-41. Inserción automática del identificador del nuevo Equipo de Respuesta.	132
Figura 4-42. Se deshabilitan CSIRT y CSIRT_ID al volver a reducir la severidad.	133
Figura 4-43. Generación manual de una nueva incidencia.	133
Figura 4-44. Ventana emergente informando del registro correcto de la nueva incidencia.	133
Figura 4-45. Control de secuencia para nuevas altas.	134
Figura 4-46. Consulta detallada de la nueva incidencia generada manualmente.	134
Figura 4-47. Consulta de la nueva incidencia mediante conexión directa a la BBDD.	134
Figura 4-48. Interfaz de gestión de Equipos de Respuesta.	135
Figura 4-49. Modificación de un componente de un Equipo de Respuesta.	136
Figura 4-50. Ventana emergente informando sobre el cambio realizado correctamente.	136
Figura 4-51. La tabla de Equipos de Respuesta actualizada refleja el cambio.	136
Figura 4-52. Registro en incidencia del cambio de componente en el Equipo de Respuesta.	137
Figura 4-53. Ventana emergente de aviso de personal repetido.	137
Figura 4-54. Interfaz para la gestión del personal de Seguridad de la Información.	138
Figura 4-55. Selección de personal participando en uno o varios Equipos de Respuesta.	139

Figura 4-56. Cambio de situación del personal.	140
Figura 4-57. Mensaje informando sobre la actualización correcta de la situación.	140
Figura 4-58. Actualización del personal en la tabla STAFF.	140
Figura 4-59. Situación de los Equipos de Respuesta ante baja temporal.	141
Figura 4-60. Comprobación de validación de la entrada.	142
Figura 4-61. Alta de nuevo personal correcta, con mensaje emergente de confirmación.	142
Figura 4-62. El alta se refleja correctamente en la tabla del personal (STAFF).	143
Figura 4-63. Interfaz web del servicio de Análisis.	143
Figura 4-64. Número de incidencias por año.	144
Figura 4-65. Recuento número de incidencias por año desde conexión directa a BBDD.	144
Figura 4-66. Número de incidencias mensual para el año 2017.	145
Figura 4-67. Número de incidencias para el periodo 20/06/2018 a 20/10/2018.	145
Figura 4-68. Recuento de incidencias para el periodo 20/06/2018 a 20/10/2018.	146
Figura 4-69. Intervalo entre la Detección y la Notificación de las incidencias.	146
Figura 4-70. Comprobación intervalo entre Detección y Notificación de las incidencias.	146
Figura 4-71. Intervalo entre la Detección y el Cierre de las incidencias.	147
Figura 4-72. Comprobación intervalo entre la Detección y el Cierre de las incidencias.	147
Figura 4-73. Estadísticas relativas a los falsos positivos detectados en la plataforma.	147
Figura 4-74. Estadísticas relativas a los falsos negativos detectados en la plataforma.	147
Figura 4-75. Comprobación estadísticas de falsos positivos y falsos negativos detectados.	148
Figura 4-76. Distribución por Severidad de las Incidencias.	148
Figura 4-77. Comprobación de la distribución por Severidad de las Incidencias.	149
Figura 4-78. Distribución por Categorías de las Incidencias (tipo).	149
Figura 4-79. Comprobación de la distribución por Categorías de las Incidencias (tipo).	150
Figura 4-80. Estadísticas relativas a los Equipos de Respuesta conformados.	150
Figura 4-81. Comprobación de estadísticas sobre Equipos de Respuesta conformados.	150
Figura 4-82. Escalado de incidencias.	151
Figura 4-83. Comprobación del escalado de incidencias.	151
Figura 4-84. Distribución de Incidencias según Origen (SIEM / Personal).	151
Figura 4-85. Comprobación distribución de Incidencias según Origen, años 2015 y 2016.	152
Figura 4-86. Comprobación distribución de Incidencias según Origen, años 2017 y 2018.	152
Figura 4-87. Servicio de gestión de Conocimiento.	153
Figura 4-88. Incidencias por categoría.	153
Figura 4-89. Separador para la información de cada incidencia.	154
Figura 4-90. Localización incidencia según tipo y orden en la lista de Conocimiento.	154
Figura 4-91. Información de la incidencia localizada.	154

Figura 4-92. Selección de una incidencia notificada.....	155
Figura 4-93. Selección de una incidencia notificada. Gestión de la incidencia.	155
Figura 4-94. Servicio de Información.	156
Figura 4-95. Ejecución del script siem.py cada hora.	156
Figura 4-96. Comprobación de la ejecución del script siem.py cada hora.....	156
Figura 4-97. Información de la incidencia generada desde el simulador del sistema SIEM.	157
Figura 4-98. Notificación ante posible violación de la seguridad de los datos personales.	158
Figura 4-99. Notificación ante la detección de una incidencia de severidad Crítica o Alta.	158
Figura 4-100. Notificación ante el escalado de una incidencia a un órgano superior.....	158
Figura 4-101. Notificación de alta en la plataforma Soteria.	159
Figura 4-102. Notificación de cambio de un componente de un Equipo de Respuesta.	159
Figura 4-103. Notificación cambio de un componente de un Equipo por baja.....	159
Figura A2-1. Configuración de la aplicación Flask en caso de utilizar el servidor interno.	175
Figura A2-2. Configuración de la aplicación Flask en caso de utilizar un servidor externo.	176
Figura A2-3. Extracción del nombre del usuario recién autenticado.	177
Figura A2-4. Proceso de alta de nuevo usuario.....	177

ÍNDICE DE TABLAS

Tabla 1-1. Resumen de objetivos.	29
Tabla 2-1. Recursos software necesarios.	47
Tabla 3-1. Campos declarados como datos fundamentales.....	84
Tabla 3-2. Recursos software necesarios.	92
Tabla 5-1. Verificación del logro de objetivos.....	163

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción y contexto

Ciberseguridad* se ha convertido, sin duda, en uno de los términos más populares en cualquier ámbito de la sociedad. De hecho, consultando las palabras más buscadas en Internet se puede observar cómo la tendencia es claramente alcista en los últimos años:

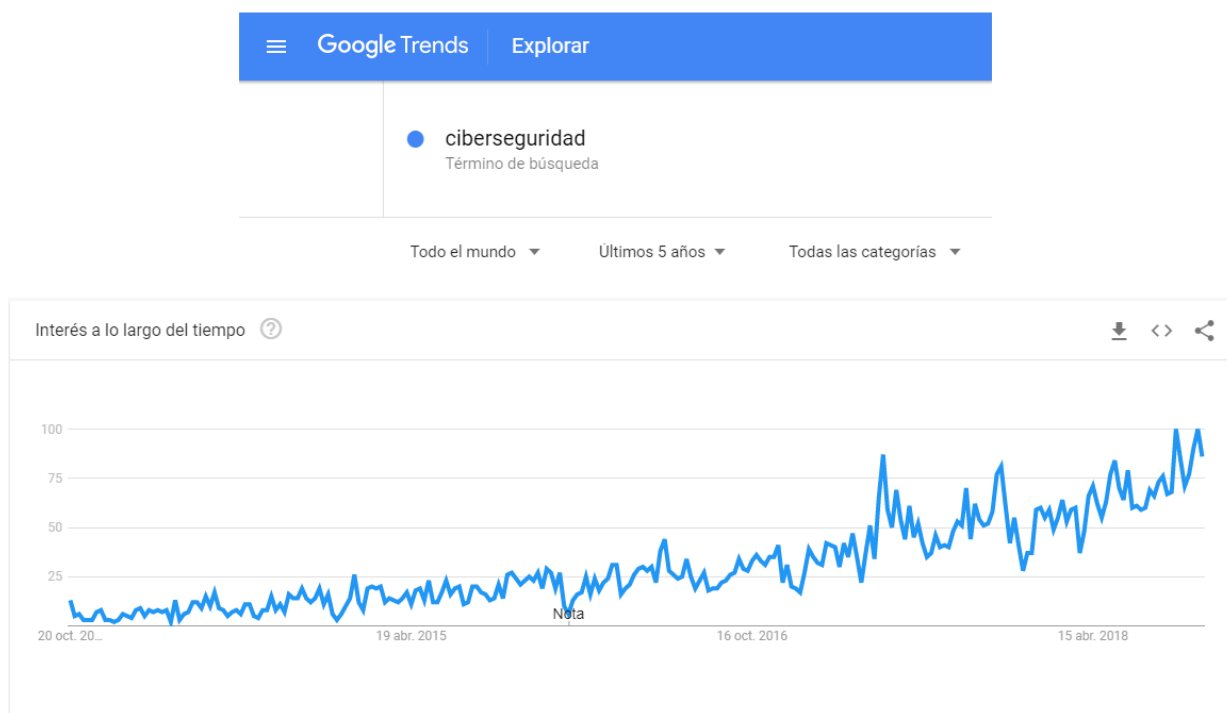


Figura 1-1. Tendencia búsqueda de la palabra *ciberseguridad* durante los últimos 5 años.

Fuente: <https://trends.google.es/trends/explore?date=today%205-y&q=ciberseguridad>

Ya sea por la preocupación que despierta la amenaza de casos tan sonados como el descubrimiento del Ransomware* Wannacry*, el pasado mayo de 2017, por la toma de conciencia de las organizaciones en la importancia de tener cubierto este apartado (consecuencias económicas y legales), o simplemente por la curiosidad que despierta entre la sociedad, es claramente un término de moda.

***En adelante, los términos marcados con * podrán encontrarse desarrollados en el ANEXO I: GLOSARIO.**

Si bien, aunque está claro que **la ciberseguridad** supone uno de los núcleos y pilares fundamentales de la Seguridad de la Información, no hay que perder de vista que **no es el único integrante**. Las amenazas no vienen únicamente desde el punto de vista informático y la exposición de las Tecnologías de la Información y las Comunicaciones (en adelante, TIC), por el hecho de encontrarse accesibles mediante redes informáticas. Una amenaza tan válida como cualquier otra y que requiere tratarse igualmente puede ser simplemente haber encontrado una nota en papel en el suelo de la organización con los datos de acceso de una cuenta corporativa, o el hecho de hallar un documento en las cercanías de los depósitos de basura con información sensible de la organización. En resumen, **la seguridad de una organización, desde el punto de vista de sus activos* de información y personal, estará cubierta con cierto nivel de garantía cuando lo esté la Seguridad de la Información de la organización en su conjunto**. En la siguiente figura se muestra el ámbito global de la Seguridad de la Información, y qué espacio ocupa la Ciberseguridad:

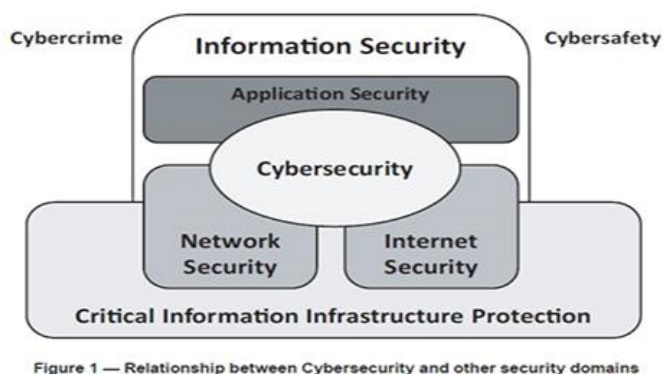


Figura 1-2. La Ciberseguridad en el ámbito global de la Seguridad de la Información.

Fuente: <https://www.indracompany.com/es/blogneo/reto-ciso-ciberespacio>

Fuente original: ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.

Como se observa, la ciberseguridad supone un espacio intermedio entre la seguridad en las aplicaciones, la seguridad en las redes y la seguridad en Internet, cubriendo por tanto una parte de la dimensión técnica del ámbito global de la Seguridad de la Información.

Al hacer una abstracción superior, se llega a dicho ámbito global de la Seguridad de la Información, representado por las siguientes perspectivas fundamentales:



Figura 1-3. Perspectivas fundamentales de la Seguridad de la Información.

Fuentes de los iconos: <http://www.iconarchive.com> y <https://www.flaticon.es>

- La perspectiva legal incluye principalmente las regulaciones internacionales, nacionales y regionales orientadas a proteger la privacidad y los derechos de propiedad intelectual.
- La perspectiva técnica incluye los aspectos de seguridad relacionados con el desarrollo, análisis, configuración y despliegue de los componentes técnicos (hardware, software y redes).
- La perspectiva organizativa incluye la seguridad orientada al negocio, cuyo objetivo principal es garantizar que los procesos de negocio se realizan sin interrupciones en cuanto a las **dimensiones de seguridad de la información**. Su base es el análisis de riesgos.
- La perspectiva del factor humano incluye los aspectos de sensibilización y formación, aplicados a **todo el personal** de la organización, desde los directivos a los empleados. Requiere así mismo la definición de funciones y obligaciones del personal, de tal manera que cada persona de la organización conozca el alcance de su trabajo.

Mientras que las **perspectivas legal y organizativa** se encargan de **qué hay que proteger, por qué y de qué**; la **perspectiva técnica** se encarga de **cómo hay que proteger los activos** desde el punto de vista técnico.

La **seguridad de la información engloba**, por tanto, **todos aquellos aspectos que permitan la protección de los activos de tal manera que la organización cumpla su misión**. Por tanto, se trata de una **actividad crítica**.

Respecto a las **dimensiones de la Seguridad de la Información**, tradicionalmente se ha considerado el triángulo conocido como la Tríada CIA:

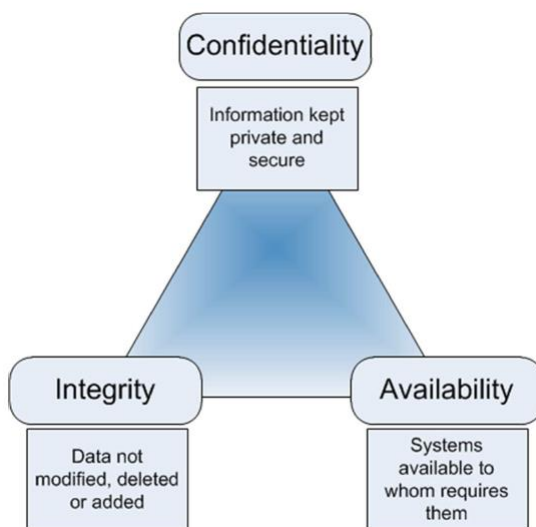


Figura 1-4. Tríada CIA: Confidentiality, Integrity and Availability.

Fuente: material docente de la asignatura COM11: Gestión de la seguridad y análisis de riesgos.

Donde cada una de las dimensiones expuestas incluyen los siguientes aspectos principales:

- **Confidencialidad (Confidentiality):** se refiere a la propiedad de prevenir la revelación y divulgación, intencionada o no, de información sensible a personas o sistemas no autorizados. Con información sensible se incluye la relativa a la privacidad de las personas, a los secretos industriales o, en definitiva, cualquier información que pueda comprometer de alguna manera a una organización.
- **Integridad (Integrity):** se refiere a la propiedad de mantener los datos libres de modificaciones no autorizadas. Ello incluye igualmente evitar el borrado o la adición de datos no autorizados.

- **Disponibilidad (Availability):** se refiere a la condición de la información de encontrarse a disposición de quienes están autorizados para acceder a ella, ya sean personas, procesos o aplicaciones.

Si bien es cierto que las tres dimensiones mencionadas constituyen el núcleo fundamental de la Seguridad de la Información, no hay que olvidar que, en realidad, consta de cinco dimensiones, por lo que habría que añadir:

- **Autenticidad:** se refiere a la capacidad de los usuarios y sistemas legítimos de determinar la autenticidad del origen de la información, o bien, la autenticidad del destinatario de la misma. También incluye otros aspectos importantes como el no repudio:
 - No repudio en origen: prueba que el autor envió la comunicación.
 - No repudio en destino: prueba que el destinatario recibió la comunicación.

El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Está orientado principalmente a aspectos de verificación legal.

- **Trazabilidad:** por último, la trazabilidad se refiere a la capacidad de poder determinar quién accede a los recursos, qué hace sobre dichos recursos, a quién se le presta los servicios, etcétera. Incluye dos perspectivas:
 - Trazabilidad del uso del servicio: el objetivo es tener un control sobre a quién se le presta un determinado servicio.
 - Trazabilidad del acceso a los datos: el objetivo es conocer en todo momento quién accede a qué datos y qué hace con ellos.

Es una dimensión tan importante o más que las integrantes de la tríada, pues está **relacionada directamente con la Auditabilidad**, es decir, con la capacidad de realizar un análisis exhaustivo que permita determinar de manera fiable las causas de posibles incidentes o eventos anómalos, mediante la reconstrucción, revisión y análisis de la secuencia de eventos.

Por tanto, una vez expuestas las características e importancia de cada dimensión de seguridad, sirva de adelanto el anunciar que **el presente trabajo ofrecerá la posibilidad de trabajar con las cinco.**

Otro aspecto a destacar englobado en el marco de la Seguridad de la Información es la **Defensa en Profundidad**, entendida como el concepto de aplicar medidas que garanticen la seguridad en todos aquellos puntos de interés para la seguridad de la organización. Tradicionalmente se tendía a pensar que adoptar una (o un conjunto reducido de medidas) de gran calado era suficiente para garantizar la seguridad corporativa. Esto puede llevar a uno de los grandes problemas de la seguridad: la falsa sensación de seguridad, confiarse y creer que se está a salvo. Cuando se necesitan implementar medidas de seguridad, ya sea de manera más compleja mediante la implantación de un Sistema de Gestión de Seguridad de la Información (en adelante, SGSI), o mediante un estudio más modesto, se debe aplicar el **principio del eslabón más débil**, basado en el símil de la cadena física: una cadena es tan fuerte como lo es su eslabón más débil. De igual manera, **la fortaleza de la seguridad de una organización es tan elevada como la del eslabón más débil de su seguridad**. En resumen, cuando se intenta asegurar una organización, **se hace necesario asegurar con cierta garantía todos aquellos puntos y aspectos en donde podría producirse un fallo que desemboque en un incidente de seguridad. El objetivo, por tanto, de la Seguridad de la Información es evitar o minimizar esos puntos o aspectos de una organización que pueden generar algún tipo de incidente en relación a los sistemas de información que alberga.**

Cuando se exponían anteriormente las perspectivas de la Seguridad de la Información, mostradas gráficamente en la Figura 1-3, se observaba que una de ellas es el Factor Humano. Tradicionalmente se tendía a pensar que la organización estaba suficientemente protegida mediante la aplicación de medios

técnicos. La experiencia ha demostrado que, **en realidad, el eslabón más débil de toda organización está representado por su personal, por el factor humano**. De hecho, conforme la tecnología y el desarrollo de sistemas y técnicas de seguridad avanzan, cada vez resulta más costoso a los atacantes saltar las medidas de protección, por lo que optan por abrir brecha a través del personal de la organización objetivo. Para ello, suelen servirse de vectores de ataque* iniciales como la ingeniería social*, el phishing* o la inserción de troyanos* a través del personal de la organización, de tal manera que les permitan ir escalando hasta lograr acceso a los activos principales de la organización.

Por otro lado, **la Seguridad de la Información debe abordarse como un proceso**, no como un producto. Es decir, se trata de una actividad de aplicación continua durante la vida de la organización, que incluye las siguientes actividades:

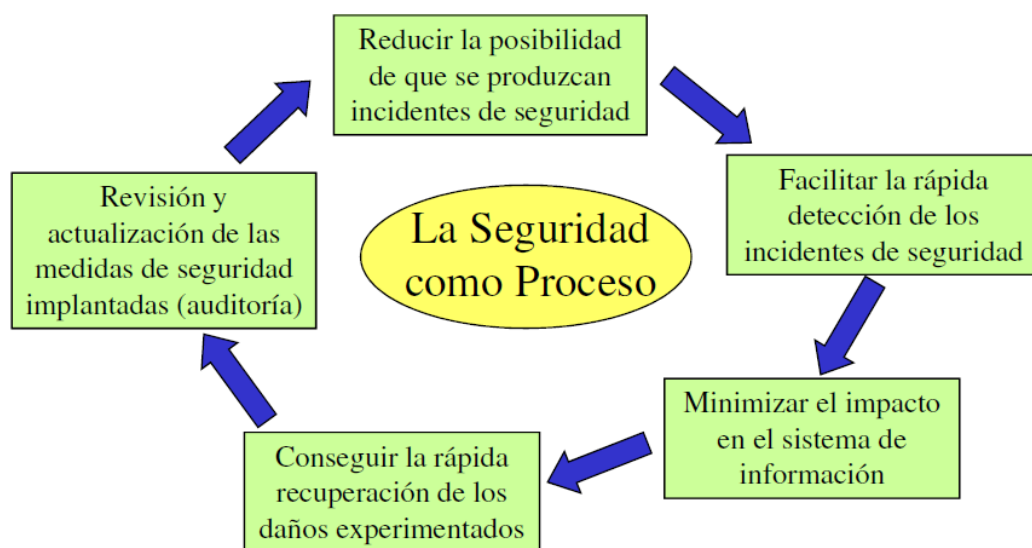


Figura 1-5. Seguridad de la Información como Proceso: Actividades.

Fuente: material docente de la asignatura COM11: Gestión de la seguridad y análisis de riesgos.

La consecuencia final de aplicar un sistema de Seguridad de la Información se materializa mediante los **controles de seguridad** que se aplican para garantizar la misma. En el ámbito de las Administraciones Públicas (en adelante, AA.PP.) en el que se enmarca el desarrollo de este trabajo, a los controles de seguridad se les denomina **medidas de protección**. Su objetivo es establecer mecanismos para reducir la probabilidad de ocurrencia de incidentes y, en el caso de producirse, disminuir su impacto sobre los activos de la organización. En resumen, **las medidas de protección persiguen reducir los efectos de una amenaza o vulnerabilidad de la seguridad**.

La forma de determinar las medidas de protección aplicables viene marcada por un estudio previo denominado **Análisis de Riesgos**, en el cual **se tiene en cuenta además la dimensión económica**. El Análisis de Riesgos permite concluir la categorización del sistema y las medidas correspondientes a aplicar. En el marco de este trabajo, no se hace necesario un Análisis de Riesgos previo para categorizar el sistema, pues la plataforma está pensada para sistemas de categoría Alta donde se manejen activos de información sensible, como puede ser: información gubernamental, datos personales, información clasificada, aplicación sobre sistemas de información del Ministerio de Defensa, etcétera.

Por otro lado, además de la categorización del sistema, hay que determinar **qué conjunto de medidas de protección se aplica, según el estándar o normativa con los que se opere**. En la actualidad y considerado en el ámbito nacional, existen dos estándares principales para la aplicación de medidas de protección (o controles de seguridad):

- **ISO 27000:** se trata de un estándar de ámbito internacional, que se puede aplicar de manera voluntaria por parte de las organizaciones. Está enfocado a las organizaciones de ámbito privado, y permite el diseño e implantación de un SGSI. Constituye una familia de estándares:
 - ISO 27001: contiene las especificaciones para la implantación de un SGSI. Se trata de una **norma certificable**.
 - ISO 27002: código de buenas prácticas. Incluye un conjunto de **controles de seguridad** aplicables, estructurados en **Dominios, Objetivos y Controles en sí**.
 - ISO 27003: guía de implantación de un SGSI.
 - Etcétera.

Reseñar que toda la documentación relativa a este estándar es **de pago**.

- **Esquema Nacional de Seguridad (ENS):** se trata del estándar para la Seguridad de la Información establecido para las AA.PP. Se trata de un conjunto de normativas (Leyes y Reales Decretos) que tienen por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Ámbito de aplicación: AA.PP., entidades de derecho público vinculadas o dependientes de las mismas; los ciudadanos en sus relaciones con las AA.PP.; y relaciones entre las distintas AA.PP.

Se desarrolla en forma de guías, publicadas por el Centro Criptológico Nacional (en adelante, CCN), y contempla 75 medidas de seguridad:

75 MEDIDAS DE SEGURIDAD RECOGIDAS EN EL ENS



Figura 1-6. Esquema Nacional de Seguridad: Medidas de Seguridad.

Fuente: <https://www.ccn-cert.cni.es/ens.html>

El presente trabajo se centrará en el uso del ENS, con una pretensión clara de su aplicación en el ámbito de las AA.PP. y, llegado el caso, su adaptación para el uso en el Ministerio de Defensa (en adelante, MINISDEF).

Como se observa, el conjunto de medidas de seguridad del ENS se distribuye en tres apartados:

- **Marco Organizativo:** según define la guía CCN-STIC 804, de Implantación del ENS, en su versión de junio de 2017, se trata del conjunto de medidas relacionadas con la organización global de la seguridad.
- **Marco Operacional:** medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
- **Medidas de Protección:** desarrolla las medidas de protección en sí, a aplicar para la protección de los activos, y según el nivel requerido en cada dimensión de seguridad.

De los tres apartados, este trabajo se centrará en el relativo a las **Medidas de Protección**, toda vez que están **directamente relacionadas con la Gestión de Incidentes de Seguridad de la Información**. Los apartados Organizativo y Operacional, como puede consultarse en la mencionada guía, sientan las bases teóricas para la preparación de la seguridad del sistema, pero no aportan medidas concretas para la gestión de incidentes.

Para poder seguir contextualizando el entorno en el que se enmarca el trabajo, se hace necesario introducir el concepto de **Centro de Operaciones de Seguridad (en adelante, COS)**, también conocido por su término homónimo en inglés, Security Operations Center (SOC), ya que el núcleo fundamental de estas instalaciones suele ser un aplicativo del estilo del que se pretende desarrollar a lo largo del presente trabajo.

En la actualidad, la Seguridad de la Información ha adquirido tal importancia que, para las grandes organizaciones, ya sean de carácter público o privado, no es suficiente con disponer de ciertos recursos (hardware, software y personal) dedicados a garantizar la seguridad de la corporación, como era habitual tradicionalmente. En la mayoría de casos han desplegado un centro propio de operaciones relacionadas con la seguridad, donde la Seguridad de la Información ocupa un lugar destacado. El propio MINISDEF dispone de varios de ellos: el Mando Conjunto de Ciberdefensa dispone de dos en sus instalaciones de Retamares que centraliza la seguridad de todo el ámbito militar: uno para las redes que manejan información clasificada, y por otro para las redes de propósito general. El CESTIC, aunque más limitado y con mejor recorrido y experiencia, dispone de otro COS. Incluso el propio Ejército del Aire dispone de uno propio en su Cuartel General. Durante el desarrollo de las prácticas con la empresa Telefónica tuve el placer de visitar su COS principal ubicado en Gran Vía, 28 de Madrid, y tengo que decir que me sorprendió muy gratamente. Aprovechando mi experiencia en la visita a dicho COS, sin duda uno de los más avanzados en la actualidad, y la **entrevista al Sr. Alejandro Ramos, actualmente Global Digital Security Officer (GDSO) de Telefónica, publicada en la revista red seguridad, nº 81, segundo trimestre 2018**, resumiré e introduciré los aspectos principales de las líneas de actuación y funciones desarrolladas en un COS.

Lo primero que se observa es una nueva estructuración de la gestión de la Seguridad de la Información. Lo que tradicionalmente se conoce como Seguridad de la Información, sigue teniendo su departamento propio y se encarga de las medidas preventivas. Por otro lado, se crea un nuevo departamento, denominado Ciberseguridad, encargado de las tareas de anticipación, detección y respuesta. Gráficamente la estructura sería así:

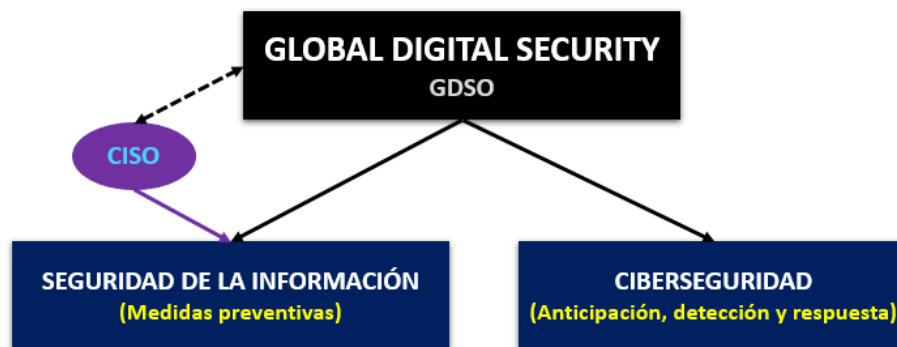


Figura 1-7. Nueva estructura de Seguridad Digital Global de Telefónica.

El jefe del apartado de Seguridad de la información continúa siendo el CISO* (Chief Information Security Officer), si bien se encuentra integrado en el equipo del GDSO.

Esta nueva estructura facilita seguir el ciclo de vida de la amenaza.

Cuenta con los siguientes medios para cubrir cada aspecto de las amenazas:

- Cuenta con un departamento denominado Ciberinteligencia dedicado a la anticipación. Su objetivo principal es analizar las nuevas amenazas. Consta de las siguientes partes:
 - Recopilación de información para la toma de decisiones, con datos e información desde una perspectiva técnica. Esta información se cruza con la del departamento de Inteligencia, para obtener la componente contextual (social, política, etcétera).
 - Indicadores de compromiso: se agrupan y comparten todas las huellas de los incidentes del Grupo Telefónica.
 - Técnicas de *deception*: consisten en poner trampas para ver qué actores les están agrediendo tecnológicamente.

Con todo ello pueden formar una Base de Conocimiento, lo que permite estar mejor preparado para las futuras amenazas.

- El departamento de Seguridad de la Información se encarga de la seguridad más tradicional, centrada en la prevención y las medidas técnicas.
- Cuenta con otros departamentos para funciones específicas, como el de Gobierno, el de Arquitectura o el de Transformación.
- Cuenta con un Red Team* para la detección de nuevas amenazas.
- Cuenta con un nutrido número de equipos de respuesta ante incidentes de seguridad informática (CSIRT, Computer Security Incident Response Team), desplegados por los países por donde Telefónica tiene presencia. En el caso de que se materialice una amenaza que no haya podido ser prevenida ni anticipada, la conformación de un CSIRT permite obtener una respuesta rápida. Ello reduce los tiempos de indisponibilidad y de recuperación.
- Por último, pero no menos importante, cuenta con un grupo de analistas dedicados a la detección de nuevas amenazas de tipo social, político o económico: hacktivismo, campañas de desprestigio, coordinación de actos vandálicos, ataques a partidos políticos, ciberterrorismo, etcétera. Esta parte, quizá la más novedosa y atrayente, ya se encontraba integrada en la plataforma de gestión de incidencias del COS de Telefónica.

De todo ello, se hace necesario ahondar en algunos apartados.

Por un lado, ampliando el concepto de **anticipación**, el objetivo es contar con información suficiente que permita, a partir de posibles indicios, como pueden ser eventos o comportamientos anómalos, identificar una posible amenaza no contemplada anteriormente. Ello sirve para la detección temprana, e incluso para la aplicación de una posible salvaguarda si ya se cuenta con ella. Este apartado se potencia de manera considerable cuando la organización cuenta con un Red Team de alta capacidad.

Por otro lado, a medio camino entre la Seguridad de la Información tradicional (prevención, ante amenazas conocidas) y la anticipación (detección de amenazas aún no conocidas), se encuentran los sistemas automáticos **SIEM (Security Information and Event Management)**. Como su propio nombre indica, se trata de sistemas de gestión de eventos y de información de seguridad que complementan los sistemas tradicionales de detección de amenazas en el que se emplean analistas. En sus últimas versiones están dotados de capacidades avanzadas, incluyendo Machine Learning*, lo cual reduce significativamente el nivel de falsos positivos y de falsos negativos en la detección. Además de la detección en sí que ofrecen a partir de la correlación de los eventos detectados, estas herramientas ofrecen información valiosa gracias a la cual se pueden mejorar las medidas de seguridad. Se basan en dos técnicas principales:

- Fusión de datos: el objetivo es capturar y estructurar toda aquella información que puede ser relevante para detectar problemas de seguridad.
- Correlación de eventos: a partir de los eventos detectados, son capaces de correlarlos y llegar a la conclusión de si un conjunto de eventos puede considerarse una amenaza.

El motor para la correlación es la clave para la efectividad del sistema SIEM, empleando en la actualidad y, como se comentaba, sistemas avanzados como Machine Learning.

Su despliegue suele ser específico para cada escenario, en función de las características de la organización, puntos de acceso exteriores, dimensiones de las instalaciones, subredes, etcétera. En la siguiente figura se representa un esquema tipo de una organización, con una serie de recursos, y dónde se aplicaría el sistema SIEM:

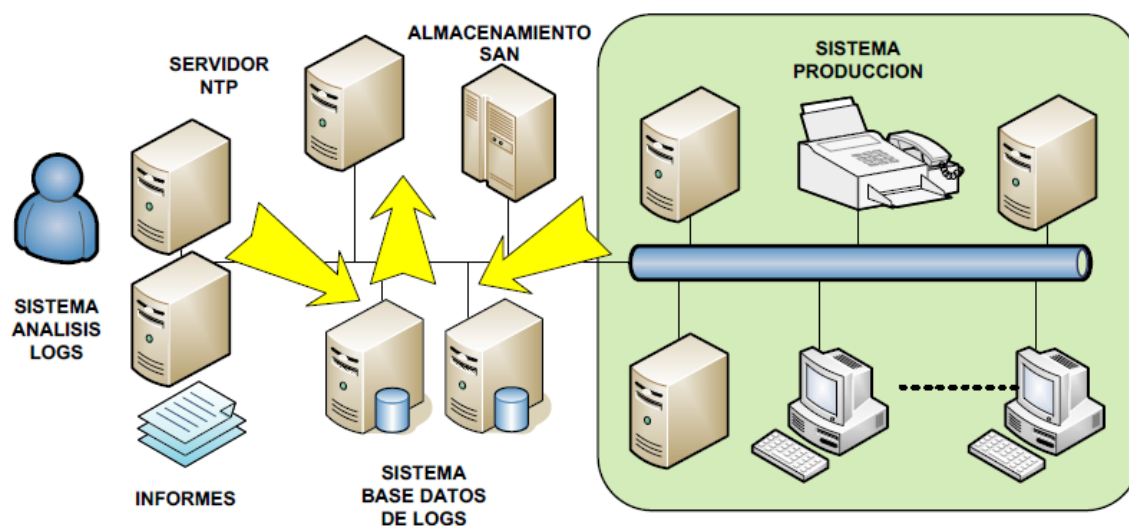


Figura 1-8. Escenario de aplicación de un sistema SIEM.

Fuente: material proporcionado por el profesorado de la asignatura Ciberseguridad, del Máster Universitario en Ingeniería de Telecomunicación, Universidad de Alcalá, curso 2015/2016.

Como se observa, **los puntos de interés sobre los que actúan el SIEM son aquellos donde reside información de registro de actividad**. La tarea de realizar la inspección por parte de analistas (personal humano) es bastante compleja, reservando este escenario únicamente para situaciones de

amenazas muy avanzadas y cuando se sabe qué se está buscando. Para el resto de escenarios, lo más habitual es utilizar sistemas de detección automático de tipo SIEM. En la siguiente figura se representa el esquema típico de la funcionalidad que alberga un sistema SIEM:

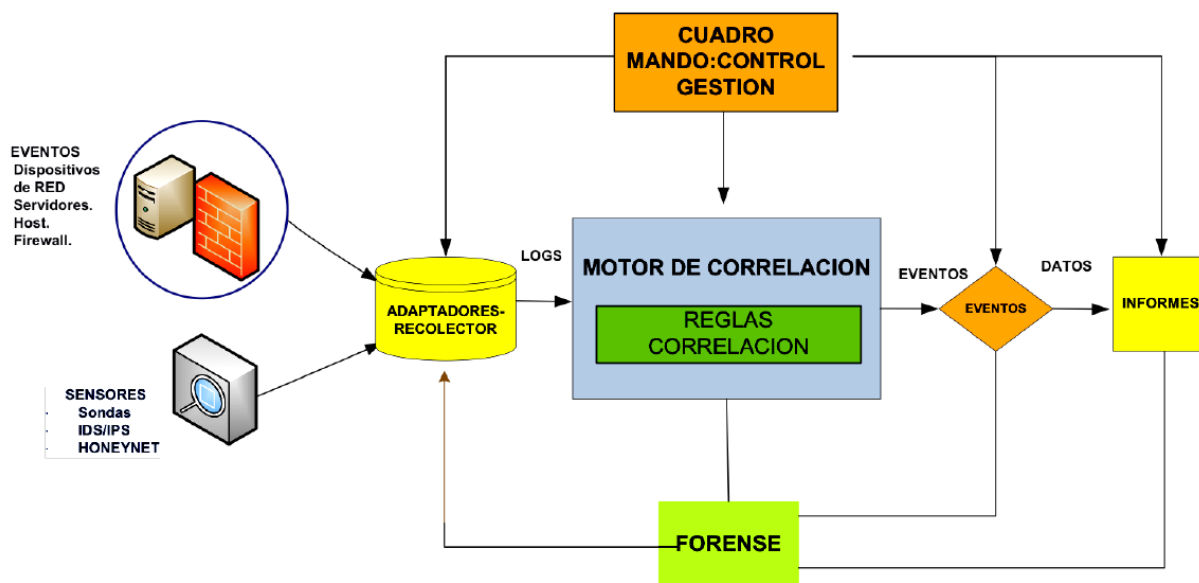


Figura 1-9. Estructura funcional de un sistema SIEM.

Fuente: material proporcionado por el profesorado de la asignatura Ciberseguridad, del Máster Universitario en Ingeniería de Telecomunicación, Universidad de Alcalá, curso 2015/2016.

Los bloques funcionales principales de que consta son:

- Recolector: se encarga de capturar y fusionar toda aquella información de interés relativa a eventos de actividad.
- Motor de correlación: constituye el núcleo del sistema. Se encarga de correlar la información de los eventos que recibe a partir de unas reglas de correlación. La complejidad de estas reglas y la forma de interpretarlas y aplicarlas por parte del motor de correlación es la clave para la efectividad en la detección. En este punto es donde se están empezando a aplicar técnicas avanzadas, como el Machine Learning, por ejemplo.
- Eventos: mediante este módulo el sistema resuelve los eventos que haya determinado en base a los registros de actividad y la aplicación de motor de correlación.
- Informes: el sistema emite informes a partir de los eventos detectados.
- Forense: a partir de los eventos que haya determinado y los informes confeccionados, se realiza un análisis forense que sirve para realimentar y mejorar el propio sistema, aplicándolo tanto sobre el recolector, como sobre el propio motor de correlación.
- Cuadro de mando: el sistema en su conjunto se encuentra orquestado por el cuadro de mando, donde se centraliza el control de la gestión.

Este trabajo contempla el uso de un sistema SIEM para la detección de incidentes de Seguridad de la Información. Por limitaciones de tiempo, este apartado se ha tenido que simular, generando los datos, bajo ciertos criterios, que ofrecería un sistema de estas características. **Sería muy interesante, y ya se adelanta como posible línea de trabajo futura, el poder adaptar un sistema SIEM real, a ser posible de desarrollo propio para evitar la dependencia de terceros, a la plataforma Soteria.** Contribuiría en gran medida a mejorar la calidad de la detección, reducir el nivel de amenazas y liberar al personal de seguridad de aquellas tareas más tediosas de análisis y detección.

Por último, sería interesante destacar el papel, cada vez más relevante, que están adquiriendo los **Equipos de Respuesta (CSIRT ≡ Computer Security Incident Response Team, término empleado en Europa, o el término protegido y registrado en EE.UU. CERT ≡ Computer Emergency Response Team)**. Ello viene reforzado principalmente por dos factores: el hecho de que cada vez se producen más ciberataques, de mayor extensión y mayor afectación; y el hecho de que las organizaciones comienzan a ser conscientes de las bondades de contar con un equipo de estas características: reducción de los tiempos de indisponibilidad y reducción de los tiempos de recuperación, redundando en una disminución considerable del lucro cesante.

Hay que ser conscientes, sin embargo, de que **disponer de un CSIRT o grupos de CSIRT's supone un coste elevado**, que no todas las organizaciones se lo pueden permitir, especialmente las PYME's*. En estos casos existen dos alternativas principales:

- **Contratar un servicio de seguridad:** cubren, según lo contratado, determinadas garantías en el apartado de Seguridad de la Información. Según las coberturas, la prima puede ser elevada.
- **Transferir el riesgo mediante la contratación de un seguro:** puede ser una opción más económica que la anterior, pero requiere que la organización cuente con un mínimo de medidas de seguridad, y que el riesgo residual sea aceptable. De no ser así, es posible que ninguna empresa de seguros acepte cubrir tu empresa.

La situación no es fácil para las empresas de reducido nivel de facturación, ya que en la actualidad queda demostrado que se requiere un buen nivel de seguridad, y ello requiere un presupuesto acorde.

Cuando se habla de equipos de respuesta de tipo CSIRT, normalmente se suele referir al organismo que se encarga de la respuesta ante incidentes de seguridad en tecnologías de la información, y que engloba un conjunto de recursos, así como un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. En el presente trabajo **el concepto de CSIRT se aplicará en forma de microcélulas formadas por tres (3) expertos en Seguridad de la Información**. El objetivo será muy similar, pero enfocado y aplicado sobre la gestión de una determinada incidencia de severidad crítica. Ante este tipo de eventos, tres personas puede ser un número idóneo en el sentido de poder mantener una buena coordinación, y al mismo tiempo poder dividirse las diversas tareas de gestión que requiera la atención de la incidencia.

Lógicamente, el contar con células de tres personas para este objetivo quiere decir que la organización debe ser de la suficiente entidad y contar con el suficiente personal como para poder permitirse un despliegue de estas características. Un caso de uso típico podría ser un ayuntamiento de una gran ciudad, o un ministerio, donde la envergadura de las instalaciones, los recursos de información que alberga y el elevado número de personal con que cuenta, puede suponer un escenario ideal. En el ámbito del **MINISDEF**, un escenario típico también podría ser un gran organismo como **las instalaciones del propio Ministerio, un Cuartel General, o la Agrupación de un conjunto de UCO's** (Unidades, Centros u Organismos) en una base aérea.

Una vez expuestos los conceptos fundamentales relacionados con el presente trabajo, se muestra un esquema general del contexto donde cabría aplicar la plataforma Soteria:

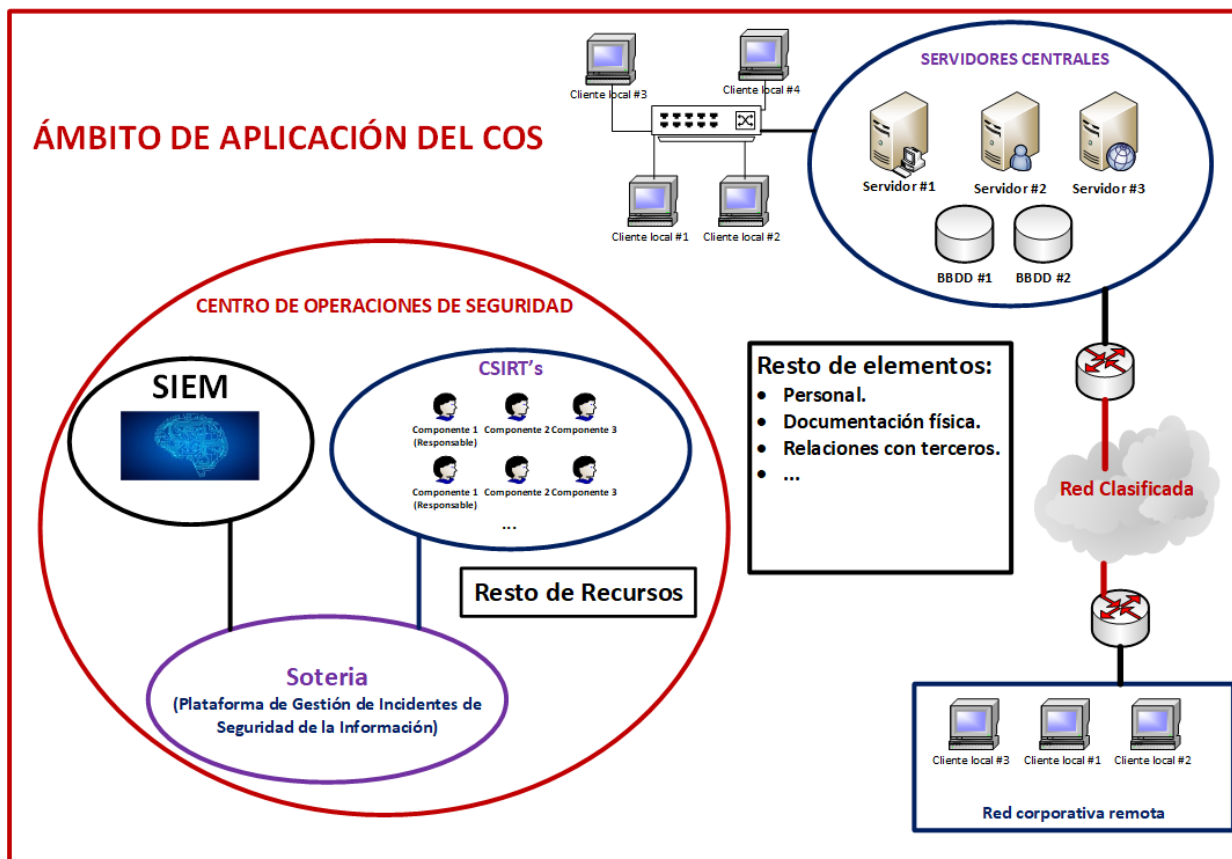


Figura 1-10. Esquema general de aplicación de la plataforma Soteria.

En un escenario tipo, los componentes principales del esquema serían los siguientes:

- **Recursos corporativos:** incluye todos aquellos recursos destinados al normal desempeño de la organización, redes propias, servidores centrales, terminales de acceso cliente, redes corporativas remotas, etcétera. Se puede apreciar un detalle importante que se representa en el esquema y que no conviene dejar para el final, y es el hecho de que la plataforma Soteria pretende cubrir cualquier ámbito de la Seguridad de la Informática, en todas sus áreas. De ahí que se representen también el conjunto de elementos o resto de componentes de la organización que no son estrictamente recursos informáticos: personal, documentación física, relaciones con terceros (otras organizaciones, proveedores, etc.). Como se comentaba anteriormente, un incidente de seguridad puede ser tanto el hecho de un intento no autorizado mediante medios telemáticos, como el hecho de encontrarse una nota por el suelo con los datos de autenticación de una cuenta, o el hecho de encontrarse documentación física clasificada en una papelería.
- **Centro de Operaciones de Seguridad (COS):** constituye el núcleo centralizado de la Seguridad de la Información en la organización, de ahí que **deba tener visibilidad de todos los recursos** de la organización para un desempeño efectivo. Según cómo esté conformado, la envergadura de la organización, los aspectos de Seguridad de la Información que se cubran, etcétera; podrá disponer de unos bloques funcionales u otros. Previamente se mostraba el ejemplo concreto del COS principal de Telefónica en Gran Vía, 28 de Madrid. En el caso del escenario tipo planteado para este trabajo, su composición es la siguiente:
 - **Plataforma de Gestión de Incidentes de Seguridad de la Información:** en este caso, representada por Soteria. Como su propio nombre indica, se trata de una plataforma

con una serie de recursos cuyo objetivo principal es centralizar y facilitar la gestión de incidencias al personal responsable de seguridad que integra el COS.

- Equipos de Respuesta: representa el conjunto de recursos humanos que actuarán como personal responsable de seguridad para atender aquellas incidencias más críticas, cuando las circunstancias precisen la conformación de un Equipo de Respuesta. Será, por tanto, un apartado importante y la gestión de dicho personal se podrá realizar desde la misma plataforma de gestión.
- SIEM: como se mostró anteriormente, contar con un sistema automatizado de detección contribuye a incrementar considerablemente la eficiencia del COS y reducir el nivel de amenaza. Se estima que este componente será cada vez más relevante y utilizado en los centros de seguridad, en especial, en las grandes corporaciones.
- Resto de recursos: incluye el resto de elementos del COS, como otros departamentos relacionados con la seguridad, personal directivo y de coordinación, como el CISO, recursos de apoyo, etcétera.

Como se observa en el esquema, tanto el conjunto de personal de responsable de seguridad integrante de los Equipos de Respuesta, como el sistema SIEM ofrecen sus servicios a Soteria, es decir, **la Plataforma de Gestión de Incidentes integra ambos componentes**.

Planteado este escenario, originalmente el autor de este trabajo se planteó trabajar en algunas de las dos líneas siguientes:

- Plataforma de Gestión de Incidentes de Seguridad de la Información: supone un reto interesante el poder diseñar, implementar y ofrecer una solución sencilla, segura y de fácil acceso, para la gestión de incidentes. Es un trabajo eminentemente práctico.
- SIEM: supone también un reto muy interesante, en el sentido de poder contribuir al diseño y desarrollo de un sistema de estas características, con las bondades que ofrece de cara a la mejora en la detección, y en la reducción de amenazas. Es un trabajo con una base fundamentalmente teórica.

A día de hoy, resulta difícil encontrar una solución de gestión de incidencias de Seguridad de la Información de las características pretendidas en el ámbito de las AA.PP., que aúne los distintos conceptos expuestos. En el MINISDEF, tal como se verá en el siguiente apartado, se ha tenido que optar por un desarrollo externo. Por lo que esta opción parecía sin duda la más práctica e interesante. **De ahí que se haya optado por esta línea.** No obstante, queda la duda de qué hubiera pasado de haberse elegido la otra línea de trabajo, también muy interesante y necesaria. Como se verá en el apartado de líneas futuras, sin duda, el **completar este esquema de Seguridad de la Información con un sistema SIEM** sería un gran logro. Hay que tener en cuenta, además, que los sistemas de Machine Learning se basan en el uso de ejemplos y experiencia humana, por lo que el paso previo a desarrollar un SIEM suele ser poder completar un proyecto que recolecte dichos datos, como es el caso del presente trabajo. **Ojalá pueda verse algún día.**

Por último y aunque su aplicación se sale del alcance de este trabajo, se hace necesario, cuando menos, hacer una referencia a los Sistemas de Gestión de Seguridad de la Información (SGSI). Por un lado, es conveniente aclarar que un SGSI y la aplicación que se pretende desarrollar mediante el presente trabajo son conceptos distintos, si bien Soteria cubriría una parte importante parte de lo que ofrecería un SGSI. Por otro lado, un SGSI está más enfocado a su aplicación en el sector privado. En el sector público, el propio ENS ya constituye en sí mismo un SGSI. En cualquier caso, son sistemas distintos, y la aplicación de un SGSI se sale del alcance de este trabajo. En la referencia [1], se indican algunas normativas relativas a la gestión de incidentes en el marco de un SGSI.

1.2 Motivación

Una vez planteados los aspectos principales del contexto en el que se enmarca el presente trabajo, la pretensión del mismo consiste en diseñar e implementar una plataforma web para la Gestión de Incidentes de Seguridad de la Información, en el marco del ENS, con vistas a su posible uso en el entorno de las AA.PP. y, llegado el caso, en el ámbito del MINISDEF. El objetivo es aunar bajo una misma plataforma de acceso seguro y multiusuario, los distintos conceptos vistos en la introducción, en especial, los relativos a la gestión de incidencias, gestión de equipos de respuesta, gestión de personal de seguridad y gestión del Conocimiento.

La idea original surgió antes incluso de comenzar las prácticas asociadas al Curso en Distrito Telefónica. El autor del presente trabajo contaba con alguna experiencia en el desarrollo de servicios web, y la idea de desarrollar un sistema centralizado de gestión de incidencias de Seguridad de la Información era, sin duda, la primera opción.

Cuando se plantearon las empresas en las que podía desarrollar las prácticas, no hubo duda, el contenido de las mismas, basado principalmente en la gestión de incidentes, llevó a seleccionar Telefónica en primer lugar. Para ser sincero y honesto, no se pudo enfocar las prácticas como hubiese gustado: más orientado a la gestión de incidencias, a nivel de gestión, dirección, coordinación. Las prácticas, en lo fundamental, se basaron en el seguimiento de un curso de Red Team. Pero la organización de las mismas incluía la visita al COS principal de Telefónica, en Gran Vía, 28 de Madrid, lo cual supuso el punto de inflexión para decidirse por asumir el reto de este desarrollo.

Otro aspecto a valorar en su momento era la existencia de sistemas similares en el ámbito de las AA.PP., especialmente en el ámbito del MINISDEF. Se descubrió que la única herramienta de similares características era LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas). Según se describe en la propia página [2] del CCN: *es una herramienta desarrollada por el CCN-CERT* para la Gestión de Ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Con ella se pretende mejorar la coordinación entre el CERT Gubernamental Nacional y los distintos organismos y organizaciones con las que colabora. LUCIA ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados. Con la herramienta LUCIA, el organismo podrá gestionar tres tipos de ciberincidentes:*

- *Los incidentes propios del Organismo.*
- *Los provenientes del Sistema de Alerta Temprana de Red SARA (SAT-SARA*).*
- *Los provenientes del Sistema de Alerta Temprana de Internet (SAT-INET).*

Como se observa, es una herramienta muy completa, si bien comporta algunos inconvenientes, en algunos casos difíciles de salvar:

- Es una herramienta de **difícil curva de aprendizaje**.
- Se trata de una herramienta de escritorio para sistemas CentOS Linux. Para disponer de acceso requiere su despliegue sobre un sistema Linux y conocimientos de administración de dicho Sistema Operativo. Ello **impide** además **el acceso corporativo a través de dispositivos móviles, como teléfonos inteligentes o tablets**.
- En el entorno del MINISDEF, aunque el CCN desea que todo se centralice a través de esta herramienta, es de difícil adaptación y uso, ya que, según explica personal de ISDEFE* destinado en la *Sección de Gestión de Incidentes y Monitorización* del Mando Conjunto de Ciberdefensa, **al pasar los datos a la herramienta LUCIA pierden el control sobre los mismos**. Esto, por un lado, tiene su lógica para evitar la duplicidad e incoherencia de los datos. Pero hay que entender que **perder el control de los datos**, teniendo en cuenta que se trata de un organismo de seguridad del MINISDEF, y de los datos a que se refiere, **no es**

aceptable. Además, el hecho de que un organismo militar pase información a otro organismo/ámbito de las AA.PP., no está bien visto por los Mandos. Finalmente, se optó por un desarrollo personalizado de una herramienta llamada SIRIUS IT PRO [3]. El problema de los desarrollos externos, además de que normalmente necesitan ser adaptados, presentan el inconveniente de **la dependencia de empresas**, algo tampoco bien visto en el MINISDEF. La herramienta tuvo además que ser adaptada, pues estaba pensada como servicio de gestión de incidencias de tipo general, por lo que carecía de la recogida de datos y funcionalidades específicas para la gestión de incidencias de Seguridad de la Información. Por último, comentar que trabaja sobre el sistema OTRS (Open-Source Ticket Request System), el cual es una plataforma de comunicación de gestión de procesos y de ticketing* que puede ser utilizado para normalizar los identificadores empleados en las peticiones. Si bien, está pensado más para gestión de solicitudes que para incidencias, y, en el caso de incidencias, está pensado para tratar incidencias de tipo general.

- Otro inconveniente, en este caso **insalvable**, viene del hecho de que la herramienta LUCIA trabaja de modo centralizado, **empleando redes abiertas** para la interconexión entre sus nodos (Internet en el caso de INET, o bien la red SARA). En el caso de redes de propósito general, como puede ser la red WAN-PG del MINISDEF, cabría aplicarse la herramienta. Pero **en el caso de redes clasificadas sería imposible**, ya que dichas redes deben permanecer **aisladas**, sin acceso a redes abiertas. Es por ello que **una de las premisas de este trabajo es que pueda accederse y ejecutarse, con el 100% de su funcionalidad, desde redes cerradas y aisladas.**

La única herramienta que, quizá, se acerque algo a lo que se pretende es la iniciativa de código abierto OSSIM (Open Source Security Information Management) [4]: se trata de un sistema para la gestión automatizada de información de seguridad y de eventos. Está dotado de un sistema SIEM y cuenta con distintas herramientas para los administradores de seguridad informática, incluida la generación de gráficas. El problema que plantea es el ser una iniciativa de código abierto, donde el mantenimiento reside en la “comunidad” y, por tanto, no se tiene control sobre él ni está respaldado por una firma. Por otro lado, está enfocado, como en la mayoría de este tipo de herramientas, en las incidencias de seguridad informática, no cubre el ámbito global de la Seguridad de la Información.

Por tanto, se considera que **el poder proponer una herramienta de desarrollo interno de estas características puede ser de gran interés y utilidad.** Como es lógico, está basado en un Trabajo de Fin de Máster de 6 créditos, y desarrollado por una única persona, por lo que debe considerarse como un proyecto muy preliminar de lo que tal vez pueda convertirse algún día en una herramienta utilizable.

Otro factor de gran importancia a tener en cuenta se refiere a las bondades que ofrece el disponer de un sistema de gestión de incidentes de Seguridad de la Información:

- Contar con una solución en donde el personal responsable de seguridad y los equipos de respuesta puedan registrar, valorar y tratar los incidentes de manera ágil y eficaz.
- Tener la tranquilidad de que toda la información relacionada con un incidente se encuentra integrada y disponible cada vez que se requiera.
- Poder responder fácilmente a los entes de control y de auditoría acerca de la debida diligencia en la atención de incidentes (Auditabilidad y servicio de Notificaciones).
- Convertir los datos en información valiosa descubriendo cómo los incidentes afectan a la organización y cuál es la tendencia de los mismos (Gestión del Conocimiento).
- Poder identificar cual es la eficacia en la gestión de los incidentes y poder así establecer las capacidades que se deben fortalecer (Gestión del Conocimiento).

El disponer de una base de Conocimiento ofrece, además, una gran ventaja competitiva:

- Disminuye la ocurrencia de incidentes de seguridad: seguridad activa.
- Disminuye su impacto en caso de producirse: seguridad pasiva.
- Reduce los tiempos de respuesta y de recuperación: mejora de la Disponibilidad.
- Posibilita el desarrollo de un sistema SIEM.

Dichas ventajas contribuyen a mantener la Continuidad del Negocio o, siendo más exactos, contribuye a minimizar los tiempos de interrupción del negocio, mejorando la satisfacción del cliente. En el caso de su aplicación en el ámbito de las AA.PP., no cabe el concepto de competitividad, pero sí el de **satisfacción del cliente (ciudadanos)**.

Esta sinergia de beneficios contribuye a:

- La credibilidad: las organizaciones que cuentan con un sistema de gestión de Seguridad de la Información robusto cuentan con mejor credibilidad por parte de clientes, proveedores y, en resumen, de terceros. En el caso de las AA.PP., la credibilidad principal viene por parte de los ciudadanos que utilizan sus servicios.
- La confianza: al igual que en el caso anterior, también se cuenta con mejor confianza por parte de terceros.
- Cumplimiento de la ley: se demuestra que se cumple con la normativa legal vigente.
- Eficiencia y ahorro en costes: contar con un sistema de gestión de Seguridad de la Información contribuye al ahorro en costes, ya sea directos, en base a la mejora en eficiencia, o indirectos, como puede ser el evitar sanciones.
- Continuidad del negocio: se ofrecen mejores garantías de ello.

Añadir que, tal como se verá en el apartado 2.5 *Normativa y legislación*, el Real Decreto 3/2010, de 8 de enero, por el que **se regula el Esquema Nacional de Seguridad**, establece la necesidad de contar con procedimientos de gestión de incidentes de seguridad. De hecho, la redacción de su **artículo 24**, relativo a **incidentes de seguridad**, **recoge precisamente el espíritu fundamental del presente trabajo**.

Como último apunte en relación al porqué de este desarrollo: **quizá sea un buen punto intermedio de partida, una buena solución intermedia, entre el ámbito de las AA.PP. y el del MINISDEF.**

1.3 Objetivos y alcance

Una vez expuesto el escenario de trabajo, la línea elegida y la motivación para la elección de dicha línea de trabajo, se pasa a sentar los objetivos y el alcance, los cuales marcarán el desarrollo de la funcionalidad de la plataforma.

Los objetivos principales se fundamentarán en reducir lo máximo posible el tiempo de interrupción de los servicios informáticos, así como evitar la fuga de información sensible. El disponer de una herramienta de estas características contribuye a lograr dichos objetivos y a mantener un adecuado nivel de seguridad, de alerta y de concienciación y formación del personal en materia de Seguridad de la Información. Todo ello, en conjunto, favorece la continuidad del negocio y mantener la buena imagen de la organización.

Por otro lado, la Seguridad y la Eficiencia serán los dos aspectos clave que marquen el diseño e implementación de la plataforma web.

Bajando a un nivel más detallado, en lo relativo al diseño e implementación de Soteria, se establecen los siguientes objetivos:

- Recogida de incidentes de seguridad de la información, catalogación y registro: la plataforma debe ser capaz de recoger los datos relativos a la detección de una nueva incidencia y registrarlos en una Base de Datos (en adelante, BBDD). Los datos relativos a cada incidencia deben ser lo suficientemente característicos para permitir la gestión efectiva y eficiente de la misma.
- Gestión de Equipos de Respuesta ante Incidentes de seguridad de la información: la gestión de Equipos de Respuesta será otro de los bloques funcionales principales del sistema. Debe permitir conformar y asociar un Equipo de Respuesta a aquellas incidencias de mayor severidad que lo precisen para su atención.
- Consulta de medidas de protección recogidas en la guía CCN-STIC 804, de Implantación del Esquema Nacional de Seguridad: el ámbito de aplicación pretendido de la plataforma serán las AA.PP. en general, y el MINISDEF en particular. Por tanto, se empleará el ENS y las guías elaboradas por el CCN. En concreto, se deberá emplear la Guía CCN-STIC 804, en su apartado 5, para extraer y ofrecer al personal responsable de Seguridad de la Información a través de la interfaz web las medidas de protección que contempla el ENS. Como funcionalidad adicional, además de ofrecer la consulta como referencia de dichas medidas de protección, se asociarán las mismas con cada incidencia según el tipo de incidencia de que se trate, así como se facilitará la trazabilidad de la misma mediante el control de su aplicación y las observaciones que requiera la aplicación de cada medida.
- Gestión de personal responsable de seguridad: se ofrecerá la posibilidad de gestionar los recursos humanos de la plataforma Soteria mediante el control de la situación del personal y los datos de contacto. Como funcionalidad adicional, se controlará las consecuencias que pueda tener la baja temporal del personal, como, por ejemplo, su participación en Equipos de Respuesta y su necesaria sustitución por personal en activo.
- Cuadro de mandos con estadísticas y gráficas para el apoyo a la toma de decisiones: mediante este objetivo se pretende ofrecer un conjunto de estadísticas y gráficas que ayuden al mando a la toma de decisiones. La BBDD ofrece suficientes datos como para ofrecer un amplio abanico de posibilidades. En este trabajo se desarrollarán algunas de ellas.
- Consolidación de una base de datos de Errores Conocidos (Conocimiento): a partir del histórico de incidencias cerradas, se realiza un compendio de la experiencia acumulada en su resolución. Ello permitirá utilizarlo por parte del personal responsable de seguridad como referencia de cara a facilitar la gestión de futuras incidencias. Los datos se seleccionarán y mostrarán según el tipo de incidencia, permitiendo al usuario enfocarse en el histórico de dicho tipo.
Como funcionalidad adicional, se ofrecerá también la posibilidad de consultar las incidencias notificadas, que constituyen aquellas incidencias de mayor severidad. Debido a que la propia BBDD Soteria cuenta con los suficientes datos para desarrollar esta funcionalidad, no se requiere crear una BBDD aparte de Conocimiento.
- Información específica de apoyo a la gestión de la seguridad de la información: se ofrecerá un apartado reservado para ofrecer información de interés relacionada con el ámbito de la Seguridad de la Información, como enlaces a documentos de interés, enlaces a revistas del sector, enlaces a sitios relacionados con la Seguridad de la Información en el ámbito público, etcétera.
- Acceso web seguro multiusuario: el acceso a los servicios de la plataforma se realizará mediante un canal web seguro vía HTTPS, y empleando algún sistema de autenticación. Además, se hace necesario que el acceso sea multiusuario, de tal manera que distintos usuarios puedan trabajar simultáneamente.

- Cumplimiento de la normativa legal vigente: de cara a cumplir el marco normativo, tanto español como comunitario (UE), se hace necesario implementar un servicio de notificaciones. Las notificaciones se efectuarán para las incidencias de severidad Crítica y Alta, con especial énfasis, y así debe quedar reflejado en la notificación, en las incidencias que supongan posibles violaciones de la seguridad de los datos personales. En el siguiente apartado se detalla el contexto legal que lleva al establecimiento de este objetivo.

Al margen de los objetivos principales descritos, se consideran también de interés los siguientes objetivos de cara a mejorar la seguridad y eficiencia de la plataforma Soteria:

- Validación de las entradas: aunque la plataforma no está pensada inicialmente para su uso en redes abiertas, se hace necesario la validación de los datos de entrada a través de la interfaz web. No ya desde el punto de vista de seguridad y evitar ataques de tipo inyección de código*, sino para evitar un malfuncionamiento del aplicativo al intentar procesar datos de un tipo distinto al esperado.
- Comprobación de la coherencia de los datos introducidos por los usuarios: se cuidarán todos aquellos detalles que pueden llevar a un malfuncionamiento de la plataforma, como, por ejemplo, iniciar una nueva incidencia, o modificar una ya existente, y no seleccionar ninguna dimensión de seguridad; o intentar asignar un Equipo de Respuesta a una incidencia de severidad inferior a Crítica; o seleccionar dos/tres veces el mismo usuario en los listados desplegables al modificar un Equipo de Respuesta.
- Depuración de efectos colaterales: se cuidarán detalles como:
 - Tal como se ha comentado antes, la baja de un personal responsable de seguridad, el cual estaba nombrado para participar en algún Equipo de Respuesta. Su baja podría afectar el normal desempeño del Equipo de Respuesta, por lo que se sustituye por otro miembro en activo.
 - Se cuidará también, por ejemplo, que, a la hora de conformar un Equipo de Respuesta, se seleccione únicamente entre el personal en activo disponible en ese momento. Se cuida también que las alteraciones de personal sean notificadas a los afectados. Por ejemplo, si un personal pasa a sustituir por baja temporal a otro compañero en un Equipo de Respuesta, se le notifica al correo registrado del mismo.
 - El cambio de los componentes de un Equipo de Respuesta es un aspecto muy importante de cara a la trazabilidad, por lo que se dejará reflejado en el campo de detalles de la propia incidencia.
 - Solo se permite cambiar la composición de Equipos de Respuesta para incidencias en activo o cuarentena. Si la incidencia está cerrada, además de no tener efectividad práctica ya que la incidencia está cerrada, afectaría a su trazabilidad.
 - Etcétera.

La siguiente tabla recoge un resumen de los objetivos propuestos. Será muy útil de cara al análisis de los objetivos logrados, una vez completado el trabajo:

Objetivo

Recogida de incidentes de seguridad de la información, catalogación y registro
Gestión de Equipos de Respuesta ante Incidentes de seguridad de la información
Gestión de medidas de protección recogidas en la guía CCN-STIC 804
Gestión de personal responsable de seguridad
Cuadro de mandos con estadísticas y gráficas para el apoyo a la toma de decisiones
Consolidación de una base de datos de Errores Conocidos (Conocimiento)
Información específica de apoyo a la gestión de la seguridad de la información
Acceso web seguro multiusuario
Cumplimiento de la normativa legal vigente (incluido servicio de notificaciones)
Validación de las entradas
Comprobación de la coherencia de los datos introducidos por los usuarios
Depuración de efectos colaterales

Tabla 1-1. Resumen de objetivos.

Respecto al **alcance**, aquellos **aspectos que sí atenderán** y se dará solución mediante el presente trabajo se encuentran recogidos en el detalle de los objetivos recién descritos. Los **aspectos que no se atenderán** serán los siguientes:

- Gestión de incidencias de tipo general: la plataforma Soteria, a priori, está pensada y diseñada para la gestión de incidentes de Seguridad de la Información de manera concreta. El resto de incidencias que pudiera sufrir una organización queda fuera del ámbito de este trabajo.
- Gestión de personal: la gestión del personal en Soteria se circunscribe al personal responsable de Seguridad de la Información, y con los datos mínimos necesarios para el adecuado desempeño de la plataforma. Queda fuera del ámbito de este trabajo la gestión del resto de personal de la organización, así como la gestión detallada y control de personal, que incluye la ficha de datos completos de cada trabajador de la organización. La plataforma Soteria no necesita esos datos, ni se ocupa de la gestión de personal fuera del ámbito de la Seguridad de la Información.
- Gestión de medidas de protección: como se indicaba unas líneas más arriba al exponer los objetivos, el presente trabajo está enfocado a su aplicación en el ámbito de las AA.PP., o del MINISDEF en concreto, y al amparo del ENS, por lo que las medidas de protección se circunscribirán a las recogidas en la Guía CCN-STIC 804, de Implantación del ENS, en su apartado 5. No obstante, se deja abierta la posibilidad, y así se reflejará en las posibles líneas de trabajo futuras, el poder aplicar otro conjunto de medidas de protección, o incluso añadir nuevas medidas por parte del propio personal responsable de seguridad.
- Información y apoyo a la decisión: la información y opciones de análisis que se ofrecen a través de la plataforma Soteria están enmarcadas en el ámbito de la Seguridad de la Información. No se contemplará, por tanto, aquello que se salga de dicho ámbito.
- SGSI: como quedaba expuesto en el apartado 1.1 *Introducción y contexto*, la aplicación de un SGSI en paralelo al despliegue de la plataforma Soteria se sale del alcance de este

trabajo. No obstante, hay que tener en cuenta que el ENS constituye un SGSI en sí mismo, y que la pretensión inicial es que la aplicación de la plataforma fruto de este trabajo se aplique en el ámbito de las AA.PP.

1.4 Organización de la documentación

La documentación que recoge el desarrollo del presente trabajo se encuentra organizada mediante los siguientes apartados:

- Apartado 1: introducción y objetivos. Recoge los conceptos y principios fundamentales sobre los que se asienta este desarrollo, así como el contexto de su aplicación.
- Apartado 2: estado del arte. Recoge un repaso a la situación actual en materia de sistemas de gestión de incidencias de Seguridad de la Información.
- Apartado 3: desarrollo del TFM. Recoge los aspectos fundamentales relacionados con el desarrollo del presente trabajo. Debido a que se trata de un trabajo técnico con implementación de software, este apartado supondrá el núcleo principal del trabajo, además de contener una carga técnica importante.
- Apartado 4: verificación. Como continuación del apartado anterior, en este apartado se ofrece la documentación relativa a la validación de la plataforma Soteria y su validación. Se demostrará la funcionalidad que ofrece finalmente la plataforma, lo cual permitirá por un lado validarla y, por otro, comparar la funcionalidad inicial pretendida con la funcionalidad final obtenida.
- Apartado 5: conclusiones y líneas futuras. A lo largo de este apartado se expondrán las conclusiones a las que se ha llegado una vez completado el trabajo, así como se enunciarán e introducirán las posibles líneas futuras a que da pie el mismo.
- Apartado 6: bibliografía. Recogerá las referencias utilizadas para la elaboración del presente trabajo, especialmente en relación a la documentación.
- Anexos. Mediante los anexos se ofrece diversa información de apoyo de interés relacionada con el presente desarrollo. Destacar especialmente el glosario ofrecido a través del Anexo I, el cual ofrece las definiciones fundamentales de los conceptos más importantes tratados a lo largo de este trabajo.

1.5 Fuentes de información

Para la confección de algunos aspectos del apartado *1 Introducción y Objetivos* se ha empleado material proporcionado por el profesorado de diversas asignaturas del presente Máster, así como de la asignatura Ciberseguridad del Máster Universitario en Ingeniería de Telecomunicación, Universidad de Alcalá, curso 2015/2016.

2 ESTADO DEL ARTE

2.1 Introducción

Mediante el apartado 2 *Estado del arte* se exponen diferentes aspectos enmarcados en el ámbito del presente trabajo, y relacionados con la situación actual en sus distintas facetas: tecnologías, estándares, Seguridad de la Información, normativas, etcétera. En concreto, se tratarán los siguientes aspectos:

- Aplicaciones de similares características: se realizará una exposición breve del estado del arte y características de algunas de las aplicaciones que presenten funcionalidades similares a la plataforma Soteria.
- Tecnologías y estándares existentes: se plantearán las tecnologías y estándares más habituales en el sector, y se decidirá cuáles se emplearán finalmente para el desarrollo del presente trabajo.
- Datos necesarios para la gestión de incidencias de Seguridad de la Información: se expondrá qué datos se han establecido de interés para la gestión de incidencias, así como para los demás los servicios, de cara a poder desarrollar la funcionalidad completa de la plataforma.
- Normativa y legislación: el cumplimiento de la normativa legal vigente será uno de los pilares fundamentales de este trabajo, no solo por el hecho del obligado cumplimiento, sino también teniendo en cuenta el ámbito de aplicación pretendido.
- Seguridad de la Información: se analizará de qué manera se cubre la Seguridad de la Información en este tipo de aplicaciones, y cuál ha sido la elección de soluciones para facilitar el desarrollo del trabajo.

2.2 Aplicaciones de similares características

Este punto ha sido fundamental para analizar qué datos son de interés para la gestión de incidencias en el ámbito de la Seguridad de la Información. De hecho, constituyó la primera iniciativa realizada durante la fase de elección del Trabajo de Fin de Máster. La numerosa información y vídeos existentes sobre aplicaciones reales de similares características, junto con la visión e idea que ya se tenían medianamente claras de lo que se pretendía, marcó la elección final y el comienzo del trabajo.

Para poder encarar este apartado, se hace necesario separar las aplicaciones en **dos ámbitos muy distintos: el Sector Público y el Sector Privado**. De hecho, antes incluso de decidir por qué sector decantarse y qué tecnologías, estándares y normativas utilizar finalmente, la primera iniciativa fue buscar información sobre aplicaciones de gestión de incidentes de seguridad **informática**. En todos los

casos iniciales, la información que aparecía era sobre iniciativas comerciales y vídeos demostración del uso a través de los canales de Youtube.

Otro detalle a recalcar, tal como se habrá observado, es que se ha destacado la palabra **informática**. Ello se debe a que, para poder encontrar soluciones de este tipo, hay que buscarlas con esa denominación, pues están pensadas para tratar incidentes de tipo informático. Precisamente, uno de los primeros objetivos marcados y motivación para el presente trabajo es intentar cubrir los incidentes de seguridad de cualquiera de las áreas de la Seguridad de la Información, no únicamente el relativo a infraestructura tecnológica. Por tanto, ya se puede concluir una primera característica común de las aplicaciones que actualmente existen en el mercado: **no cubren todas las áreas de la Seguridad de la Información**. Esta será una de las **características diferenciadoras** del desarrollo pretendido.

2.2.1 En el Sector Privado

La primera aplicación de similares características que se consultó fue *ServiceDesk Plus*, cuya información se encuentra disponible a través del enlace [5]. El punto de consulta y análisis de la aplicación fue un webinar* muy interesante sobre la aplicación accesible en [6]. Sus características y servicios principales ofrecidos son los siguientes:

- Permite clasificar y priorizar incidencias.
- Permite la implementación de niveles de servicios.
- Ofrece una base de Conocimientos.
- Contempla herramientas de ITIL* para mejorar la calidad del servicio.

Merece la pena comentar algunos aspectos sobre esta herramienta.

El primer aspecto a destacar es que está enfocado a tratar incidentes relacionados con IT. Eso quiere decir que no está diseñado explícitamente para la gestión de incidentes de seguridad informática. Es un detalle mayor, en el sentido de que, según el diseño y la función pretendida, permitirá trabajar con unos datos u otros de los incidentes. Por tanto, al margen del flujograma, y de cara a entender el proceso de atención de una incidencia, no es una referencia válida.

Otro aspecto, también importante, a destacar, tiene que ver con la información que se ofrece a través del webinar. En el video, la persona que presenta el producto hace distinción entre la gestión de incidentes y la gestión de problemas. Y que, en el caso de la gestión de incidentes, *"va exclusivamente a restaurar el servicio, no se preocupa de cuáles son las causas subyacentes"*. Esta forma de proceder, claramente inadecuada, es un indicativo de que la aplicación, como se explica, está pensada para solucionar el problema y levantar los servicios lo antes posible, sin entrar en los detalles de las causas que lo originaron, lo cual limita en gran medida la base de Conocimientos, además de impedir la mejora de la prevención (seguridad activa, evitar que vuelva a ocurrir).

Se puede concluir que se trata de una herramienta enfocada a la gestión de incidentes relacionados con IT, que no contempla, por tanto, las incidencias relacionadas con seguridad informática, por lo que no cubre la funcionalidad buscada.

Otra aplicación que podría considerarse es KMKEY HelpDesk, accesible mediante el enlace [7]. Es una herramienta algo más humilde que la anterior, no integra ITIL, pero en cualquier caso y en lo que respecta a este trabajo, adolece del mismo problema: es una herramienta para la gestión de incidencias de tipo general, enfocado a recursos IT y servicios, no es específica para atender incidencias de seguridad informática.

La primera solución que se encuentra enfocada a la gestión de incidentes de seguridad informática viene de la mano de la empresa CYBSEC Security Systems, accesible en [8]. Se trata de una empresa de origen hispanoamericano, pero con presencia en España. El problema que plantea es que no ofrece sus servicios de manera integrada a través de un único aplicativo, sino que ofrece sus servicios por separado:

- Site Defender: ofrece un conjunto de servicios profesionales: reporte de vulnerabilidades software, reporte de vulnerabilidades de configuración, seguimiento de las vulnerabilidades, gestión de alertas, herramientas para diagnóstico de seguridad, test de intrusión, etc.
- FAST TEAM 365: servicio CSIRT: ofrece de forma permanente un equipo de expertos altamente entrenados en el control y neutralización de incidentes.
- Detección y Rastreo de intrusiones: permite conocer con precisión cómo se produjo y, de ser posible, el origen de la intrusión.
- Análisis Forense Informático: ofrece un equipo de expertos especializados en detectar las evidencias y producir las pruebas documentales de las mismas.

Ofrece servicios avanzados de ciberseguridad, pero por separado. Ello, además, impide a la empresa que contrate dichos servicios tener un control y visión global de la gestión de incidentes, de hecho, ni la propia CYBSEC ofrece un servicio integral. En el caso además de aplicación que ocupa este trabajo no sería rentable su contratación, pues se cuenta ya con personal experto en seguridad informática que puede cubrir esos servicios.

En cualquier caso, ninguna de estas soluciones integra distintos aspectos de la Seguridad de la información, como **la asociación automática de medidas de protección y su gestión, o la gestión de Equipos de Respuesta de manera integrada**, características ambas **diferenciadoras**.

2.2.2 En el Sector Público

Como se reflejaba en el apartado *1.2 Motivación*, lo más semejante a la plataforma que se pretende desarrollar sería la herramienta LUCIA. En dicho apartado se argumentaba los inconvenientes que presenta. Por otro lado, respecto a la funcionalidad que integra, permite la clasificación, gestión y control de trazabilidad de las incidencias. Cuenta incluso con algunas funcionalidades avanzadas respecto a ello, pero, al igual que ocurría con las herramientas del sector privado, no ofrece funcionalidades adicionales integradas como la gestión de Equipos de Respuesta, o la asociación automática de medidas de protección.

Respecto a la solución que utiliza actualmente el Mando Conjunto de Ciberdefensa, como se exponía también en el apartado *1.2 Motivación*, se trata de una adaptación de la herramienta comercial SIRIUS IT PRO. Requiere adaptación ya que, en origen, está enfocada a la gestión de incidentes en infraestructuras IT, no es una herramienta para la gestión de incidencias de seguridad informática explícitamente. Recordar también que trabaja sobre el sistema OTRS, el cual está pensado más para gestión de solicitudes que para incidencias, y, en el caso de incidencias, está pensado para tratar incidencias de tipo general.

Recopilando toda esta información se llega a la conclusión de que, en la actualidad, **ni en el sector privado ni en el sector público se cuenta con una herramienta que integre la funcionalidad pretendida**.

2.3 Tecnologías y estándares existentes

El desarrollo del presente trabajo aglutina una serie de aspectos técnicos que conviene analizar antes de tomar una decisión respecto a cada uno de ellos.

El primer paso que se precisa es tener una visión global del sistema que se pretende desarrollar. La Figura 1-10 recogía de manera muy esquemática, pero clara, el esquema general del contexto donde se aplicaría Soteria. En el marco de dicho esquema, esta sección se centrará en el apartado relativo al COS y, más concretamente, en la funcionalidad que Soteria aporta al COS. Para poder tener una visión más nítida de lo que se pretende, se reproduce a continuación dicho apartado:

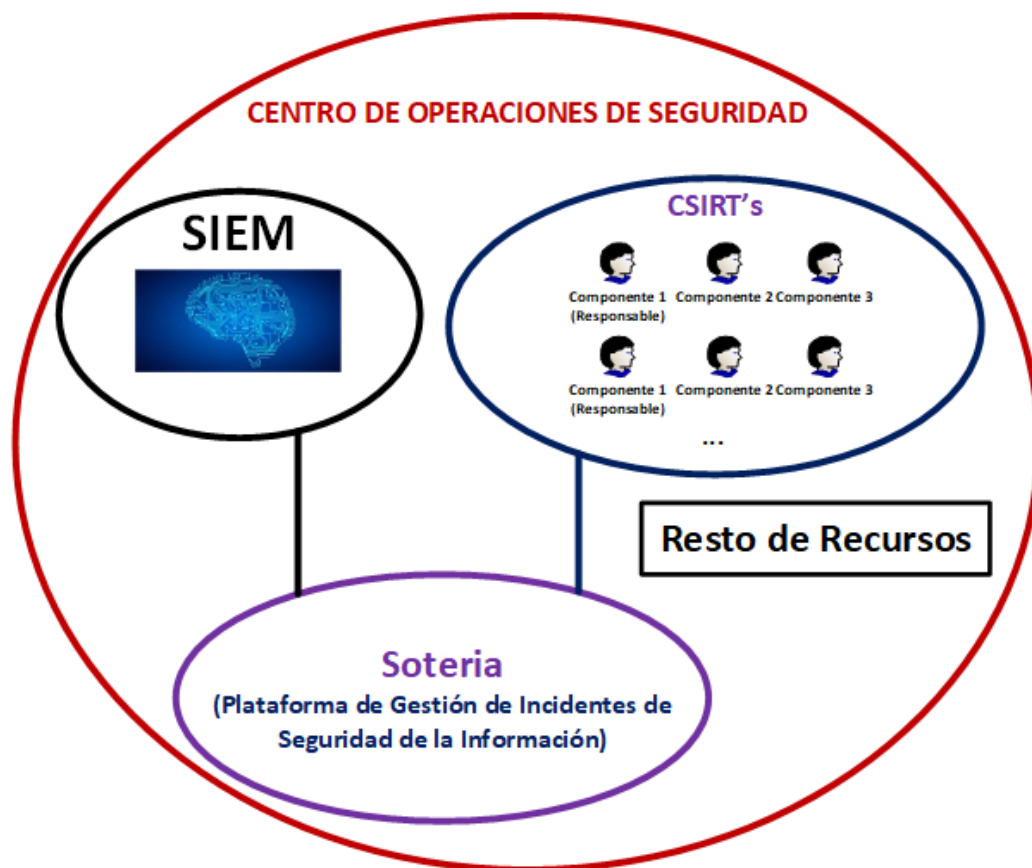


Figura 2-1. Ámbito del COS.

Como se observa, consta de cuatro (4) grandes bloques:

- Sistema SIEM: se cuenta con un sistema SIEM que aporta gran valor al proceso de detección de amenazas. De cara al presente trabajo, este bloque se simulará. En el apartado 3.5.2 *Tareas automatizadas* se expone cómo dar solución a ello.
- Equipos de Respuesta (CSIRT's): se cuenta con personal responsable de seguridad formado y preparado para conformar Equipos de Respuesta ante las situaciones más críticas, o aquellos momentos fuera del horario de trabajo donde se requiere atender una incidencia de elevada severidad a la mayor brevedad posible. Habrá que plantearse cómo organizar los Equipos de Respuesta y cómo poder gestionarlos desde la plataforma.
- Plataforma Soteria: constituye el núcleo fundamental del COS, y el motivo para el desarrollo del presente trabajo. Su función principal es integrar la gestión de los distintos aspectos que se pudieran presentar en el quehacer diario de un COS, centrándose en el ámbito de la Seguridad de la Información y, más concretamente, en la gestión de incidencias de Seguridad de la Información.
Tiene una fuerte vinculación con los dos bloques anteriores. Por un lado, recoge la información aportada por el SIEM en materia de detección de nuevas amenazas potenciales. Por otro lado, permite la gestión y control de los Equipos de Respuesta.
- Resto de recursos: recoge todos aquellos sistemas y recursos que apoyan al COS para su normal desempeño. Dentro de este bloque, se tiene pensado implementar también la gestión del personal responsable de Seguridad de la Información. No se cubrirá la gestión de todo el personal que pueda prestar sus servicios al COS, se limitará al personal mencionado. Por otro lado, la gestión está enfocada a garantizar el buen funcionamiento de la plataforma, no está pensada como una gestión integral del personal, se trata de una gestión operativa, no administrativa.

A través de los siguientes subapartados se exponen los aspectos principales relacionados con las tecnologías, metodologías y soluciones planteadas, que servirán de base para poder desarrollar la plataforma Soteria.

2.3.1 Sistema SIEM

En el contexto de un COS, el empleo de un sistema SIEM ayuda a mejorar la capacidad de detección de nuevas incidencias, así como hacer más fácil la tarea de análisis al personal responsable de Seguridad de la Información. Como se introdujo en el apartado *1 Introducción y objetivos* del presente documento, contar con un sistema de estas características libera al personal de realizar las tareas más tediosas, como es el caso del análisis de los registros de eventos en los sistemas. Por otro lado, incrementa notablemente la calidad en la detección, lo que permite reducir el nivel de exposición a las amenazas. De cara al presente trabajo, el sistema SIEM será una caja negra simulada. Se supondrá que, en base al motor de detección que posea, las reglas configuradas y las capacidades que albergue, podrá ofrecer la detección de incidencias en el formato que se le indique. Los datos necesarios para configurar una nueva incidencia se tratarán en el siguiente apartado. Este subapartado se enfocará en lo que puede ofrecer el SIEM y la relación que tendrá con la plataforma Soteria en su conjunto.

Como se vio en el apartado introductorio, la finalidad del sistema SIEM es correlar la detección de diversos eventos en búsqueda de posibles amenazas. El resultado que ofrece su motor de correlación se transforma finalmente en un informe. Como también se introdujo, hubiera sido también muy interesante haber desarrollado la segunda línea de trabajo, enfocada al desarrollo de un sistema SIEM propio, con interfaz capaz de ofrecer la información según se configure. De cara al presente trabajo, se considerará que se cuenta con dicha funcionalidad, de tal manera que, configurado convenientemente, una vez detectado un evento que podría considerarse como una amenaza, el sistema SIEM es capaz de ofrecer los datos necesarios para generar de manera automática una nueva incidencia. El proceso sería el siguiente:

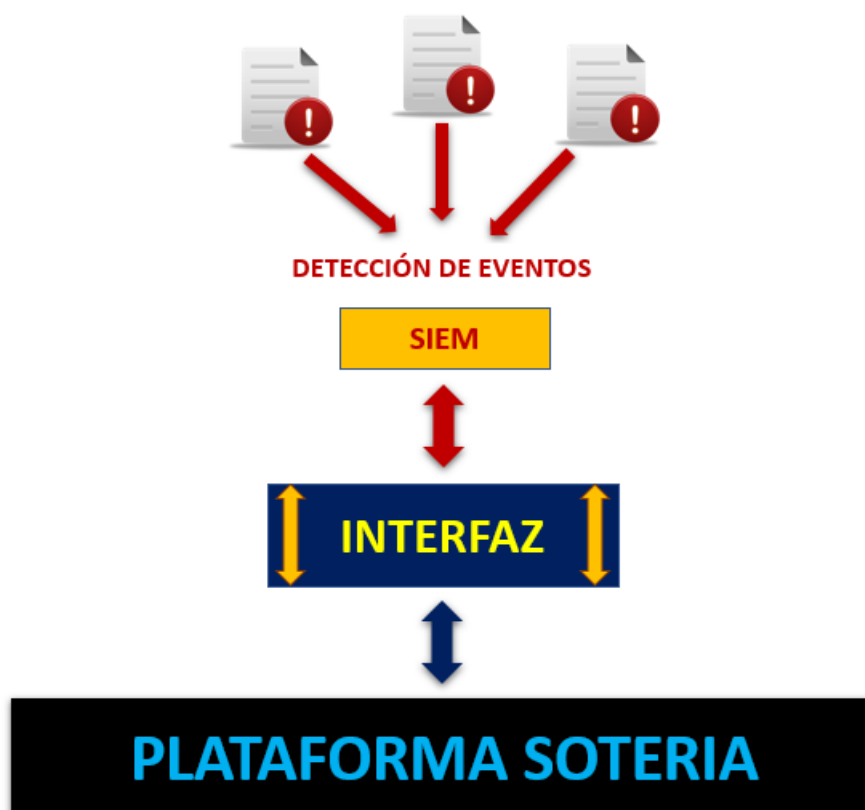


Figura 2-2. Interfaz SIEM ↔ Soteria.

Si se observa la figura anterior, la interfaz entre el sistema SIEM y la plataforma Soteria se ha indicado como bidireccional. En este caso se hace necesario porque el sistema SIEM no se limitará a detectar incidencias y notificarlas, sino que será capaz de tener acceso a información de la plataforma Soteria para generar una nueva incidencia. Esto supondría un gran avance en el sentido de que, desde el momento en que el SIEM detecta una nueva amenaza y la transforma en incidencia, se puede gestionar desde Soteria o, lo que es lo mismo, se puede atender. No es un detalle menor, pues significa que la incidencia desde ese primer momento está integrada de pleno en Soteria y se puede aplicar sobre ella toda la funcionalidad disponible en la plataforma para su atención.

Para salvar los posibles inconvenientes que puedan acarrear los falsos positivos en la detección de las amenazas, las incidencias que se generen desde el sistema SIEM no lo hacen en estado activo directamente, sino que se mantienen en estado de *Cuarentena* hasta ser atendidas por personal responsable de Seguridad de la Información. Una vez el analista compruebe los datos, los indicios detectados en el sistema SIEM y los condicionantes necesarios, puede decidir que se trata de una amenaza real y pasarla al estado *Activa*, o bien marcarla como falso positivo, anotar las consideraciones necesarias en el campo de detalles y cerrarla.

En el caso de los falsos negativos, por definición, se tratará de aquellas amenazas que el sistema SIEM no haya sido capaz de identificar. Por tanto, no se puede delegar la detección de amenazas en su totalidad al sistema SIEM, se requiere que exista un trabajo de análisis por parte del personal responsable de Seguridad de la Información para intentar detectar esos casos.

Para que este esquema funcione, se requieren dos condiciones:

- Datos: el sistema SIEM debe ser capaz de ofrecer el informe de detección en forma de datos que coincidan con el conjunto de información mínima para generar una nueva incidencia en la plataforma Soteria. Esta parte no es negociable, en el sentido de que si no se ofrecen unos datos mínimos (se verá en el siguiente apartado), no se podrá contar con el alta de la incidencia, sólo con el aviso. Por tanto, hasta que los datos no sean procesados por personal de seguridad para dar de alta la incidencia, no se podría gestionar a través de Soteria.
- Acceso a los recursos de Soteria: tal como se exponía unas líneas más arriba, el sistema SIEM debe ser capaz de acceder a cierta información de la plataforma para poder generar el alta de una nueva incidencia. En concreto, necesita detalles tales como información sobre el personal responsable de Seguridad de la Información, información que relacione el tipo de incidente detectado con las posibles medidas de protección aplicables (otro de los pilares fundamentales de este trabajo), o información para poder numerar e identificar de manera unívoca la nueva incidencia, por ejemplo.

Cumplir con estos dos condicionantes significa que el sistema SIEM está integrado de pleno en la plataforma. De hecho, así es como se ha intentado reflejar desde un primer momento, desde el momento de diseñarse el esquema de la Figura 1-10 y su conexión con Soteria.

La dificultad para el sistema SIEM en su interconexión con Soteria estriba, por un lado, en ser capaz de ofrecer la información relacionada con la posible amenaza detectada de manera que pueda servir para generar una nueva incidencia y pueda ser atendida desde su creación. Por otro lado, debe de ser capaz de comunicarse con Soteria y obtener los datos necesarios para completar y registrar el alta de una nueva incidencia. Existen dos aproximaciones posibles, dependiendo de la responsabilidad que se quiera otorgar al sistema SIEM:

- Alta de la Incidencia en Soteria: en este escenario se podría desarrollar un script* de sistema que automatice la recogida de datos y, una vez dentro de Soteria, es la propia plataforma la encargada de generar el alta de la incidencia. En este caso el sistema SIEM se limitaría a depositar en la plataforma unos datos mínimos relacionados con el nuevo evento

detectado, y sería la plataforma Soteria la responsable de recoger dichos datos, completar la información y registrar el alta de la nueva incidencia.

Gráficamente el esquema de actuación podría ser de la siguiente manera:

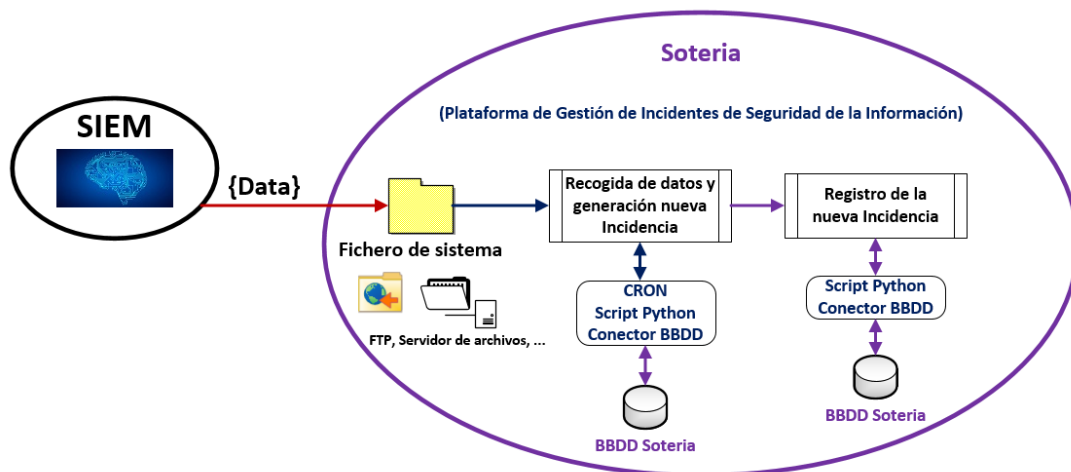


Figura 2-3. Relación SIEM-Soteria: aproximación 1ª.

Como se puede observar en la figura, el sistema SIEM podría depositar los datos *{Data}* relativos al nuevo evento detectado en una carpeta del sistema de Soteria, mediante distintas tecnologías como puede ser un servidor FTP*, un servidor de archivos o un sistema de repositorio. En realidad, los datos que proporciona el SIEM tienen una estructura relativamente simple y de poco volumen, por lo que se podría utilizar cualquier sistema simple de transferencia de información.

Una vez la información se encuentre en el fichero de sistema, mediante un script Python que se ejecuta de manera periódica gracias al gestor de tareas automatizadas CRON de Linux, se comprueba si existen nuevos datos procedentes del sistema SIEM. En caso afirmativo, el proceso de generación se conecta a la BBDD de Soteria para completar la información necesaria. Una vez se tiene completa la información, mediante el proceso de registro se inserta la nueva incidencia en la BBDD de la plataforma. Los procesos de recogida de información, generación de nueva incidencia y registro de la misma se pueden desarrollar a través del mismo script Python.

La parte importante de este esquema que merece la pena destacar, es el hecho de que **es la propia plataforma Soteria la que se conecta con su BBDD y gestiona realmente el alta de la incidencia. El sistema SIEM se limita a depositar un listado de datos mínimos sobre el evento detectado.**

- Alta de la Incidencia desde el propio sistema SIEM: en este caso el procesado del sistema SIEM incluiría, además lógicamente de la detección del evento que haya concluido puede suponer una amenaza, el acceso a la plataforma Soteria, recogida de datos para completar el alta y registro de la nueva incidencia en la plataforma por el propio sistema SIEM. Como se observa, en esta aproximación **el sistema SIEM cuenta con mayor margen de actuación en Soteria**. Tal vez, de implementarse correctamente, quizá sea la opción más potente, pues le ofrece al sistema SIEM la posibilidad de mejorar su base de conocimiento y experiencia, de mejorar con ello su capacidad de detección (normalmente basado en aprendizaje automático), lo cual redundaría en definitiva en ofrecer un mejor nivel de seguridad. No obstante, significa también mayor complejidad, además del hecho de diseñar e implementar funcionalidades que, en principio, no están previstas en un sistema de estas características. Gráficamente esta aproximación podría esquematizarse de la siguiente manera:

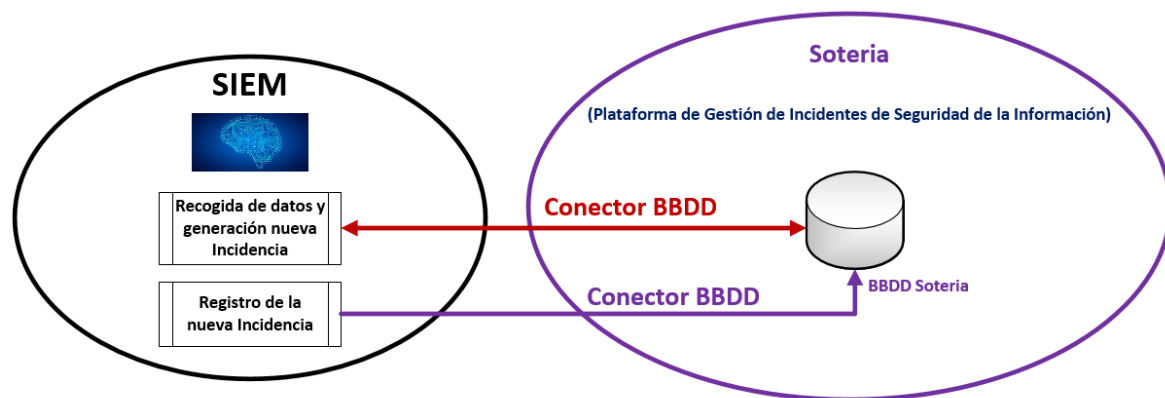


Figura 2-4. Relación SIEM-Soteria: aproximación 2ª.

Como se observa en esta segunda aproximación, la funcionalidad del sistema SIEM queda extendida en mayor magnitud, liberando con ello a Soteria de los procesos de recopilación de datos y generación de nuevas incidencias procedentes del sistema SIEM, así como ahorrando el tener que desarrollar un script y su automatización. El sistema SIEM en este caso debe ser capaz de conectarse a la BBDD de Soteria, completar los datos que pudiera requerir y ejecutar el registro del alta de la nueva incidencia.

De nuevo, se ha separado en dos procesos, pero se puede fundir en un único proceso en el sistema SIEM que desarrolle toda esta funcionalidad, así como un único conector.

En ambas aproximaciones, el conector con la BBDD puede ser de tipo programático.

En el siguiente subapartado se exponen el conjunto de recursos elegidos para el diseño e implementación de la plataforma Soteria, incluidos los aspectos relativos a la BBDD.

De cara al presente trabajo y como se introducía, el sistema SIEM será una caja negra simulada en el que se dará por hecho que es capaz de generar y registrar de manera automática nuevas incidencias. En el apartado 3 *Desarrollo del TFM* se expondrán las características del script Python desarrollado para generar datos de prueba, mediante el que se creará una determinada proporción de incidencias con origen en el sistema SIEM. Por otro lado, también se simula la inserción de nuevas incidencias originadas por el SIEM con cierta periodicidad, mediante el desarrollo de un segundo script Python y su programación a través del gestor de tareas automáticas de Linux. También se tratará en el apartado 3.

En lo sustancial, de cara a la funcionalidad de Soteria, el hecho de contar con un sistema SIEM será transparente.

2.3.2 Equipos de Respuesta (CSIRT)

Contar con Equipos de Respuesta empieza a hacerse muy popular, incluso necesario para las grandes corporaciones. Como se argumentó en el apartado 1 *Introducción y objetivos*, supone un esfuerzo económico y organizativo importante, pero se está demostrando que ayudan en gran medida a reducir los tiempos de indisponibilidad del negocio.

La plataforma Soteria, en su ámbito de actuación en el COS de una organización, permitirá la gestión de Equipos de Respuesta de manera eficiente. Para ello tendrá en cuenta la situación del personal, y la conformación de Equipos en grupos de tres (3) componentes.

No requerirá tecnología, ni estándares específicos ya que su gestión se encontrará plenamente integrada en la plataforma, por lo que sus requisitos técnicos se incluyen de manera implícita en Soteria, y se tratarán en el subapartado correspondiente. Sólo requiere el acceso a información del personal responsable de Seguridad de la Información:

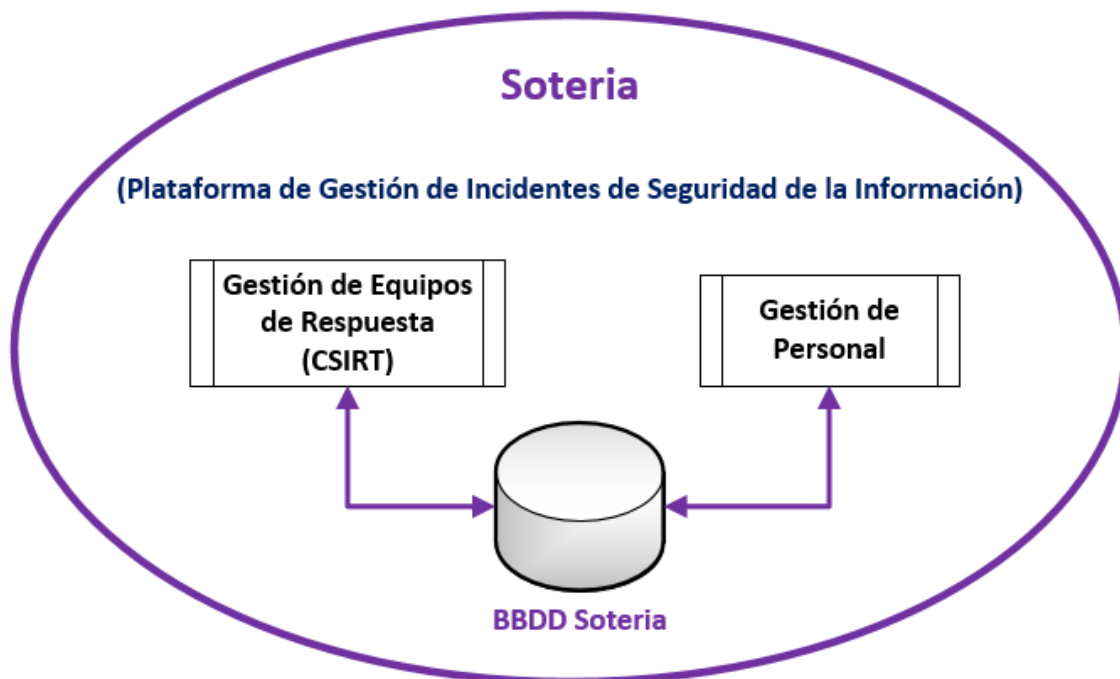


Figura 2-5. Gestión de Equipos de Respuesta (CSIRT).

2.3.3 Plataforma Soteria

Mediante este subapartado se analizan las principales tecnologías y estándares adoptados como base para el desarrollo de la plataforma. A continuación, se presentan los aspectos técnicos fundamentales que requieren estudiarse:

- Sistema anfitrión que alojará los componentes software y datos de Soteria: lo primero que se necesita es analizar y decidir cuál será el sistema anfitrión sobre el que se desplegará la plataforma.
- Servicio de páginas web: a la mayor parte de la funcionalidad que ofrece la plataforma se accede en forma de servicios web. Se precisa, por tanto, determinar qué software de servidor se empleará para ofrecer dicho servicio.
- BBDD: se requiere contar con un punto común que centralice la gestión y disposición de los principales datos que maneja la plataforma. La elección de una BBDD y un sistema de gestión de dicha BBDD será fundamental en el desempeño de Soteria.
- Lenguaje de programación del lado del servidor: se hará necesario contar con un lenguaje de programación y su plataforma de ejecución para el procesado de los datos de Soteria.
- Generación dinámica de páginas web: se requiere algún tipo de Middleware* que funcione de intermediario entre los datos generados en el servidor tras el procesado, y la visualización de las páginas web en el lado del cliente.
- Programación de tareas automáticas de apoyo: por último, se requiere también un sistema que permita el desarrollo de tareas de ejecución automática para labores de apoyo.

La elección del sistema anfitrión que albergue la plataforma vendrá determinada por los componentes software que requiera desarrollar, así como los componentes relacionados con los datos y su gestión. Debido a las características de los datos (simplicidad y poco volumen), se considerará que software y datos compartirán plataforma física. Realmente, en la actualidad la extensión de paradigmas como la Virtualización* o el Clustering* en los sistemas de servidor hace complicado que se tenga

control sobre la plataforma física sobre la que opera en realidad el software. No obstante, en esta parte no se entrará, pues es transparente para la ejecución de la plataforma. Lo relevante respecto a este trabajo es donde se desplegará y ejecutará el software.

Los Sistemas Operativos más habituales para este tipo de aplicaciones son:

-  **Linux**: se trata de un Sistema Operativo (en adelante, SO) libre, multiplataforma, multiusuario y multitarea, basado en UNIX. Se trata de una combinación de varios proyectos, entre los cuales destacan GNU (encabezado por Richard Stallman y la Free Software Foundation) y el núcleo Linux (encabezado por Linus Torvalds). Existen distribuciones tanto gratuitas como de pago. Ofrece grandes ventajas, entre ellas:
 - Existen distribuciones gratuitas, reduciendo el coste de despliegue.
 - Cuenta con numerosas herramientas y alternativas para prácticamente cualquier funcionalidad en el mundo de la computación que se pueda necesitar, por lo general de uso gratuito.
 - Se encuentra muy extendido y tiene un gran soporte internacional. De hecho, gracias al desarrollo del presente Máster los alumnos tuvieron la oportunidad de conocer la siguiente estadística:
 - El proyecto **Top500** es un ranking de las 500 supercomputadoras con mayor rendimiento del mundo, que se publica cada 6 meses.
 - Para medir el rendimiento de los sistemas se utiliza una versión portable del benchmark Linpack para ordenadores de memoria distribuida.

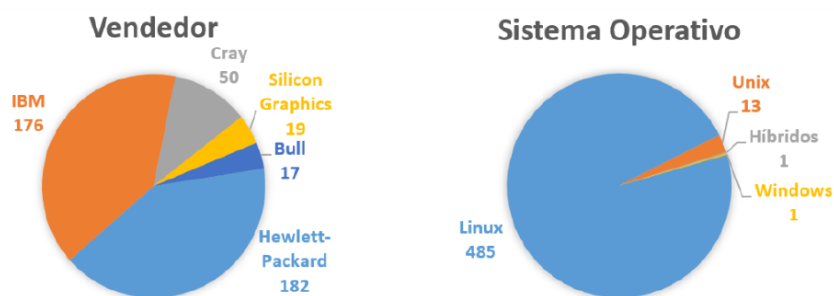


Figura 2-6. Ranking Top500 de supercomputadores.
Fuente: material docente de la asignatura INF1 – Sistemas de Computación.

Es decir, según la lista TOP500, la inmensa mayoría de supercomputadores existentes en la actualidad a nivel mundial operan sobre Sistemas Operativos Linux. Los motivos para ello no son relevantes de cara a este trabajo, ya que son ámbitos de aplicación muy distintos, pero sí resulta curioso conocer que la mayoría de supercomputadores optan por distribuciones del SO Linux.

-  **Windows**: SO de pago propiedad de la compañía estadounidense Microsoft. Ofrece distintas versiones según el ámbito de aplicación: *Home* para usuarios particulares, *Pro* para usuarios profesionales o terminales de usuario corporativos, versiones *Pro for Workstations* para aplicaciones avanzadas en terminales corporativos y versiones *Server* para aplicaciones de servidor [9]. Todas son versiones de pago. Es un SO también muy extendido en ambientes corporativos, de hecho, la mayor parte del parque informático de las AA.PP. en general, y del MINISDEF en concreto, operan sobre este SO.
-  **UNIX**: se trata de diversas variantes de SO de pago, diseñadas específicamente para sistemas de servidor, propiedad actualmente de SCO Group, si bien, la marca UNIX sigue bajo la propiedad de Novell [10]. El principal problema que plantea es que hace años que comienza

a estar en desuso. Tiene poco soporte, y el poco que ofrece suele ser de pago, con un coste económico elevado. Se descarta, por tanto, esta opción.

La duda se plantea, por tanto, entre el uso de un sistema anfitrión para la plataforma Soteria basado en SO Linux, o bien SO Windows. El hecho de contar con distribuciones gratuitas y amplio soporte ha hecho **decantar la balanza finalmente a favor de Linux**.

Respecto al servidor web que ofrezca los servicios de la plataforma Soteria a los clientes, las premisas serán las siguientes:

- Código abierto* y licencia gratuita.
- Amplio soporte.
- Debe ser capaz de soportar elevado número de peticiones simultáneas.
- Ejecutable sobre distribuciones Linux.

Con ello, las alternativas más habituales se reducen a:

-  **Apache HTTP Server**: Apache es un software de servidor web gratuito y de código abierto con el cual se ejecutan casi la mitad de los sitios web de todo el mundo. El nombre oficial es Apache HTTP Server, y es mantenido y desarrollado por la Apache Software Foundation. Presenta dos grandes ventajas: la gran extensión que muestra, consecuencia de ofrecer un elevado nivel de compatibilidad, y el amplio soporte con que cuenta. Sus características y resultados lo convierten en la opción ideal para el despliegue de todo tipo de servicios web.
- **NGINX**: servidor web ligero y de proxy reverso. Es muy estable, fácil de configurar y consume pocos recursos. Ofrece una gran potencia, siendo capaz de administrar un sitio web de elevado tráfico. Usado por Hulu, WordPress.com, la página de ventas de apps de Facebook, entre otros sitios. En la actualidad, sobre el servicio web básico de código abierto, la empresa que lo mantiene también ofrece productos y servicios de pago, relacionados con características avanzadas en el acceso a servidores web, como balanceadores de carga o caché de contenidos. Es una opción también interesante, aunque no cuenta con la compatibilidad y el soporte de Apache HTTP Server. Hay también riesgo de que la empresa de origen decida dejar de proporcionar el servidor web de manera gratuita y mediante código abierto. Sería una buena opción para organizaciones donde el coste, en caso de convertirse en una opción de pago, no suponga un inconveniente, y con elevadas necesidades de tasa de tráfico, como pueden ser los servicios de distribución de contenidos, por ejemplo.
- **Lighttpd**: se trata de un servidor web muy liviano. Representa una buena alternativa para servir contenido estático y ha ganado reconocimiento en diversas comunidades. Algunas webs que lo usan son: YouTube, Imageshack, Wikipedia, entre otras. En el caso de este trabajo no cabría aplicarse pues se precisa poder trabajar con contenido web dinámico.
- **Servidor web propio de la plataforma Flask**: realmente no debería considerarse como una alternativa, pues implementa un servicio servidor HTTP básico de relativa baja capacidad, si bien, merece la pena mencionarlo en el sentido de ser el punto de inicio para las pruebas mediante el uso de la plataforma Flask.

Por tanto, **Apache HTTP Server será el software que se encargue de dicho servicio en Soteria**.

Respecto a la gestión de la BBDD, existen diversas alternativas para dar solución al presente desarrollo. Las premisas que se establecen son:

- BBDD relacional: debido a que se trabajará con tipos de datos estructurados, la mejor opción se contar un gestor de BBDD relacionales.
- Desarrollo de código abierto y gratuito: contar con herramientas gratuitas y con acceso a los ficheros fuente del desarrollo (código abierto), **elimina el oscurantismo** de las herramientas profesionales (cerradas y de pago) **y la dependencia** de ellas para seguir operando, además de suponer un ahorro en coste económico. En el apartado 3 *Desarrollo del TFM* se muestran los detalles de diseño e implementación de todos los aspectos relacionados con la BBDD de Soteria y su gestión.
- Facilidad de integración con el resto de recursos de la plataforma: se requiere una opción fácilmente integrable con el resto de recursos. Ello incluye también contar con un buen soporte.
- Compatible con el estándar ISO/IEC 9075:2011: es decir, que implemente el estándar SQL* para la gestión de consultas sobre la BBDD.

Para analizar las alternativas, la siguiente figura muestra el ranking de sistemas de gestión de BBDD (en adelante, SGBD) relacionales más populares, actualizado a octubre de 2018:

141 systems in ranking, October 2018

Rank			DBMS	Database Model	Score		
Oct 2018	Sep 2018	Oct 2017			Oct 2018	Sep 2018	Oct 2017
1.	1.	1.	Oracle +	Relational DBMS	1319.27	+10.15	-29.54
2.	2.	2.	MySQL +	Relational DBMS	1178.12	-2.36	-120.71
3.	3.	3.	Microsoft SQL Server +	Relational DBMS	1058.33	+7.05	-151.99
4.	4.	4.	PostgreSQL +	Relational DBMS	419.39	+12.97	+46.12
5.	5.	5.	DB2 +	Relational DBMS	179.69	-1.38	-14.90
6.	6.	6.	Microsoft Access	Relational DBMS	136.80	+3.41	+7.35
7.	7.	7.	SQLite +	Relational DBMS	116.74	+1.29	+4.76
8.	8.	8.	Teradata +	Relational DBMS	78.63	+1.25	-1.45
9.	9.	↑ 11.	MariaDB +	Relational DBMS	73.13	+2.49	+16.73
10.	10.	↑ 12.	Hive +	Relational DBMS	61.10	+1.47	+9.66
11.	11.	↓ 9.	SAP Adaptive Server +	Relational DBMS	58.57	+0.52	-8.67
12.	12.	↓ 10.	FileMaker	Relational DBMS	56.04	+0.74	-5.02
13.	13.	13.	SAP HANA +	Relational DBMS	54.37	+1.64	+4.28
14.	14.	↑ 16.	Microsoft Azure SQL Database +	Relational DBMS	26.27	+1.02	+4.42
15.	15.	↓ 14.	Informix	Relational DBMS	26.24	+1.33	-1.66

Figura 2-7. Sistemas de Gestión de BBDD más populares.

Fuente: <https://db-engines.com/en/ranking/relational+dbms>

De los principales SGBD expuestos, aquellos que cumplen las premisas son (fuentes en [11]):

- PostgreSQL: el problema que plantea es que es relativamente lento en inserciones y actualizaciones en bases de datos pequeñas, PostgreSQL está diseñado para ambientes de alto volumen. En comparación con MySQL es más lento en inserciones y actualizaciones, ya que cuenta con cabeceras de intersección que no tiene MySQL. Consume más recursos que MySQL. La sintaxis de algunos de sus comandos o sentencias puede llegar a no ser intuitiva si no tienes un nivel medio de conocimientos en lenguaje SQL.
- SQLite: a diferencia del resto de sus competidores, SQLite no emplea una arquitectura Cliente/Servidor. En lugar de ello, la biblioteca SQLite se enlaza con el programa pasando a ser parte integral del mismo. El programa utiliza la funcionalidad de SQLite a través de llamadas simples a subrutinas y funciones. Esto reduce la latencia en el acceso a la base de

datos, debido a que las llamadas a funciones son más eficientes que la comunicación entre procesos. El conjunto de la base de datos es guardado como un sólo fichero estándar en la máquina host. Presenta limitaciones en la cláusula *WHERE* de cara a consultas anidadas. Además, adolece de la falta de claves foráneas cuando se realiza la creación de la tabla desde el modo consola.

-  **MariaDB**: se considera como una escisión (fork) de MySQL. Nace como una alternativa libre a MySQL tras la compra de ésta por Oracle. El objetivo es mantener un base de datos libre, garantizando la licencia GPL. Para ello, con cada nueva versión de MySQL, aparece una nueva de MariaDB, incluyendo sus avances. Introduce dos motores de almacenamiento nuevos, uno llamado Aria —que reemplaza a MyISAM— y otro llamado XtraDB —en sustitución de InnoDB—. Tiene una alta compatibilidad con MySQL ya que posee las mismas órdenes, interfaces, API y bibliotecas, siendo su objetivo poder cambiar un servidor por otro directamente. En todos los foros y fuentes consultadas, parece ser que la única desventaja que puede tener es el hecho de realizar la migración de MySQL a MariaDB, y la compatibilidad 100% una vez completada la migración.

Una vez expuestas las características de los principales SGBD aplicables, se concluye que **MariaDB es la mejor opción**.

Como lenguaje para cubrir la parte programática del servidor se ha elegido **Python**, ya que ofrece la posibilidad tanto de cubrir los aspectos relacionados con la generación dinámica de páginas web y su procesamiento, **como del procesamiento de tareas del sistema en general**. Se trata de un lenguaje de programación de propósito general, multiplataforma y multiparadigma. Ofrece simpleza, legibilidad y similitud con el idioma inglés, lo cual facilita el desarrollo y la posterior interpretación del código. Al ser un lenguaje multiplataforma, reduce los posibles problemas de utilizar una plataforma u otra. Cuenta además con suficiente soporte, documentación y una gran comunidad en Internet que apoya su uso. Ello facilita las tareas de desarrollo y de mantenimiento. Al igual que ocurría con el gestor de BBDD, Python también es un lenguaje de programación de código abierto. El posible inconveniente que presenta este lenguaje es que, al ser interpretado, puede ofrecer un rendimiento inferior a lenguajes compilados, por lo que pueden existir implementaciones más eficientes de cara al procesamiento en el lado del servidor. En realidad, la apreciación de la eficiencia requeriría poder comparar sistemas que procesen gran cantidad de peticiones de usuario y manejen grandes volúmenes de datos. De cara al presente trabajo, debido a sus características y funcionalidad, las peticiones simultáneas, en el peor de casos, se podrían contar por decenas de ellas. Ello se produciría en un escenario donde Soteria se despliegue sobre una organización de grandes dimensiones, que cuente con un número elevado de personal responsable de Seguridad de la Información. Aun así, manejar decenas de peticiones simultáneas, teniendo en cuenta las capacidades de los servidores actuales, incluidos los más modestos, no debería plantear problemas de eficiencia, por lo que seguramente no sería apreciable. Por otro lado, el tipo y volumen de datos que maneja Soteria tampoco debería ser un factor problemático que suponga una pérdida de eficiencia apreciable.

Su competidor más directo y alternativa principal en el desarrollo de servicios web, como lenguaje de programación interpretado, habría que considerar a PHP: acrónimo recursivo en inglés de PHP Hypertext Preprocessor (preprocesador de hipertexto), es un lenguaje de programación de propósito general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. Fue creado originalmente por el programador canadiense Rasmus Lerdorf, en el año 1995. Nunca pretendió ser un lenguaje de programación, sino que fue creado con la intención de contar con un conjunto de herramientas para el mantenimiento de las páginas web. PHP ha evolucionado por lo que ahora incluye también una interfaz de línea de comandos que puede ser usada en aplicaciones gráficas independientes. Puede ser usado en la mayoría de los servidores web al igual que en muchos sistemas operativos y plataformas sin ningún costo.

Otras alternativas podrían ser: Java, C#, ASP .NET, Visual Basic .NET, etcétera. En estos casos se trata de lenguajes compilados, por lo que suelen ser más eficientes, si bien, ofrecen por otro lado una complejidad mayor para la programación activa del servidor web. En algunos casos se trata de alternativas que requieren licencias de pago.

La siguiente figura muestra cómo se encuentran extendidos a nivel mundial los principales lenguajes de programación, recogidos mediante la lista TIOBE:

The TIOBE Programming Community index is an indicator of the popularity of programming languages. The index is updated once a month. The ratings are based on the number of skilled engineers world-wide, courses and third party vendors. Popular search engines such as Google, Bing, Yahoo!, Wikipedia, Amazon, YouTube and Baidu are used to calculate the ratings. It is important to note that the TIOBE index is not about the *best* programming language or the language in which *most lines of code* have been written.

The index can be used to check whether your programming skills are still up to date or to make a strategic decision about what programming language should be adopted when starting to build a new software system. The definition of the TIOBE index can be found [here](https://www.tiobe.com/tiobe-index/).

Oct 2018	Oct 2017	Change	Programming Language	Ratings	Change
1	1		Java	17.801%	+5.37%
2	2		C	15.376%	+7.00%
3	3		C++	7.593%	+2.59%
4	5	▲	Python	7.156%	+3.35%
5	8	▲	Visual Basic .NET	5.884%	+3.15%
6	4	▼	C#	3.485%	-0.37%
7	7		PHP	2.794%	+0.00%
8	6	▼	JavaScript	2.280%	-0.73%
9	-	▲	SQL	2.038%	+2.04%
10	16	▲	Swift	1.500%	-0.17%

Figura 2-8. Lista TIOBE: extensión principales lenguajes de programación. Octubre 2018.

Fuente: <https://www.tiobe.com/tiobe-index/>

Destacar, en primer lugar, el puesto que ocupa el lenguaje elegido, *Python*: 4º puesto, ascendiendo desde el 5º puesto de hace un año. Destacar también el puesto elevado del lenguaje general de consulta para el acceso a BBDD, *SQL*. Curioso también el salto en un año que ha experimentado el lenguaje *Swift*, avalado por Apple: se trata de un lenguaje de programación multiparadigma creado por Apple y enfocado al desarrollo de aplicaciones para iOS y macOS. Se sale del objetivo de este trabajo, pero es evidente que tendrá un soporte sólido.

Para no correr el riesgo de encasillarse y ajustarse tan sólo a una lista, se ofrecen a continuación un par de listas más donde Python sale incluso mejor posicionado. La primera viene de la mano de IEEE Spectrum [12], la revista y sitio oficial de la organización IEEE, la cual publica la aparición de una aplicación que permite determinar, según se configuren distintos parámetros, la popularidad de los lenguajes de programación más habituales. Se aclara que la lista puede tener cierta variación en función de la configuración establecida. No obstante, es curioso la lista por defecto el resultado que ofrece:

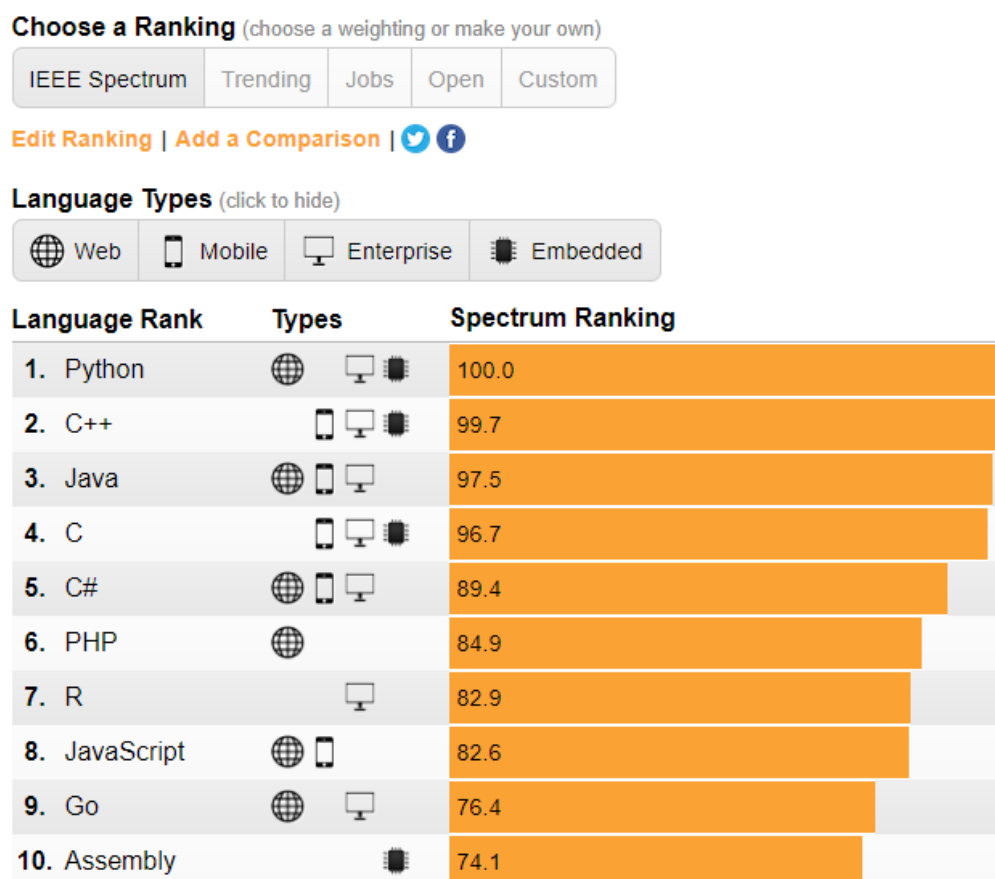


Figura 2-9. Ranking de lenguajes de programación para diversos criterios.

Fuente: <https://spectrum.ieee.org/static/interactive-the-top-programming-languages-2018>

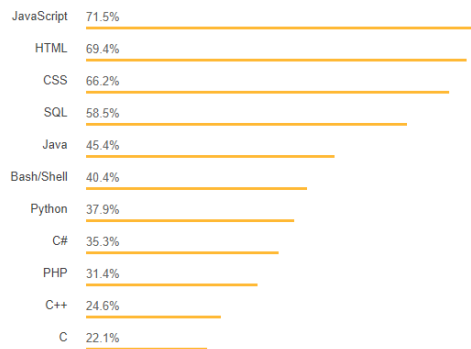
Si se observa en la parte superior de la figura, se pueden seleccionar distintos ámbitos sobre los que se han aplicado las estadísticas: IEEE Spectrum original, tendencia, puestos de trabajo y sistemas abiertos. Algunos lenguajes varían alguna posición de una configuración de estadística a otra, pero en todos los casos Python aparece en primer nivel.

Una última encuesta viene por la famosa página de apoyo al desarrollo software  **stackoverflow**, sin duda **el referente principal para todo programador**. Antes de pasar a mostrar la encuesta, el resumen global del informe indica en la presentación, y se cita textualmente: *“Python has risen in the ranks of programming languages on our survey, surpassing C# in popularity this year, much like it surpassed PHP last year.”* El informe es actual, referido a 2018. Es un informe extenso que ofrece gran cantidad de información de interés, se recomienda su lectura. Centrándose en el apartado que nos ocupa, las estadísticas sobre los lenguajes de programación más habituales, se pueden consultar diferentes figuras. A continuación, se presentan dos figuras de interés:

Programming, Scripting, and Markup Languages

All Respondents

Professional Developers



Most Loved, Dreaded, and Wanted Languages

Loved

Dreaded

Wanted

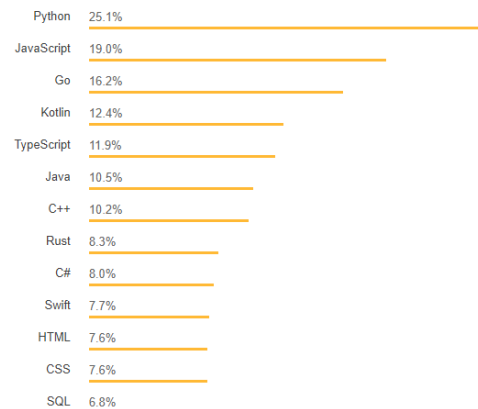


Figura 2-10. Encuestas stackoverflow sobre sistemas de desarrollo software 2018.

Fuente: <https://insights.stackoverflow.com/survey/2018/>

Por tanto, en conjunto, **sopesan más las ventajas** que ofrece el lenguaje **Python** que sus posibles inconvenientes respecto al resto de alternativas, **motivo por el cual se ha elegido** de cara a cubrir el desarrollo del presente trabajo.

El **nexo de unión entre el SGBD MariaDB y los scripts Python** que desarrollan el procesado de la parte activa del servidor será **el controlador *mysql-connector-python***.

El software para la generación dinámica de páginas web permitirá actuar como intermediario o Middleware entre la programación activa del servidor, basada en Python, y la maquetación HTML que representa la visualización final que se mostrará del lado de los clientes.

En este caso las alternativas de código abierto, gratuitas, compatibles y con amplio soporte son:

- 
Flask: se trata de un framework* escrito en Python que permite crear aplicaciones web rápidamente y con un mínimo número de líneas de código. Está basado en la especificación WSGI de Werkzeug y el motor de templates Jinja2 y tiene una licencia BSD. Ofrece buena compatibilidad con la programación en Python y su uso en el servidor web Apache HTTP Server.
- Django**: se trata de un framework de desarrollo web de código abierto, escrito en Python, que respeta el patrón de diseño conocido como Modelo–vista–template. Fue desarrollado en origen para gestionar varias páginas orientadas a noticias de la World Company de Lawrence, Kansas, y fue liberada al público bajo una licencia BSD en julio de 2005. La meta fundamental de Django es facilitar la creación de sitios web complejos. Django pone énfasis en la reutilización, la conectividad y extensibilidad de componentes y el desarrollo rápido.
- Bottle**: se trata de un framework rápido, simple y ligero de reducida capacidad, basado en WSGI* para Python. Es una versión excesivamente minimalista, ofrece poco nivel de escalado y está enfocado a proyectos de funcionalidad muy reducida.
- Existen numerosas alternativas que pueden consultarse en [13].

Del espectro de opciones propuesto, se decide finalmente por **Flask como Middleware para la generación dinámica de páginas web**.

Por último, respecto a la ejecución de tareas automáticas, se empleará, por un lado, la potencia que ofrece la programación de *scripts Python* para todo tipo de tareas del sistema, así como el **planificador de tareas automatizadas nativo de Linux: CRON**. Sin duda, es la opción más directa, sencilla y económica.

En resumen, el conjunto de recursos software para el desarrollo de la plataforma Soteria será el siguiente:

Software	Versión
Sistema Operativo <i>Ubuntu Server Linux</i>	14.04.5 LTS
Servidor Web <i>Apache HTTP Server</i>	2.4.7
Módulos <i>python-setuptools</i> y <i>libapache2-mod-wsgi</i>	40.5.0, 3.4
Gestor de BBDD <i>MariaDB</i>	10.3.10
Programación activa del servidor mediante <i>Python</i>	2.7.15
Acceso programático a la BBDD mediante <i>mysql-connector-python</i>	8.0.13
Acceso a la BBDD mediante línea de comandos mediante <i>mysql</i>	15.1
Generación dinámica de páginas web mediante <i>Flask</i>	1.0.2
Planificador de tareas mediante <i>CRON</i>	Integrado en Linux

Tabla 2-1. Recursos software necesarios.

El resto de software y herramientas adicionales que pudieran necesitarse como apoyo para el desarrollo y despliegue de la plataforma Soteria, se ha elegido siempre siguiendo los siguientes criterios:

- De código abierto.
- Gratuito.
- Compatible con el resto de componentes software.
- Debe contar con amplio soporte.

2.3.4 Resto de recursos

Como se introducía al comienzo del apartado, aquí se incluyen aquellos sistemas y recursos que apoyan al COS para su normal desempeño. En concreto, como funcionalidad adicional pero necesaria para el normal desarrollo de Soteria, se incluye la gestión del personal responsable de la Seguridad de la Información. Recordar, de nuevo, que Soteria no pretende hacer un control y gestión del personal integral a nivel administrativo, el objetivo es la gestión operativa del personal para asegurar el normal desempeño de la plataforma.

La gestión es similar a la desarrollada para los Equipos de Respuesta, con la salvedad de la diferencia en los datos que se manejan. Al igual que ocurría para la gestión de los CSIRT's, no requerirá tecnología, ni estándares específicos ya que su gestión se encontrará plenamente integrada en la plataforma, por lo que sus requisitos técnicos se incluyen de manera implícita en Soteria. La Figura 2-5 recogía el esquema lógico, tanto de la gestión de los Equipos de Respuesta, como de la gestión del personal responsable de Seguridad de la Información. El diseño e implementación de la funcionalidad se recogerán en el apartado 3 *Desarrollo del TFM*.

2.4 Datos de interés para la gestión de incidencias de Seguridad de la Información

Una vez analizadas diversas herramientas de similares características, se puede idear y establecer qué datos serán necesarios para desarrollar la funcionalidad pretendida. Para ello, se requiere partir de dos componentes: los servicios que pretende ofrecerse y el flujo de trabajo en la gestión.

Comenzando con la funcionalidad pretendida, se hace necesario un repaso de los principales objetivos:

- Recogida de incidentes de seguridad de la información, catalogación y registro.
- Gestión de Equipos de Respuesta ante Incidentes de seguridad de la información.
- Gestión de medidas de protección recogidas en la guía CCN-STIC 804.
- Gestión de personal responsable de seguridad.
- Cuadro de mandos con estadísticas y gráficas para el apoyo a la toma de decisiones.
- Consolidación de una base de datos de Errores Conocidos (Conocimiento).
- Información específica de apoyo a la gestión de la seguridad de la información.
- Acceso web seguro multiusuario.
- Cumplimiento de la normativa legal vigente.

La información relativa a Acceso web seguro multiusuario y Cumplimiento de la normativa legal vigente, se tratarán en el apartado 2.6 *Seguridad de la Información*.

Para determinar los datos necesarios en cada apartado, se reagrupan los objetivos por bloques funcionales. El primero se refiere a la **gestión de incidentes de Seguridad de la Información**, el cual engloba:

- Recogida de incidentes de seguridad de la información, catalogación y registro.
- Gestión de medidas de protección recogidas en la guía CCN-STIC 804.

Como se adelantaba unas líneas más arriba, para terminar de sentar las bases que permitan determinar qué datos se precisan, se hace necesario exponer también el flujo de trabajo para la gestión de incidencias o, lo que es lo mismo, el **ciclo de vida de las incidencias**:

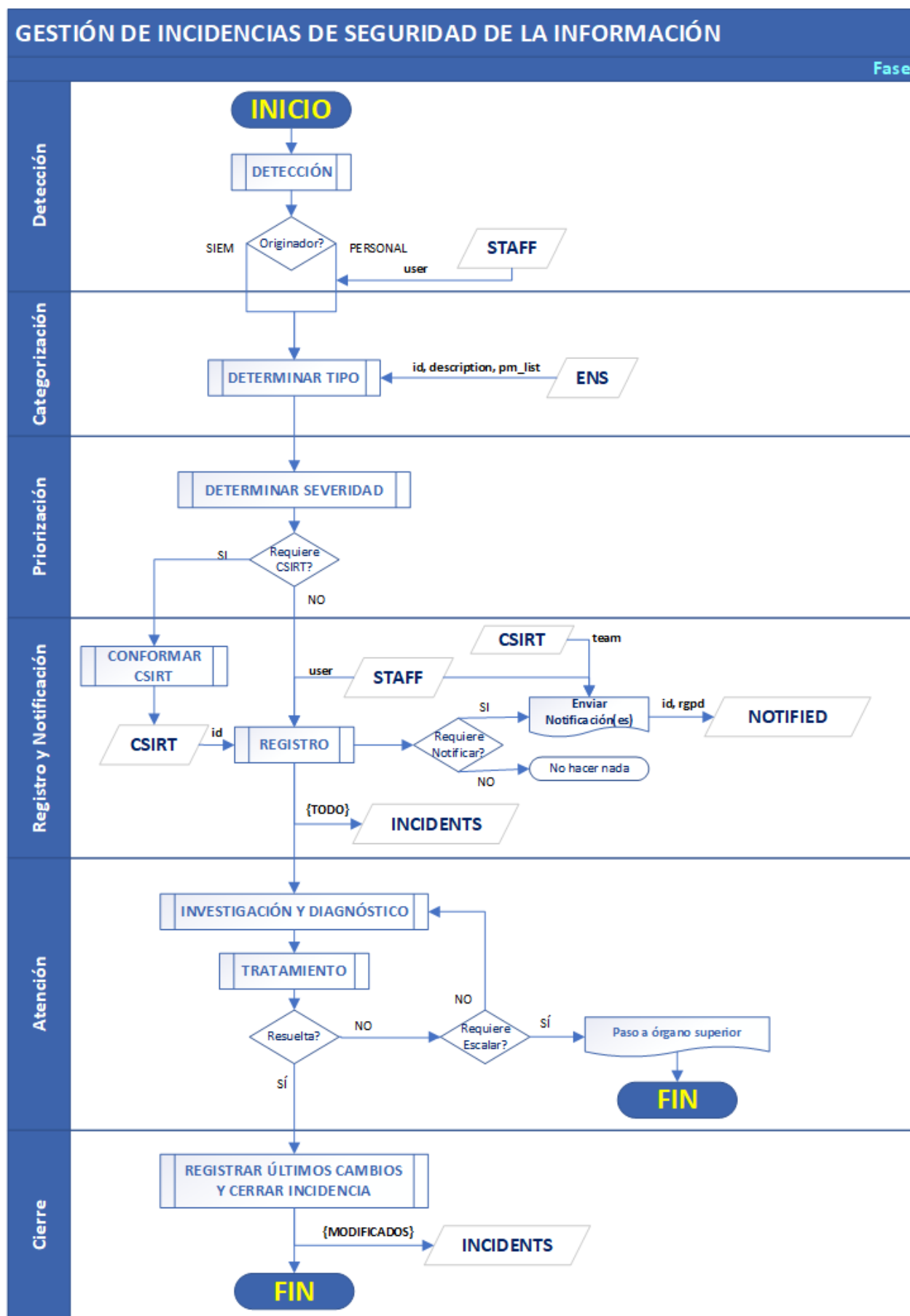


Figura 2-11. Ciclo de vida de las incidencias en Soteria.

En el caso de que, por cualquier motivo, el órgano actual que atiende la incidencia no sea capaz de encontrar una solución, se podría escalar para su atención en un órgano superior del COS. El diagrama de flujo para la atención de la incidencia en el órgano superior sería idéntico:

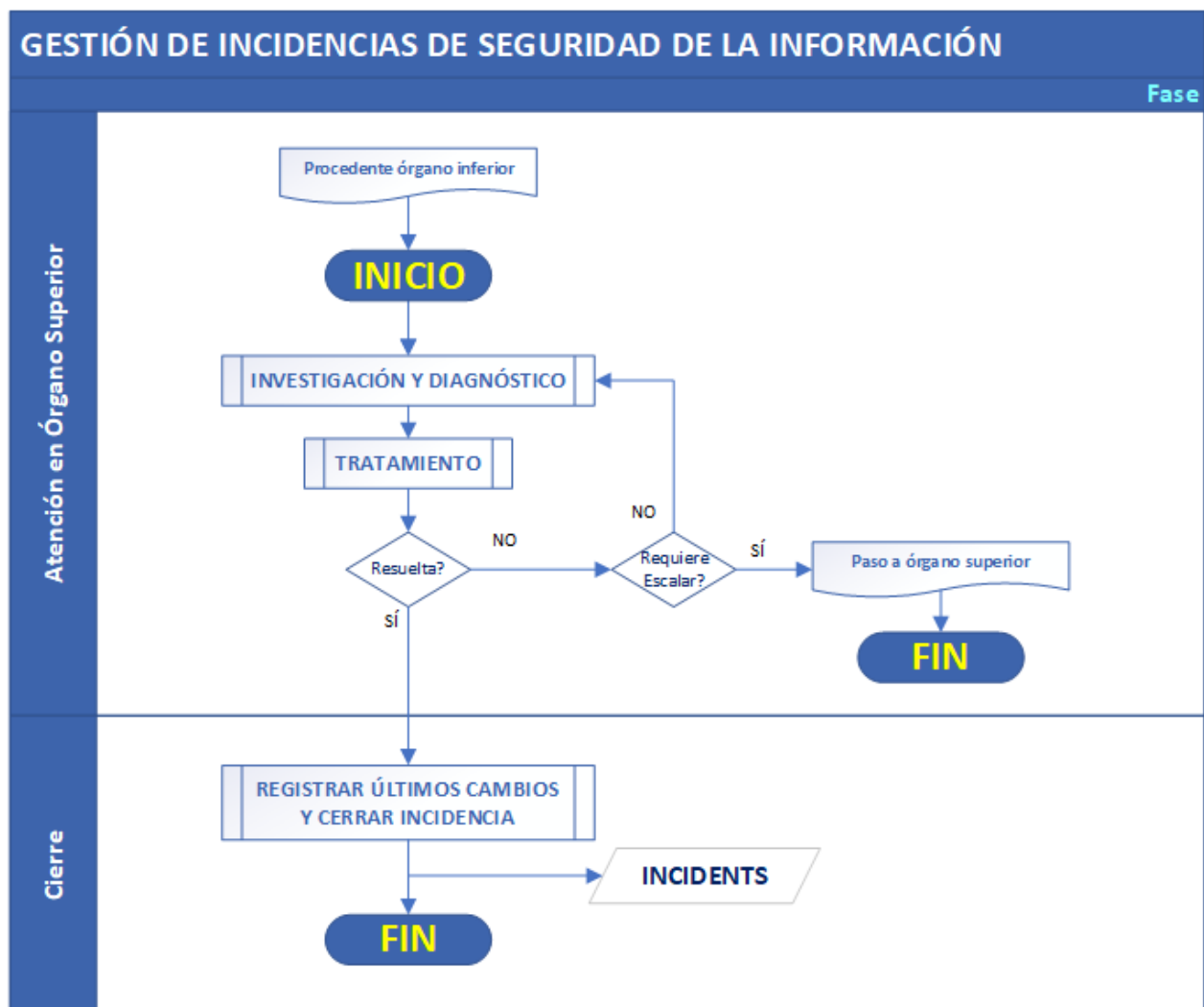


Figura 2-12. Atención de la incidencia en órgano superior.

Si se dispone de varios órganos, el proceso sería iterativo, escalando sucesivamente. El diagrama de flujo sería idéntico en cada escalón. En el presente trabajo se considerará un (1) nivel de escalado, con notificación a un escalón superior.

La BBDD sería común, ya que la incidencia y los datos asociados no tendrían por qué variar, por lo que la única diferencia sería cómo se atiende en cada nivel, lo cual a su vez dependerá de los recursos y capacidad con que cuente cada nivel. Por tanto, la plataforma en su conjunto sería común para la gestión de la incidencia, independientemente del nivel en que se atienda. Ello ofrece ventajas como:

- Evitar duplicidades de datos.
- Evitar inconsistencia de datos entre distintos niveles.
- Ahorro en espacio de almacenamiento.
- La formación y manual de uso de la plataforma son comunes para todos los niveles y usuarios.
- Todo ello redundará en una mayor eficacia y eficiencia.

Retomando el diagrama de flujo para la gestión de incidencias (Figura 2-1), se pasa a detallar la acción en cada una de las fases, así como los datos necesarios:

- Fase 1, detección: el inicio del ciclo de vida de una incidencia se desencadena mediante su detección. Dicha detección puede originarse, o bien de manera automática por parte del sistema SIEM integrado en la plataforma, o bien por parte del personal responsable de seguridad. Este aspecto es importante porque determina quién será el originador, lo cual a su vez será útil de cara a la fase de análisis.

En el caso de que el originador sea personal responsable de seguridad, se registrará su nombre de usuario. Ello requerirá contar anteriormente con algún origen de datos con los nombres de usuario. Este origen de datos se materializará en el diseño en forma de una tabla, perteneciente a la BBDD de Soteria, denominada **STAFF**. En el apartado relativo a gestión de personal se analizará dicha tabla en detalle. El nombre de usuario se obtendrá mediante el campo **user**.

- Fase 2, categorización: en esta fase se decide y establece el tipo de incidencia, determinada a partir de la clasificación de las medidas de protección aplicables, contempladas en el ENS, en concreto, en la Guía CCN-STIC 804, de Implantación del ENS. El origen de datos se materializará a la hora del diseño en una tabla denominada **ENS** y contenida en la BBDD de Soteria. Los datos necesarios serán extraídos mediante los campos **id**, **description** y **pm_list**. El campo **id** recoge la identificación del tipo de incidencia según la mencionada guía, el campo **description** recoge una descripción rápida del tipo, mientras que el campo **pm_list** aglutina el conjunto de medidas aplicables para cada categoría (tipo).

Esta fase tiene una especial importancia en la plataforma Soteria. La selección del tipo será fundamental para la correcta gestión de la incidencia, pues marca una referencia principal de cómo debe atenderse, de a qué aspectos de la Seguridad de la Información afecta, y, sobre todo, marca las medidas de protección que aconseja aplicar el ENS. Se considerará, por tanto, un **dato fundamental que no admitirá modificación**, pues cada tipo lleva asociado las medidas de protección que le corresponden. Variar el tipo, significaría romper con la trazabilidad de la gestión de la incidencia, romper con el histórico de medidas de protección que se llevan aplicadas hasta el momento. Por tanto, no puede ser un campo modificable. Su correcta elección será un aspecto fundamental. En caso de detectarse un error en la selección del tipo, la solución en estos casos pasa por cerrar la incidencia indicando en el campo de detalles (se verá en su momento) la situación, y abrir una nueva incidencia con la selección del tipo adecuada, indicando también en el campo de detalles de esta nueva incidencia la situación, el motivo de su apertura, y hacer referencia a la incidencia que le antecede.

- Fase 3, priorización: en esta fase se decide la severidad de la incidencia, atendiendo a los diversos aspectos que se estimen adecuados: recursos comprometidos, nivel de afectación, etcétera. Habrá que decidir también si, debido a la severidad de la incidencia, hora de detección, etcétera, debiera conformarse un Equipo de Respuesta (CSIRT) o no. Las condiciones para ello se exponen en el apartado 3.3 *Diseño e implementación de la base de datos*.

- Fase 4, registro y notificación: esta fase se encarga del registro de la incidencia, así como de la notificación, si así procede.

Respecto al registro, para poder efectuarlo se requiere contar con todos los datos mínimos de partida. Parte de esos datos procederán de las tablas que alberga la BBDD de Soteria, y otra parte procederá de los datos que, o bien el usuario a través de la interfaz web, o bien el sistema SIEM, ha insertado para el alta de la nueva incidencia. En el apartado 3.3 *Diseño e implementación de la base de datos* se exponen con detalle el conjunto global de datos necesarios (descripción, tipo y cometido) para poder desarrollar la funcionalidad completa de la plataforma Soteria. Este apartado se centrará en los datos que se reflejan en la Figura 2-1.

En el caso de que se conforme un Equipo de Respuesta, mediante la tabla **CSIRT** y una vez creado el Equipo de Respuesta, se ofrecerá la identificación de dicho Equipo mediante el campo **id**.

Mediante la tabla **STAFF** se obtendrá el responsable principal de atención de la incidencia. En el apartado 3.3 *Diseño e implementación de la base de datos* se exponen los criterios de selección y modificación del personal. El usuario se obtendrá mediante el campo **user**.

Una vez se cuenten con todos los datos mínimos necesarios para el alta de una nueva incidencia, se registrará en la tabla **INCIDENTS**. La lista **{TODO}** simboliza el conjunto de datos iniciales para el alta de la nueva incidencia.

Respecto a las notificaciones, según la severidad y tipo de incidencia se requerirá notificar al responsable. Si se ha conformado un Equipo de Respuesta, la notificación se realizará a los tres (3) componentes del Equipo. Por tanto, el proceso de notificaciones requiere, o bien el código de usuario del responsable a través del campo **user** de la tabla **STAFF**, o bien el código de usuario de los tres componentes del equipo a través del campo **team** de la tabla **CSIRT**. Como resultado, además de enviar la(s) notificación(es) pertinente(s), registra en la tabla **NOTIFIED** la nueva incidencia, mediante su **id**, y si resulta de aplicación el Reglamento General de Protección de Datos comunitario (en adelante, RGPD) mediante el campo **rgpd**.

- Fase 5, atención de la incidencia: en esta fase se desarrollará la atención a la incidencia, por lo que se trabajará de manera interna con todos los campos de la incidencia registrados en la tabla **INCIDENTS**. En el caso de tener que escalar la incidencia, no requiere la transferencia de datos, pues la gestión de la incidencia y el uso de la BBDD es común a todos los niveles a través de la propia plataforma Soteria.
- Fase 6, cierre de la incidencia: por último, en la fase de cierre el operario registrará los últimos cambios, seleccionará el estado *Cerrada* y ejecutará la actualización pulsando el botón correspondiente. El último paso será volcar los últimos datos modificados y recogidos de la interfaz web al registro correspondiente de la tabla **INCIDENTS**, mediante la lista **{MODIFICADOS}**, la cual simboliza el conjunto de datos que han sufrido modificación, el resto de campos no se verán afectados. Los detalles del diseño e implementación se expondrán en el apartado 3.3 *Diseño e implementación de la base de datos*.

El segundo bloque funcional engloba los objetivos relacionados con **gestión de personal**, que incluye:

- Gestión de personal responsable de seguridad.
- Gestión de Equipos de Respuesta ante Incidentes de seguridad de la información.

Comenzando por el personal de seguridad, de cara a este trabajo se definirán y manejarán aquellos datos personales mínimos imprescindibles para poder identificar al personal y desarrollar la funcionalidad necesaria en la plataforma, a saber:

- Código de usuario: cadena breve que identifica de manera unívoca a cada usuario. Se recogerá mediante el campo **user**.
- Nombre y apellidos completos: se recogerá mediante los campos **name** y **surname**, respectivamente.
- Situación del personal: se recogerá mediante el campo **status**.
- Dirección de correo electrónico para notificaciones: se recogerá mediante el campo **email**.

Dichos campos se recogerán mediante una tabla en la BBDD de Soteria denominada **STAFF**.

Respecto a los Equipos de Respuesta, su gestión precisará los siguientes datos:

- Identificación del Equipo: se necesitará identificar cada Equipo de Respuesta de manera unívoca. Ello se realizará mediante el campo **id**.
- Identificación de la incidencia atendida: se necesitará identificar la incidencia que atiende el Equipo de Respuesta y motivo por el que fue creado. Se recogerá mediante el campo **id_incid**.

- Identificación de los componentes del Equipo de Respuesta: se necesita identificar los tres componentes del Equipo, representado mediante el campo **team**.
- Fecha de conformación: se necesita tener constancia del momento en que se originó el Equipo de Respuesta, representado mediante el campo **team_date**.

Dichos campos se recogerán mediante una tabla en la BBDD de Soteria denominada **CSIRT**.

Gráficamente, los datos necesarios quedarían así:

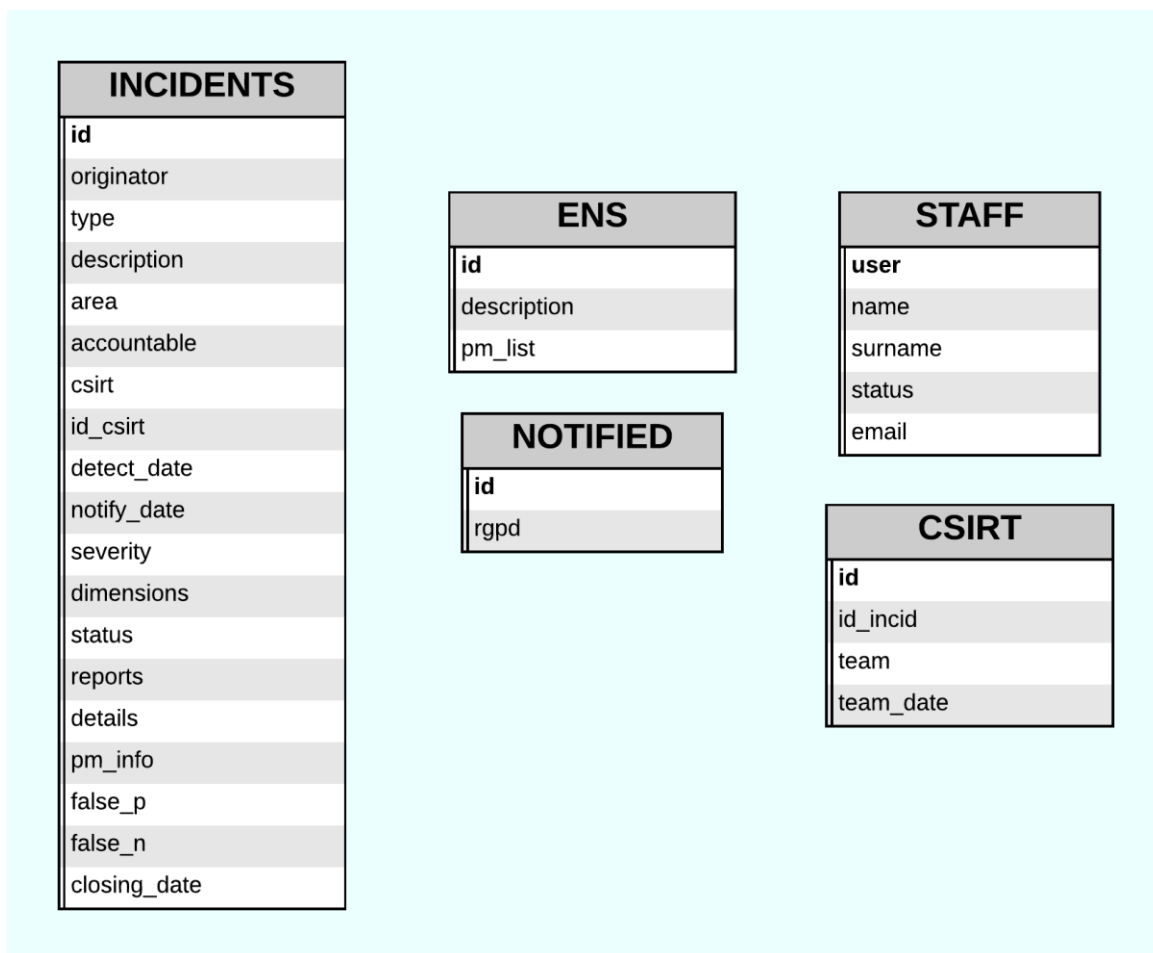


Figura 2-13. Datos de interés.

Notar que, en el caso de la tabla *INCIDENTS*, se muestran todos los datos contenidos en la lista **{TODO}** de la Figura 2-1.

El tercer bloque funcional engloba los **datos generados a partir de los ya existentes**, e incluye los siguientes objetivos:

- Cuadro de mandos con estadísticas y gráficas para el apoyo a la toma de decisiones.
- Consolidación de una base de datos de Errores Conocidos (Conocimiento).

Este bloque funcional no requiere la definición de nuevos datos ni genera nuevas tablas o campos en la BBDD de Soteria, pues su contenido se genera en tiempo de consulta a partir de la información que alberga la BBDD. Por tanto, no requiere definir nuevos datos.

Por último, el bloque funcional relativo a la **información adicional de apoyo** incluye el objetivo:

- Información específica de apoyo a la gestión de la seguridad de la información.

En este caso tampoco precisa definir nuevos datos. La información que se proporciona se refiere a enlaces a sitios en internet relacionados con la materia tratada, enlaces a revistas del sector de la Seguridad de la Información, enlaces a normativa relacionada, etc.

Con ello se completa el conjunto de datos de interés para la gestión de incidencias de Seguridad de la Información. En el apartado 3.3 *Diseño e implementación de la base de datos* se expone el conjunto global de datos necesarios y sus características.

2.5 Normativa y legislación

Debido a la importancia de los aspectos regulatorios, se hace necesario dedicarle un apartado específico, donde se ponga de manifiesto la situación actual en materia de normativa y legislación, y en qué afecta para el desarrollo del presente trabajo.

El objetivo es doble: por un lado, se trata de tener una visión global de lo que significa la Seguridad de la Información y cómo se aborda desde el punto de vista legal. Se tratarán aspectos generales de la normativa en el ámbito de la Seguridad de la Información, aspectos propios en el ámbito de las AA.PP., y aspectos concretos del MINISDEF.

Por otro lado, se hace **necesario para el cumplimiento de la normativa legal vigente**, máxime, teniendo en cuenta que el presente trabajo está enfocado a su aplicación en el ámbito de la AA.PP. en general, y en ámbito del MINISDEF en particular.

En el punto 1.1 *Introducción y contexto*, se introducían las perspectivas que engloba la Seguridad de la Información, como se puede ver en la Figura 1-3. Una de ellas era la perspectiva legal, representada por la normativa y aspectos regulatorios aplicables. De cara a este trabajo, se estudiarán dos aspectos principales que se hace necesario conocer para cumplir con la normativa legal vigente y lo que ello supondrá para diseñar, implementar y encauzar algunas tareas:

- Seguridad de la Información.
- Protección de los Datos Personales.

Empezando por el primer aspecto que marcará el desarrollo de este trabajo, **la Seguridad de la Información**, es de aplicación la siguiente normativa:

- **Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.** En su artículo 42.2 creaba el **Esquema Nacional de Seguridad**, el cual establece las condiciones necesarias de confianza en el uso de los medios electrónicos a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. Dicha Ley queda derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la seguridad de la información. Si bien, lo importante es el hecho de la creación del ENS.
- **Real Decreto 3/2010, de 8 de enero**, por el que se regula el **Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica**: desarrolla la normativa en relación a la aplicación del ENS: objetivos, ámbito de aplicación, aspectos relacionados con la gestión de la seguridad de la información, auditoría de seguridad, respuesta a incidentes, mecanismos de control, etcétera. **El ENS será un elemento central en este trabajo debido al ámbito de aplicación del mismo**

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, establece algunos preceptos de gran interés relacionados con el presente trabajo, que merece la pena enunciar:

- El artículo 14, relativo a gestión de personal, establece que, para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad. Con ello **se habilita la posibilidad de la trazabilidad del uso de los servicios y del acceso a los datos**, lo cual **permite** a su vez **la auditabilidad de los sistemas**.
- El artículo 16, relativo a la autorización y control de los accesos, establece que, el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas. La plataforma Soteria no deja de ser un sistema de información en sí misma, por lo que **se requerirá implementar un sistema de control, de tal manera que sólo se permita el acceso al personal habilitado al efecto, en este caso, el personal responsable de seguridad**.
- El artículo 24, relativo a **incidentes de seguridad**, establece lo siguiente:
 1. Se establecerá un sistema de detección y reacción frente a código dañino.
 2. Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Dicho artículo recoge precisamente la esencia del presente trabajo.

- Por último, caben destacar los artículos 29 y 36 en relación al Centro Criptológico Nacional y su papel fundamental en el ámbito de la Seguridad de la Información en las AA.PP.:
 - El artículo 29, relativo a instrucciones técnicas de seguridad y guías de seguridad, establece que, para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, **el Centro Criptológico Nacional**, en el ejercicio de sus competencias, **elaborará y difundirá las** correspondientes **guías de seguridad** de las tecnologías de la información y las comunicaciones. Esto marcará un aspecto fundamental del presente trabajo: el conjunto de medidas de protección aplicables en función del tipo de incidente detectado, regulado por la Guía CCN-STIC 804 de Implantación del ENS, en su versión de junio de 2017.
 - El artículo 36, relativo a capacidad de respuesta a incidentes de seguridad de la información, establece que:
 - El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.
 - Las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I del presente real decreto.

El artículo 36 establece dos aspectos importantes: por un lado, **atribuye al CCN la responsabilidad de actuar como centro de coordinación ante la Respuesta a Incidentes de Seguridad**. Observar que se suele utilizar el

término CERT, de origen estadounidense, en lugar del término utilizado normalmente en el seno de la UE: CSIRT (Computer Security Information Response Team). En este trabajo se utilizará el acrónimo CSIRT. Por otro lado, **establece que las AA.PP. deberán notificar al CCN aquellas incidencias de Seguridad de la Información que tengan un impacto significativo en la Seguridad de la Información manejada y en los servicios prestados.** Este segundo aspecto es muy importante de cara al presente trabajo en el sentido de que **se hace necesario establecer un sistema de notificaciones de tal manera que se pueda cumplir dicho precepto legal.** En el apartado 3.5.4 *Implementación del servicio de notificaciones*, se expone cómo se ha diseñado e implementado la solución a este aspecto.

Respecto al segundo aspecto, **la Protección de Datos Personales**, una limitación importante al acceso a la información viene dada por el deber de proteger los datos de carácter personal. En el presente trabajo, la plataforma Soteria, en sí, maneja un nivel de datos de carácter personal muy bajo, tan sólo unos datos básicos necesarios para la operatividad relacionados con el personal responsable de Seguridad de la Información que tiene acceso a la plataforma. Podría darse el caso de que, de alguna manera, algún que otro informe pudiera contener datos personales, aunque no es habitual. No obstante, según el nivel de implementación y la gestión del personal, podría haber un volumen de datos personales mayor.

Por otro lado, al margen de los datos personales relativos al personal que opera la plataforma, dependerá del ámbito donde se aplique, es decir, del sistema y los servicios **sobre los que se esté realizando la gestión de incidentes.** Suponiendo que se emplea en el ámbito de las AA.PP., sería factible que la plataforma pueda trabajar con datos personales de ciudadanos, o bien con datos personales de otros trabajadores públicos, por lo que **se hace necesario considerar la protección de datos personales y la normativa legal vigente sobre ello, a saber:**

- **Ley Orgánica 15/1999, de 13 de diciembre**, de Protección de Datos de Carácter Personal (**en adelante, LOPD**). Además de las consideraciones generales de esta normativa a tener en cuenta en lo relativo a la protección de datos personales, merece la pena destacar que gracias a ella **se establece la Agencia Española de Protección de Datos (en adelante, AEPD)** como un ente derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de la AA.PP. en el ejercicio de sus funciones, entre las cuales destaca el ser el órgano encargado de tutelar los derechos de los interesados y de tramitar, en su caso, los procedimientos sancionadores por infracciones a los preceptos de dicha Ley.
- **Real Decreto 1720/2007, de 21 de diciembre**, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO** de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Conocido de manera abreviada como **RGPD** (Reglamento General de Protección de Datos). Implica que parte de los preceptos de la LOPD y de su Reglamento de desarrollo (Real Decreto 1720/2007) queden desplazados por la nueva normativa comunitaria.
- **Real Decreto-Ley 5/2018, de 27 de julio**, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea (**en adelante, UE**) en materia de protección de datos. Lo que hace básicamente es trasponer el Reglamento de la UE de manera urgente sobre la legislación local (España) a la que pueda afectar.

El **RGPD**, al ser Reglamento, es **de aplicación directa en los países miembros de la UE**, con **entrada en vigor el pasado 25 de mayo de 2018**. Además, de toda la normativa expuesta, supone la norma de mayor jerarquía en el apartado de protección de datos personales.

Añadir que, en virtud del artículo 51.1 de dicho Reglamento, el Estado español nombra a la **AEPD** como **autoridad de control** para supervisar la aplicación del Reglamento, con el fin de proteger los derechos y libertades fundamentales de las personas físicas, en lo que respecta al tratamiento de datos personales, y de facilitar la libre circulación de datos personales en la Unión Europea. Será, por tanto, el órgano encargado de tramitar las reclamaciones y procedimientos sancionadores, así como de **recibir las notificaciones** que procedan.

El factor de mayor interés de dicho Reglamento de cara a este proyecto es el relativo a la filtración de información que afecte o pueda afectar a datos de carácter personal. En el caso de que se haya detectado una incidencia que suponga, o pueda suponer, una fuga de datos que puedan incluir datos personales, se hace necesario establecer un mecanismo de tal manera que se cumpla con el **artículo 33** de dicho Reglamento, en el sentido de comunicar la brecha de seguridad detectada a la autoridad de control competente. Para no caer en malentendidos o confusiones, a continuación, se refleja dicho artículo tal cual aparece en el RGPD:

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 27 de abril de 2016

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

(Texto pertinente a efectos del EEE)

Artículo 33

Notificación de una violación de la seguridad de los datos personales a la autoridad de control

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:
 - a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
 - b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
 - c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
 - d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.
5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Figura 2-14. RGPD: artículo 33 notificación violación seguridad personales.

Fuente: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

Para completar el apartado relativo al cumplimiento del nuevo marco normativo en el seno de la UE, se hace necesario tener en cuenta también el artículo 34, relativo a la comunicación de una violación de la seguridad de los datos personales al interesado. En dicho artículo se establece que, en el caso de que se sospeche que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento debe comunicarlo al interesado a la mayor brevedad posible. Como en el caso anterior, se reproduce tal cual aparece en el Reglamento:

Artículo 34

Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.
2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).
3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:
 - a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
 - b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
 - c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.
4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Figura 2-15. RGPD: artículo 34 comunicación al interesado.

Fuente: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

Del conjunto de normativas expuesto, hay que destacar dos en el marco legislativo actual y en el ámbito de aplicación pretendido de la plataforma Soteria:

- **Real Decreto 3/2010, de 8 de enero**, por el que **se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica**.
- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO** de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En la plataforma Soteria se tienen ambas normativas en cuenta, y, de hecho, marcarán partes fundamentales en el desarrollo de la misma.

En el ámbito concreto del MINISDEF, la información es un recurso de carácter estratégico para el Ministerio, por lo que debe garantizarse su protección, pues el cumplimiento de la misión del

MISNISDEF depende de ella. La información es un concepto abstracto e intangible que se maneja mediante elementos tangibles: personas, documentación, sistemas, instalaciones o empresas. En base a ello, se debe introducir el concepto de áreas de la Seguridad de la Información, pues uno de los objetivos del presente trabajo es cubrir todas ellas, no solo las relativas a la seguridad técnica de los sistemas. En el MINISDEF la Seguridad de la Información se divide en áreas, atendiendo al elemento tangible que hace uso de la información, ya sea elaborándola, presentándola, almacenándola, procesándola, transportándola o destruyéndola (en definitiva, manejándola).

A continuación, se enumeran y describen las características fundamentales de cada área:

- Seguridad de la Información en las Personas (SEGINFOPER): se ocupa de los requisitos exigidos a las personas con el objeto de garantizar razonablemente el correcto uso de la información por éstas, es decir, establece los requisitos a cumplir para que las personas puedan acceder a la información.
- Seguridad de la Información en los Documentos (SEGINFODOC): se ocupa de las medidas de protección aplicables a los documentos durante todo su ciclo de vida, es decir, durante su elaboración, almacenamiento, transporte o destrucción, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información que contienen.
- Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT): se ocupa de las medidas de protección aplicables en los sistemas de información y telecomunicaciones con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información que manejan.
Previamente a que un sistema comience a manejar información del Ministerio deberá estar autorizado por la autoridad facultada para ello (Acreditación de sistemas).
La autorización otorgada a un sistema le permite manejar información del Ministerio en unas determinadas condiciones de confidencialidad, integridad y disponibilidad.
- Seguridad de la Información en las Instalaciones (SEGINFOINS): se ocupa de las medidas de protección aplicables a las instalaciones con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información.
Previamente a que en una instalación se maneje información del Ministerio deberá estar autorizada por la autoridad facultada para ello.
La autorización otorgada a una instalación permite albergar recursos o manejar información del Ministerio en su interior en unas determinadas condiciones de confidencialidad, integridad y disponibilidad.
- Seguridad de la Información en poder de las Empresas (SEGINFOEMP): se ocupa de las medidas de protección dirigidas a las empresas y aplicables por ellas, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información del Ministerio manejada por éstas, como consecuencia de su participación en programas, proyectos o contratos del Ministerio.

El presente trabajo pretende cubrir incidencias de seguridad de la información que estén **relacionadas con cualquier área de las descritas**. Debido a su gran extensión y a las limitaciones que se han tenido que imponer para hacer este desarrollo viable en forma de Trabajo de Fin de Máster con una carga lectiva de 6 créditos, **la gestión de incidentes de Seguridad de la Información se circunscribirá a los enmarcados en la Guía CCN-STIC 804, de Implantación del ENS**, tal como se refleja en el apartado *1.3 Objetivos y alcance*.

En el apartado *3 Desarrollo del TFM*, se expone cómo se ha cubierto esta funcionalidad, cumpliendo la normativa legal vigente.

2.6 Seguridad de la Información

Una vez planteados los aspectos regulatorios, se muestra a continuación cómo se plasmarán en el presente trabajo, de tal manera que se respete el cumplimiento de la normativa legal vigente.

La normativa aplicable se encuentra dividida en dos partes diferentes, las cuales suponen la generación y control de funcionalidades distintas:

- Cumplimiento del ENS: en este apartado se establecerán las bases para el cumplimiento del ENS. Ello incluye dos aspectos distintos:
 - El desarrollar una plataforma de las características de las pretendidas y su aplicación en el ámbito de las AA.PP., contribuye al cumplimiento del ENS, en concreto, a cumplir con el artículo 24 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, relativo a incidentes de seguridad, el cual, como pudo comprobarse en el apartado anterior de normativa y legislación, define precisamente la esencia del presente trabajo. El desarrollo de este trabajo y su aplicación, por tanto, contribuye al cumplimiento del ENS en su conjunto.
 - Por otro lado, una de las características diferenciadoras del presente trabajo es la asociación y aplicación automática de las medidas de protección recomendadas a través de la Guía CCN-STIC 804, de Implantación del ENS. Con ello, no sólo se contribuye a cumplir con el ENS, sino que además se facilita la labor del personal responsable en el apartado de Seguridad de la Información. Este aspecto se desarrollará en el siguiente subapartado.
- Cumplimiento de la normativa comunitaria en relación al tratamiento de datos personales (nuevo RGPD en vigor desde el 25 de mayo de 2018): supone la vigilancia de brechas de seguridad en lo relativo a posibles filtraciones al exterior de datos personales albergados en los activos de la organización que se protege.

A todo ello hay que añadir uno de los objetivos principales establecidos: **acceso web seguro multiusuario**. En los siguientes subapartados se establecerán las bases para poder cubrir ambos aspectos, tanto los regulatorios como el de acceso web seguro multiusuario, de tal manera que se pueda diseñar e implementar la funcionalidad a lo largo del apartado 3 *Desarrollo del TFM*.

2.6.1 Cumplimiento del ENS.

En el ámbito de las AA.PP., la situación actual en el apartado de Seguridad de la Información viene marcado por la aplicación del ENS. Ello quiere decir que el trabajo principalmente consiste en aplicar el ENS en base a la legislación que lo desarrolla (Real Decreto 3/2010, de 8 de enero), y, llevado a la práctica, principalmente aplicar las guías y recomendaciones del CCN. Decir de antemano, y **destacar especialmente, el papel encomiable del CCN en esta materia**. Las personas que tenemos relación con el CCN y estamos suscritos a sus servicios, no podemos hacer otra cosa que aplaudir su esfuerzo y su obra. Dicho todo esto, el problema principal que se plantea es la gran extensión de las AA.PP. Cuando un operario público relacionado con la Seguridad de la Información se encuentra ante un problema, aunque se disponga de guías de gran calidad, cuesta encarar un problema, especialmente si no ha ocurrido antes y no se dispone de Conocimiento previo.

Es por ello que surge la proposición de este trabajo. Al margen de contar con una plataforma que centralice la gestión de incidencias de Seguridad de la Información e integre diversos servicios relacionados, la principal motivación venía de la mano de intentar automatizar la atención de las incidencias y facilitar la labor a los operarios. En la actualidad no se conoce ninguna herramienta que permita categorizar las incidencias y asociarles, de partida, medidas de protección que les sean aplicables, lo cual facilita en gran medida la tarea y acelera el poder atender la incidencia.

Para poder implementar esta funcionalidad se diseñó la tabla ENS, con los datos que se reflejaban en la Figura 2-3, y que por comodidad se vuelve a reproducir aquí:

ENS	
id	
description	
pm_list	

Figura 2-16. Tabla ENS.

El campo **pm_list** es la **clave** que permite desarrollar la funcionalidad pretendida. Recoge el listado de medidas de protección que se consideran aplicables en función de la categorización de seguridad del sistema y las medidas propuestas en la guía CCN-STIC 804, de Implantación del ENS, en su apartado 5 de medidas de protección, para cada tipo de incidente.

Para poder trabajar con cada una de las medidas de protección por separado se hace necesario establecer algún tipo de formato que permita separar y procesar programáticamente cada medida. Para poder entender este tratamiento y cómo establecer un formato que permita el procesado programático, se hace necesario en primer lugar analizar cómo se recogen las medidas de protección en la guía CCN-STIC 804: sección 5 de medidas de protección [MP]. A continuación, se muestra un extracto de la guía CCN-STIC 804 donde se puede comprobar el formato:

5.3.2 [MP.EQ.2] BLOQUEO DE PUESTO DE TRABAJO

- 400. Se debe bloquear automáticamente el puesto de trabajo desde el que se accede a servicios o datos de nivel medio o superior al cabo de un tiempo de inactividad, que se marcará por parte de la entidad o compañía.
- 401. Se debe requerir al usuario autenticarse de nuevo para reanudar la actividad en curso.
- 402. El tiempo mencionado será parte de la configuración del equipo y no podrá ser alterado por el usuario.
- 403. Se cancelarán las sesiones abiertas tanto desde dicho puesto de trabajo como las remotas al cabo de un tiempo de inactividad (superior al bloqueo del puesto de trabajo).
- 404. El tiempo mencionado será parte de la configuración del equipo y no podrá ser alterado por el usuario.
- 405. ISO/IEC 27000
 - 27002:2013:
 - 11.2.8 - Equipo de usuario desatendido
- 406. NIST SP 800-53 rev. 4
 - [AC-11] Session Lock
 - [AC-12] Session Termination

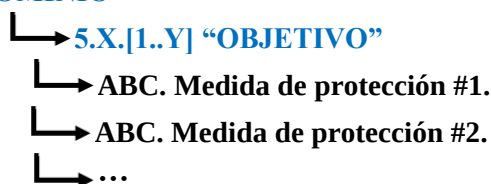
5.3.3 [MP.EQ.3] PROTECCIÓN DE EQUIPOS PORTÁTILES

- 407. Debe existir un inventario de los equipos portátiles, que identifique el equipo portátil junto a la persona responsable del mismo. Se debe verificar regularmente en el inventario que el equipo permanece bajo control del usuario al que está asignado.
- 408. Se recomienda que los equipos portátiles tengan instalado y activado un sistema de protección perimetral (cortafuegos personal) configurado para bloquear

Figura 2-17. Extracto de la guía CCN-STIC 804, de Implantación del ENS.

Es decir, se recogen las medidas de protección de la siguiente manera:

5.X “DOMINIO”



Cada código **5.X** referencia un dominio de seguridad; cada código **5.X.[1..Y]** referencia cada uno de los “Y” objetivos de seguridad con que cuenta cada dominio; mientras que **ABC** simboliza el código numérico de 3 cifras que emplea la guía CCN-STIC 804 para identificar de manera unívoca a cada medida de protección. **Este código (5.X.[1..Y]) se conservará en el modelo de datos de este trabajo** de cara a la referencia clara y directa respecto a la guía utilizada, así como para la trazabilidad de cada medida de protección. Es el dato que se recogerá mediante el campo **id** de la tabla **ENS**. Por su parte, el campo **description** recogerá el título del dominio de seguridad afectado. Y, por último, el campo **pm_list** albergará el **conjunto de medidas de protección aplicables**, según el formato que se estime conveniente para su procesamiento programático. En el apartado 3.3 *Diseño e implementación de la base de datos* se exponen los detalles del diseño e implementación establecidos.

2.6.2 Cumplimiento del RGPD.

El cumplimiento de la normativa europea en materia de protección de datos personales, tal como se reflejaba en el apartado 2.5 *Normativa y legislación*, afecta a este desarrollo en el sentido del deber de vigilar la posible exfiltración de datos personales, y la obligada notificación que ello suponga: como mínimo a la autoridad de control (AEPD) en cumplimiento del artículo 33 del RGPD, y, en el caso de que la organización estime que la filtración de datos personales puede perjudicar seriamente los derechos de los afectados, también debe notificarse a los afectados, en cumplimiento del artículo 34 del mismo Reglamento.

Ello se traduce en que, para cumplir esta normativa, se hace necesario establecer un servicio de notificaciones. Ante una necesidad de este tipo, las alternativas que existen para realizar notificaciones pueden ser:

- Correo electrónico: constituye una vía relativamente sencilla y rápida, teniendo en cuenta que hoy en día cualquiera tiene acceso instantáneo al correo electrónico a través del teléfono móvil. Si además se utilizan teléfonos corporativos, se puede considerar un medio ideal.
- Mensaje de texto al teléfono móvil mediante SMS: servicio también relativamente sencillo de implementar, aunque en su mayoría se trata de servicios de pago. Los servicios gratuitos que admiten la automatización y envío programático de SMS's a terminales móviles suelen tener muchas limitaciones, incluso no se asegura el servicio.
- Servicio de notificaciones Push: permiten mostrar mensajes de notificación en el terminal del usuario. Existen versiones específicas web Push, que utilizan los navegadores web como medio para comunicar las notificaciones. Es un servicio muy interesante.
- Servicio de llamada automática: permite ofrecer un mensaje grabado mediante llamada automática al teléfono móvil. Requiere acceso a internet y pago por uso a través de un operador de telecomunicaciones.

De cara a este trabajo, debido a que se pretende que pueda ser desplegado en redes corporativas cerradas, los servicios basados en conexión a través de Internet no son aplicables. La solución más fácil y práctica en estos casos es utilizar un servidor de correo electrónico corporativo, y realizar las notificaciones a través de dicho medio. El correo corporativo, ofrece la flexibilidad de que se puede acceder desde servicios de extranet con acceso seguro (VPN*). Eso sí, habrá que tener en cuenta que

no se pueden transmitir datos sensibles a través de correo electrónico, por lo que la notificación se limitará a avisar al personal responsable de seguridad de la existencia de una incidencia recién detectada de severidad crítica o alta. El personal responsable de seguridad deberá acceder a la plataforma Soteria para obtener más detalles sobre la misma.

En el apartado 3.2.6 *Servicio de notificaciones* se expone la motivación de dicho servicio, y en el apartado 3.5.3 *Implementación del servicio de notificaciones*, su implementación.

2.6.3 Acceso web seguro multiusuario.

Se requiere que la plataforma cuente con un acceso de estas características. A continuación, se describen las alternativas más habituales de cada característica, y cuál ha sido decisión final y porqué:

- Acceso web: la plataforma está pensada para que pueda ser accedida tanto en local como mediante acceso remoto. En horario de trabajo, el personal responsable de seguridad contará con el acceso a los recursos informáticos de la organización. Pero fuera del horario de trabajo o en casos de emergencia, es posible que el personal no disponga de acceso a recursos de las instalaciones corporativas. Contar un acceso ágil que pueda ser accedido en remoto desde cualquier terminal, ofrece una ventaja considerable. Por tanto, el desarrollo de una plataforma con clientes accediendo mediante software de escritorio limita mucho las posibilidades, como se argumentaba de hecho en el ejemplo de la herramienta LUCIA. Por tanto, la alternativa pasa por desarrollar la funcionalidad en forma de servicios web. Ello permite el acceso desde cualquier tipo de terminal, como puede ser un teléfono móvil o una tablet con capacidades de navegación web. Las tareas más pesadas correrán a cargo del servidor web que alberga la plataforma.
Una solución intermedia, como puede ser un sistema distribuido, tampoco sería recomendable, ya que supondría cargar los clientes de excesiva y responsabilidad, pudiendo provocar problemas de seguridad.
Por tanto, la plataforma Soteria se implementará en forma de plataforma web, donde los clientes accederán mediante navegadores web.
- Acceso seguro: debido al ámbito de aplicación y los datos que se manejan, se precisa que el acceso ofrezca garantías sobre la confidencialidad de los datos. Teniendo en cuenta que el aplicativo y el acceso se realiza vía web, la mejor solución en este caso pasa por emplear el protocolo seguro *HTTPS**, en lugar de *HTTP*. Para poder disponer de este acceso se precisa contar con un certificado digital de seguridad. El certificado puede ser firmado por una Autoridad de Certificación (en adelante, CA), o bien autofirmado. De cara a este trabajo y tal como se verá en el apartado 3 *Desarrollo del TFM*, se empleará un certificado proporcionado por un proveedor de servicios de internet y firmado por una CA. Ello permitirá acceder con garantías sin notificaciones de aviso en los navegadores, ya que la plataforma se cargará en una instancia *EC2** de *AWS**.
El objetivo de hacerlo de esta manera es probar que la funcionalidad se puede desplegar sin problemas en una máquina virtual de Cloud Computing* partiendo de cero y, por otro lado, ofrece la ventaja de facilitar al tutor observar el avance del trabajo progresivamente. Será útil además de cara a la defensa del Trabajo de Fin de Máster y su demostración.
De cara a un despliegue real de la plataforma Soteria y teniendo en cuenta que lo más probable es que requiera acceder en una red corporativa cerrada, la solución en este caso pasa por generar un certificado SSL autofirmado. Existen diversas herramientas para ello y gratuitas, como puede ser *openssl*, por ejemplo, o el propio *IIS**, el cual permite generarlo de manera sencilla desde su interfaz gráfica de gestión.
- Acceso multiusuario: por último, pero no menos importante, la plataforma debe ofrecer la posibilidad de acceder de manera simultánea por el distinto personal responsable de seguridad según lo necesite. El propio acceso web, por diseño, ya ofrece dicha funcionalidad.

Por otro lado, el acceso debe ser controlado y restringido, de tal manera que solamente acceda el personal autorizado, y que se pueda realizar una trazabilidad de dicho acceso y del uso de los servicios. En resumen, **se requiere un acceso autenticado**. Algunas de las alternativas para ofrecer un acceso autenticado pueden ser:

- Desarrollo de un servicio propio de autenticación: requiere diseñar e implementar un servicio propio, junto con una BBDD de control de usuarios.
- Empleo del protocolo OAuth: se trata de un estándar abierto que permite flujos simples de autorización para sitios web o aplicaciones informáticas. Permite la autorización segura de una API (Application Programming Interface) de modo estándar y simple para aplicaciones de escritorio, móviles y web [14]. Dicho de otro modo, permite emplear el sistema de autenticación de un proveedor tercero para autenticar la identidad del usuario. Por ejemplo, de implementarse, se podrían emplear las cuentas de Google+, Facebook o Twitter, por ejemplo, para que los usuarios se autenticquen en ellos. A partir de ese momento el proveedor utilizado para la autenticación compartiría información parcial de la cuenta de usuario con el sistema solicitante (token*). De esta manera el sistema solicitante podría comprobar la autenticidad del usuario.

Es un servicio de autenticación útil y relativamente sencillo de implementar, si bien está pensado más bien para otro tipo de aplicaciones, además de requerir acceso a Internet para acceder al proveedor tercero de autenticación.

- Utilizar algún sistema de autenticación mediante generación de tokens basados en tiempo, del estilo de Google Authenticator o Microsoft Authenticator. Ofrece un buen nivel de seguridad y es relativamente sencillo de implementar. Una gran ventaja que ofrece es que, una vez desplegado el servicio, no requiere tener acceso a Internet para funcionar. Debido a que la generación de los tokens (normalmente un PIN numérico de 6 dígitos) está basada en tiempo, sólo requiere que el cliente que los genera se encuentre sincronizado (corrección de la hora). A partir de ese momento, aunque el dispositivo donde se encuentre instalado el software cliente se quede sin acceso a Internet, seguirá generando nuevos tokens válidos (normalmente, cada 30 segundos).

Analizadas las posibilidades, la decisión no era sencilla. Quizá el empleo del protocolo OAuth sí fue sencillo de descartar, debido a que requería forzosamente acceso a Internet. Haciendo uso de los contenidos tratados en diversas asignaturas y del sistema de acceso a diversos servicios de banca electrónica en Internet, apareció la idea de intentar mejorar el nivel de seguridad en lo respectivo a la autenticación mediante el uso de un **sistema de factor múltiple de autenticación**. Buscando diversas alternativas que encajaran en el diseño de la plataforma Soteria, finalmente se dio con la solución de uso libre ofrecida a través de [15]. Para su funcionamiento requería instalar el servidor de Google Authenticator, para lo que se utilizó el manual accesible en [16]. Tras la instalación, configuración y algunos ajustes, se consiguió hacer funcionar el sistema de autenticación. De esta manera se cuenta con un sistema de autenticación robusto de doble factor, donde se requiere por un lado algo que el usuario conoce (usuario y contraseña) y, por otro lado, se requiere algo que el usuario posee (el PIN temporal). Tras varios meses de pruebas hay que decir que dicha solución funciona muy bien.

En el apartado 3 *Desarrollo del TFM* se exponen los detalles de instalación y puesta en marcha, así como el registro de nuevos usuarios.

3 DESARROLLO DEL TFM

3.1 Introducción y contexto del desarrollo.

Mediante el presente apartado 3, relativo al desarrollo del TFM, se detallan los pasos seguidos para el diseño e implementación de la plataforma web que dé solución a la iniciativa propuesta. Para ello, lo primero que se hace necesario es fijar y exponer los servicios que se pretende cubrir. En el punto 1.3 *Objetivos y alcance*, se exponían los aspectos que se pretende cubrir con el trabajo y aquellos que quedan fuera del ámbito del mismo. En el siguiente apartado se expondrán de manera más detallada los servicios que sí serán cubiertos por este TFM.

3.2 Servicios propuestos

3.2.1 Recogida de incidentes de seguridad de la información, catalogación y registro

La plataforma permitirá la recogida, catalogación y registro de incidentes de seguridad de la información, tanto de manera automática procedente de un sistema SIEM, como de manera manual mediante el registro llevado a cabo por el personal de seguridad responsable.

Debido a que el apartado relativo al sistema SIEM queda simulado en este trabajo, el registro se realizará en base al diseño de un servicio automático que se conecte a la BBDD *soteria* e inserte nuevas incidencias, tal como lo haría el sistema SIEM. Esto se desarrolla mediante el script Python *siem.py*, y se expondrá detalladamente en el subapartado relativo a la gestión de tareas automáticas.

El registro manual se realizará a través del servicio de gestión de incidentes de Seguridad de la Información implementado en la propia plataforma web.

3.2.2 Gestión de Equipos de Respuesta (CSIRT) y de personal

La plataforma permitirá la conformación de CSIRT's ante la detección de incidencias de categoría Crítica. La composición de un CSIRT se podrá realizar tanto de manera manual por parte del personal responsable de Seguridad de la Información, como de manera automática en la detección por parte del sistema SIEM.

Cada CSIRT estará compuesto por 3 miembros cualificados en la atención de incidencias de Seguridad de la Información, siendo uno de ellos nombrado responsable del equipo y de la incidencia (el que aparezca en primer lugar en el Equipo de Respuesta). Todos los miembros de seguridad poseen la mínima formación necesaria para abordar cualquier incidencia en el ámbito de la Seguridad de la Información, por lo que su nombramiento se realizará de manera aleatoria entre el personal que se encuentre actualmente en activo en la organización.

Por otro lado, para mantener la operatividad y la eficiencia en el desempeño de la plataforma, se realiza la gestión del personal responsable de Seguridad de la Información, en lo relativo a cambios de situación, participación en Equipos de Respuesta y altas de nuevos usuarios. Cabe aclarar e insistir en que se trata de una gestión operativa enfocada al desempeño de la plataforma, no se pretende una gestión administrativa completa del personal.

3.2.3 Cuadro de mandos con estadísticas y gráficas (Análisis)

El disponer de un cuadro de mandos ayudará a tener una mejor perspectiva global de la marcha de las incidencias, permitiendo de esta manera una mejor decisión del Mando.

Las estadísticas se generarán en base a distintos conceptos, a partir de los datos registrados en la BBDD *soteria*. Se podrán aplicar así mismo distintos periodos de observación y tipos de gráficas.

3.2.4 Gestión de Conocimiento

El registro y seguimiento de las incidencias a lo largo de todo su ciclo de vida ofrecerá los siguientes beneficios:

- Seguridad activa: reducción de la ocurrencia de incidentes.
- Seguridad pasiva: reducción del impacto de los futuros incidentes. Ello incluye reducir los tiempos de respuesta y de recuperación.
- Se reduce, por tanto, los tiempos de interrupción de los servicios, mejorando la disponibilidad de los mismos.

En el ámbito del Sector Privado, proporciona una ventaja competitiva. En el ámbito del Sector Público, mejora la experiencia de los usuarios y reduce el nivel de reclamaciones y gastos administrativos.

Mediante la conformación de una base de errores conocidos, base de Conocimiento o lecciones aprendidas, se apoyará al personal responsable de Seguridad de la Información para una mejor gestión de incidencias futuras.

La base de Conocimiento ofrecerá los siguientes servicios:

- Consulta del histórico de incidencias del mismo tipo: se ofrecerá un compendio de los campos que ofrecen información relevante de aquellas incidencias ya cerradas de un mismo tipo (clasificación ENS). De esta manera, se puede consultar de manera centralizada todo el histórico relativo a un mismo tipo de incidencia y cuáles han sido los distintos métodos y procedimientos para su resolución en ocasiones anteriores.
Se pretende que constituya un referente fundamental para el personal responsable de Seguridad de la Información.
- Control de incidencias de mayor severidad: mediante este servicio se ofrece, de manera centralizada y en una ubicación fácilmente alcanzable, la relación de incidencias de mayor severidad (Crítica y Alta) que se encuentran actualmente abiertas y que seguramente constituyan el foco principal de las acciones del personal. Desde ese punto se podrá seleccionar cualquiera de ellas y enlazar con el servicio de gestión de incidencias de Seguridad de la Información para su consulta detallada.

3.2.5 Acceso web seguro y multiusuario para personal de seguridad

La plataforma debe ser accesible en forma de servicios web para todo el personal de seguridad y directivos que se estime oportuno. Se debe ofrecer un acceso web seguro y autenticación de los usuarios. Los detalles se recogen en el apartado 3.8 *Seguridad*.

3.2.6 Servicio de notificaciones

Tal como se exponía en el punto 2.5 *Normativa y legislación*, la plataforma Soteria debe cumplir con la normativa legal vigente respecto a las siguientes regulaciones:

- Por un lado, respecto al **Real Decreto 3/2010, de 8 de enero**, por el que **se regula el Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica, debido a que el ámbito de aplicación pretendido de Soteria sea en el marco de las AA.PP., el ENS jugará un papel muy importante. De hecho, **constituye el núcleo fundamental para la clasificación de los incidentes detectados y la aplicación de las medidas de protección correspondientes**, siendo **esta funcionalidad** uno de los **objetivos principales** del presente trabajo. **Este servicio se implementa, por tanto, de manera implícita en el trabajo.**

Tal como se expuso en el apartado 2.5 *Normativa y legislación*, el artículo 36 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, establece que **las AA.PP. deberán notificar al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y en los servicios prestados.**

- Por otro lado, respecto al **REGLAMENTO (UE) 2016/679 (RGPD)**, en el caso de detectarse un incidente que suponga una violación de la seguridad de los datos personales, se hace necesario cumplir con el artículo 33 de dicho Reglamento, relativo a **notificación de una violación de la seguridad de los datos personales a la autoridad de control (AEPD)**. Al margen, lógicamente, de ser categorizada la incidencia como de severidad Crítica, e independientemente de que se conforme o no un Equipo de Respuesta (CSIRT), se requiere preparar un informe con los datos de que se disponga hasta ese momento de la incidencia detectada, y se remitirá vía electrónica al responsable de la incidencia.

En ese momento es posible que no se disponga de suficiente información y se requiera auditar los equipos, accesos, cuentas, registros de sistema, etcétera. La labor del responsable será, por tanto, notificado e informado de la situación vía correo electrónico, recopilar y completar el formulario en la mayor extensión que se pueda y en el menor tiempo posible, según los datos que se establecen en el artículo 33 del presente Reglamento, a saber:

- Describir la naturaleza de la violación de la seguridad de los datos personales.
- Categorías y número aproximado de interesados afectados.
- Categorías y número aproximado de registros de datos personales afectados.
- Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales.
- Medidas adoptadas para mitigar los posibles efectos negativos.

Una vez recopilada la mayor cantidad de información posible sobre el incidente, el responsable elevará el informe al CISO (Chief Information Security Officer ≡ Director de Seguridad de la Información), o cargo equivalente de la organización. El CISO a su vez, una vez revisado y dado el visto bueno, lo elevará al CSO* (Chief Security Officer ≡ Director de Seguridad) o cargo equivalente, el cual, revisado, lo elevará finalmente al **CEO* (Chief Executive Officer ≡ Director Ejecutivo)** o cargo equivalente, quien será el **responsable de**, una vez revisado el incidente y firmado el documento de remisión, **notificarlo a la autoridad de control, en este caso, a la AEPD.**

La normativa ofrece la posibilidad de que la información se vaya recopilando y ofreciendo a la autoridad de control de manera gradual conforme se vaya obteniendo, si bien, marca un **plazo máximo de 72 horas para la notificación. En caso de superarse dicho plazo, se deberá acompañar a la notificación la indicación de los motivos para el retraso.** Por tanto, el desarrollo debe ser lo más eficiente posible de tal manera que la notificación de la incidencia que pudiera cumplir estas características sea notificada a la mayor brevedad posible.

Gráficamente, el flujo desde que se detecta la incidencia hasta que se notifica a la autoridad de control sería el siguiente:



Figura 3-1. Escalado de la Notificación hasta remitirse a la Autoridad de Control (AEPD).

Hay que destacar dos detalles a tener en cuenta. Por un lado, se ha representado una organización genérica, donde se cuenta con un Director de Seguridad de la Información (CISO), un Director de Seguridad (CSO) y, por último, el Director Ejecutivo de la organización (CEO), y responsable del tratamiento de los datos personales que se manejan en la organización que dirige. La organización y denominación de los cargos puede variar, pero, en general, en una organización de mediana-gran entidad tendrán una jerarquía similar. Por otro lado, destacar la diferencia de la información que se ofrece a nivel técnico desde la plataforma de gestión de incidentes y desde el personal responsable de seguridad; a diferencia de la información que finalmente se remite a la autoridad de control. Como se expuso en el apartado 2.5 *Normativa y legislación*, la notificación legal que remite el

responsable del tratamiento de los datos personales incluye también detalles sobre la naturaleza de la incidencia, pero sin bajar al detalle del conjunto de información técnica de que dispondría la plataforma Soteria.

Además, **en cumplimiento del art. 34 del RGPD**, relativo a la comunicación de una violación de la seguridad de los datos personales al interesado, si se estima que la violación de la seguridad de los datos personales **puede entrañar un alto riesgo para los derechos y libertades de las personas físicas, el responsable de la organización debe comunicar el incidente a los afectados**. La secuencia sería similar a la anterior, salvando que no se requiere información técnica detallada del incidente, y de que en este caso la comunicación del CEO de la organización se produce sobre particulares. Gráficamente:



Figura 3-2. Escalado de la Notificación hasta remitirse a las personas físicas afectadas.

La información que debe incluir la notificación personal en este caso sería:

- Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales.
- Medidas adoptadas para mitigar los posibles efectos negativos.

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

- La organización ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.
- La organización ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado.
- Cuando la comunicación suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Habrà que determinar, por tanto y, en primer lugar, si procede el envío de la notificación personal.

Por tanto, se hace necesario implementar un servicio de notificaciones. Merece la pena aclarar e insistir en que la plataforma Soteria cubre la parte relativa a la notificación técnica, que sería el primer punto que desencadena la detección de la amenaza. A partir de ahí, una vez se comience a atender la incidencia por parte del personal responsable de Seguridad de la Información, se podrá empezar a recopilar la información necesaria y seguir el proceso descrito anteriormente hasta que, finalmente, el responsable de la organización pueda generar la notificación legal y remitirla al órgano correspondiente.

3.3 Diseño e implementación de la base de datos.

Una vez planteados los servicios que se pretenden cubrir con el presente trabajo, se hace necesario definir una estructura de datos que permita la gestión eficiente de dichos servicios a través de la plataforma web.

Para el diseño e implementación de la base de datos (en adelante, BBDD), teniendo en cuenta que se trabajará con datos estructurados, se seguirá el modelo relacional. Por tanto, se seguirán los siguientes pasos de diseño hasta obtener la implementación física final de la BBDD, así como la elección del sistema de gestión de bases de datos más apropiado.

3.3.1 Especificación de requisitos

En este apartado se describe en detalle qué datos hay que almacenar en la base de datos y cómo se deben utilizar, así como las características que debe incluir el sistema (prestaciones o seguridad, por ejemplo). Las características y requisitos se exponen conforme se declaran y definen los campos de datos, así como la justificación de su existencia en función de los servicios ofrecidos.

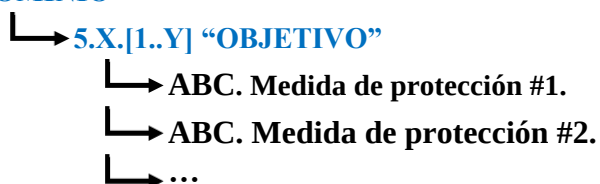
Para simplificar el diseño e implementación, evitar potenciales problemas con caracteres especiales y acortar las denominaciones, se empleará nomenclatura en inglés en la medida de lo posible, tanto en el diseño como en la codificación.

La denominación de los campos en la BBDD se referencia entre paréntesis (“*campo X*”):

- Gestión del Esquema Nacional de Seguridad (tabla ENS): se mantendrá un registro actualizado de la tipificación de los incidentes de seguridad según el marco del Esquema Nacional de Seguridad. Ello permitirá clasificar los incidentes según sus características y extraer las medidas de protección aplicables según la guía CCN-STIC 804, de Implantación del ENS. Esta tabla contendrá los siguientes campos:

- ✓ **Identificación (id):** código numérico de 3 cifras que identifica la clasificación del tipo de incidencia, en correspondencia a las medidas de protección que se consideran de aplicación según el ENS. Para su codificación se utilizará la guía mencionada, donde el campo *ENS.id* se corresponde con la numeración del Objetivo correspondiente, a partir del cual se puede acceder al desglose de medidas de protección aplicables. En subapartado relativo al campo *ENS.pm_list*, se expone la codificación empleada en la guía CCN-STIC 804 para su mejor comprensión. En resumen, el campo *ENS.id* se emplea para clasificar los tipos de incidentes que puede haber, en función de las medidas de protección aplicables, y determinadas a partir del objetivo de seguridad más acorde a la incidencia detectada. Campo numérico de 3 cifras.
- ✓ **Descripción (description):** recoge la descripción rápida (título), tal como aparece en la guía. Campo de texto alfanumérico limitado a 100 caracteres.
- ✓ **Medidas de protección (pm_list):** recoge el listado de medidas de protección que se consideran aplicables en función de la categorización de seguridad del sistema y las medidas propuestas en la citada Guía CCN-STIC 804, de Implantación del ENS, para cada tipo de incidente. Retomando el planteamiento descrito en el apartado 2.6 *Seguridad de la Información* (se recomienda repasar), se recuerda el formato que presenta dicha guía en su apartado 5 de medidas de protección:

5.X “DOMINIO”



Es decir, cada código **5.X** referencia un dominio de seguridad; cada código **5.X.[1..Y]** referencia cada uno de los “Y” objetivos de seguridad con que cuenta cada dominio; mientras que **ABC** simboliza el código numérico de 3 cifras que emplea la guía CCN-STIC 804 para identificar de manera unívoca a cada medida de protección.

Este código (5.X.[1..Y]) se conservará en el modelo de datos de este trabajo de cara a la referencia clara y directa respecto a la guía utilizada, así como para la trazabilidad de cada medida de protección. Su valor representará la categorización o tipo de incidencia.

En total y en la versión de junio 2017, dicha guía recoge: 8 Dominios de Protección, 40 Objetivos de Protección y 313 Medidas de Protección.

Debido a que esta codificación depende de la versión de la guía CCN-STIC 804 en vigor, a través del aplicativo web, **se deberá indicar la versión de la guía aplicada**, en este caso, a través de la pestaña ENS del aplicativo web, donde se puede consultar, precisamente, la guía completa en el apartado 5, tal como aparece en la misma.

Para respetar la codificación que utiliza la guía y simplificar el procesado, el contenido de cada registro *ENS.pm_list* se corresponderá con el contenido que refleja la guía para cada objetivo. Con todo ello, se seguirá el siguiente formato:

ID+Descripción OBJETIVO 5.X.Y

ID medida de protección ABC#(n). Descripción medida de protección ABC#(n)

ID medida de protección ABC#(n+1). Descripción medida de protección ABC#(n+1)
...

Como se observa, no se hace necesario separar las entradas, ya que el propio código *ID* de cada medida hace las veces de separador en caso de que se necesite procesar programáticamente. Ello nos será de gran ayuda de cara al procesado del campo *INCIDENTS.pm_info*, el cual se detalla más adelante, y del propio campo *ENS.pm_list*.

Por otro lado, para simplificar el procesado programático a la hora de la visualización de la información y hacer la navegación más rápida, se generará el campo *ENS.pm_list* conteniendo la maquetación HTML correspondiente, de tal manera que se muestre **tal como aparece en la guía**. De esta manera, a la hora de generar de manera dinámica la página web se agiliza el procesado, incrementando la eficiencia. Para la maquetación se ha empleado la codificación HTML más básica posible y con estilos autocontenidos, de tal manera que no se pueda modificar su aspecto. Gracias a ello, se garantiza que la visualización será siempre igual y acorde a como se aprecia en la Guía, evitando posibles modificaciones de estilos de manera externa que puedan generar confusión a la hora de mostrar la información y su correspondencia con el contenido de dicha Guía.

Por último, se hace necesario ofrecer suficiente espacio de almacenamiento para albergar las medidas de protección de cada objetivo. Analizada la guía CCN-STIC 804, se determina que se precisa un tamaño máximo de 7.000 caracteres (Objetivo más extenso: 5.7.4 [MP.INFO.4] *FIRMA ELECTRÓNICA*).

Campo de texto alfanumérico limitado a 7.000 caracteres.

- Gestión de incidentes (tabla *INCIDENTS*): la parte principal de la plataforma web la constituye la gestión de incidencias de seguridad de la información.

Los datos contemplados que se hacen necesarios para su correcta gestión son:

- ✓ **Identificación (id)**: código ID. Se trata de un número entero de 8 dígitos compuesto de la siguiente manera: [AAAA][NNNN], donde [AAAA] referencia al año de la detección, y [NNNN] es un número de 4 dígitos que identifica la secuencia de la incidencia dentro de ese año. Ello permite registrar hasta $10^4 = 10.000$ incidencias por año, cantidad más que suficiente.
- ✓ **Originador (originator)**: referencia a la entidad que ha registrado la incidencia: sistema SIEM en caso de detectarse de manera automática, o bien el personal responsable de Seguridad de la Información que realiza el alta de la incidencia, en el caso de registro manual. Se trata de un campo de texto limitado a 9 caracteres, conformado de la siguiente manera: si el originador es el sistema SIEM, contendrá la cadena *SIEM*, si el alta de la incidencia es manual, contendrá el nombre de usuario del personal que realiza el registro.
- ✓ **Código clasificación tipo de incidencia (type)**: representa un código numérico de 3 cifras con el que se identifica la incidencia según la clasificación del tipo de incidencia y las medidas de protección recomendadas recogidas en la guía CCN-STIC 804, de Implantación del Esquema Nacional de Seguridad.

Hay que tener presente que el objetivo principal del trabajo es disponer de un sistema de gestión capaz de categorizar la incidencia desde el punto de vista del ámbito de la Seguridad de la Información que se vea afectado, así como disponer de las correspondientes medidas de protección aplicables. Para ello, se ha seguido el ENS.

- ✓ **Descripción (description):** se trata de un campo de texto donde se describe de manera muy rápida y resumida la característica principal de la incidencia.
Ejemplo: 5.3.3 [MP.EQ.3] *PROTECCIÓN DE EQUIPOS PORTÁTILES*.
Viene determinado por la descripción de cada objetivo de seguridad que refleja la Guía CCN-STIC 804 en su apartado 5, es decir, se corresponde con el campo *ENS.description*.
Limitada a 100 caracteres.
- ✓ **Área o departamentos afectados (area):** representa el área de la organización afectada.
Campo de texto limitado a 30 caracteres.
- ✓ **Responsable (accountable):** constituye el nombramiento del personal de seguridad responsable del seguimiento de la incidencia. En el caso de que el alta de la incidencia sea manual, por defecto se reflejará como responsable la persona que ha dado de alta la incidencia (*originator*). Esta coincidencia no tiene porqué ocurrir en el 100% de los casos, por motivos como pueden ser: el ajuste logístico del personal y carga de trabajo, el personal con proximidad en las vacaciones, etc.
De cara a la generación de datasets para las pruebas, se considerará que *originator* y *accountable* coincidirán en el 80% de los casos. Por tanto, de cara a la generación de los datos de prueba, se seleccionará como responsable al mismo personal que está dando de alta la incidencia en el 80% de los casos, y se seleccionará de manera aleatoria entre el personal de seguridad en activo registrado en la tabla de personal en el 20% de los casos restantes.
En el caso de que la incidencia haya sido dada de alta como consecuencia de una detección por parte del sistema SIEM, el responsable inicial se seleccionará de manera aleatoria entre el personal de seguridad en activo registrado en la tabla de personal (*STAFF*), y la incidencia quedará en estado de cuarentena (*U*) hasta ser revisada por un analista. Si el analista valida la incidencia, deberá mantener o consignar un nuevo responsable. Ello permitirá mantener la coherencia y la trazabilidad.
Se permite la selección de otro personal responsable entre el personal en activo, tanto en tiempo de creación (manual), como en tiempo de gestión de la incidencia.
En el caso de que la incidencia sea de categoría Crítica y se conforme un CSIRT (ya sea de manera manual o automática), el responsable asignado por defecto será el usuario que aparezca en primer lugar en el Equipo de Respuesta.
Su contenido es un nombre de usuario, por tanto, limitado a 9 caracteres.
- ✓ **CSIRT asignado? (csirt):** indica si la incidencia cuenta con un equipo de respuesta asignado para su resolución.
Se asignará un equipo de respuesta en algunos de estos dos casos:
 - **Detección, alta de la incidencia y asignación de CSIRT de manera manual.**
 - **Detección automática por el sistema SIEM.**
En cualquiera de los dos casos la incidencia debe ser categorizada de severidad ‘Crítica’.
En el caso del alta manual, se deja a potestad del responsable de seguridad que genera la nueva incidencia el conformar o no un equipo de respuesta.
En el caso de la detección automática por parte del sistema SIEM y siempre que la severidad de la nueva incidencia sea ‘Crítica’, se asignará un equipo de respuesta y la incidencia quedará en estado de ‘Cuarentena’ a la espera de ser supervisada por un analista.
De tipo booleano: *Sí/No*. Por tanto, un carácter: ‘S’ / ‘N’.
Se decide utilizar un tipo de dato cadena de 1 carácter, en lugar de un tipo booleano puro, ya que permite aplicar las funciones de librería asociadas a las cadenas, lo

cual facilita el procesado programático y evita tener que realizar la conversión de tipo booleano a tipo cadena previo al procesado.

- ✓ **ID CSIRT (id_csirt):** en caso afirmativo del campo anterior (*csirt*), *id_csirt* recogerá el código que identifica al CSIRT asignado.
Por tanto, campo numérico de 6 dígitos, pues se corresponde con el campo *CSIRT.id*.
- ✓ **Fecha y hora de detección (detect_date):** indicará la fecha de detección de la incidencia. En este caso se necesita definir un formato que facilite la comparación de fechas, ya que este campo se utilizará para la búsqueda de incidencias según rango de fechas. Por tanto, se empleará el siguiente formato: *AAAAMMDDHHmm*, ya sea de tipo entero o cadena, pero teniendo la precaución de convertirlo a entero de cara a realizar comparaciones de fechas. En este caso se ha elegido de tipo cadena de 12 caracteres de longitud.
De cara a la visualización, se procesará de tal manera que se muestre en la interfaz web de manera natural a como estamos acostumbrados a leer las fechas y horas: *[DD]/[MM]/[AAAA] [HH]:[mm]*, si bien esto sólo afecta a la visualización.
Por tanto, limitado a 12 caracteres.
- ✓ **Fecha y hora de notificación (notify_date):** indicará la fecha de notificación de la incidencia (solo en el caso de ser categorizada como crítica o alta). Se empleará el formato: *[DD]/[MM]/[AAAA] [HH]:[mm]*. Por tanto, limitado a 16 caracteres.
- ✓ **Severidad (severity):** indica la categorización de la incidencia según su severidad. Se empleará la siguiente clasificación: Crítica; Alta; Media; Baja. Se tendrá cuidado a través de la interfaz web de tal manera que, si la incidencia fue categorizada con severidad Crítica y se le asignó un Equipo de Respuesta, no se puede cambiar la clasificación de su severidad.
Se registrará mediante un carácter, a saber: [C]rítica; [A]lta; [M]edia; [B]aja.
- ✓ **Dimensiones de seguridad afectadas (dimensions):** [C]onfidencialidad, [I]ntegridad, [D]isponibilidad o [A]utenticidad. Campo de texto limitado a 5 caracteres.
- ✓ **Estado (status):** según ciclo de vida de la incidencia, a saber: Abierta; Cuarentena; Cerrada. El estado de cuarentena se producirá, o bien cuando la detección proceda del SIEM y esté pendiente de estudio por un analista; o bien cuando se deje pendiente de observación, dependa de la resolución previa de otra(s) incidencia(s), de la recepción de equipamiento, de un desarrollo, etc. Los motivos de permanecer en cuarentena se deben indicar en el campo de Detalles. Se registrará mediante un carácter, a saber: [A]bierta; [C]uarentena; [C]errada.
- ✓ **Informes (reports):** si la incidencia dispone de informes se indicará aquí, con identificación de los documentos y el enlace a los mismos. Para optimizar el uso de la BBDD se seguirá el siguiente formato:

Enlace a documento #1+== +Enlace a documento #2+==...==

Es decir, el símbolo “==” se utiliza de separador entre los enlaces de cada documento y el siguiente. En este caso no se precisa un símbolo para marcar el final de la cadena, ya que con este formato se pueden extraer los datos fácilmente mediante el uso de expresiones regulares. Se debe ser cuidadoso de seleccionar los símbolos separadores de tal manera que no entren en conflicto con el contenido.

El nombre del documento se extrae del final del propio enlace: “.../nombre”.

Al margen de los informes en sí y enlaces a documentación de interés para la gestión de la incidencia, uno de los objetivos de mayor interés de este campo es el

poder incorporar acceso a los registros de actividad (logs) de sistema. Dichos registros podrían mantenerse recopilados en una base de datos documental en forma de repositorio, de tal manera que en el campo *INCIDENTS.reports* solo sea necesario incorporar el enlace.

Campo de texto limitado a 1.000 caracteres.

- ✓ **Detalles (details):** campo de texto que recogerá el histórico de la incidencia a lo largo de su ciclo de vida. Se irá rellenando de manera manual por parte del personal responsable de Seguridad de la Información, conforme se vaya realizando el tratamiento de la incidencia.

Campo de texto limitado a 3.000 caracteres.

- ✓ **Medidas de protección (pm_info):** recoge la numeración de las medidas de protección aplicables, la bandera (flag) de si se han aplicado o no, y las observaciones de cada una. Se almacenará en forma de cadena de texto con el siguiente formato:

ID Medida#1+\$\$+S/N+Observaciones#1+==+ID Medida#2+\$\$+S/N+Observaciones#2+==...

Es decir, el símbolo == se utiliza de separador entre los detalles de cada medida de protección y la siguiente. Mientras que el símbolo \$\$ se utiliza para localizar y poder separar los 3 datos de cada medida de protección. No se requiere símbolo para marcar el final de la cadena.

“ID Medida##” recoge el código de 3 cifras según las medidas de protección aplicables presentes en la guía CCN-STIC 804, de Implantación del ENS.

La extracción de la numeración de las medidas de protección aplicables se realiza mediante una consulta simple sobre el registro *ENS.pm_list* correspondiente, es decir, según el tipo de incidente (campo *INCIDENTS.type* = *ENS.id*) y, por tanto, según el objetivo de seguridad correspondiente. Una vez obtenido el listado de numeraciones de medidas de protección aplicables, se procesará de manera adecuada para mostrarlas en la interfaz web, junto con el campo de selección de aplicado o no (flag), y un campo de observaciones. **Esta manera de proceder se hace más eficiente que tratar cada medida de protección de manera independiente, y tener que consultar la tabla ENS por separado para cada una de ellas.**

El contenido en sí de las medidas de protección aplicables se puede consultar en el apartado ENS del aplicativo web, a partir de la numeración correspondiente.

Por último, se asigna suficiente espacio para albergar los campos de observaciones de cada medida de protección.

Campo de texto alfanumérico limitado a 3.000 caracteres.

- ✓ **Falso Positivo / Falso Negativo del sistema SIEM (false_p y false_n):** al disponer de un sistema SIEM, es de suponer que la mayoría de las detecciones se originarán gracias a él, ya que trabaja de manera automática e ininterrumpidamente. Habría que tener en cuenta los falsos positivos/negativos. De cara a la generación de datos de prueba y de prueba de funcionalidad de la BBDD ello no influye, pero este detalle sí se tendrá en cuenta de cara al uso real y a las estadísticas. Para ello, se permitirá a través de la interfaz web indicar esta situación:

- En el caso de que se trate de un **falso positivo**, se marcará como tal y se cerrará la incidencia. Se deja a potestad del usuario si desea aportar más detalle sobre el falso positivo en el campo de detalles antes del cierre.
- En el caso de se trate de un **falso negativo**, se marcará como tal. Si la detección se haya producido de manera automática, sería recomendable

establecer un sistema de realimentación para comunicar el incidente no detectado al equipo que gestiona el sistema SIEM. Es un factor importante y necesario de cara a mejorar la calidad de la detección. Así mismo, sería recomendable también pasar la información completa, incluidos informes si los hubiera, al cerrar la incidencia. En cualquier caso, el falso negativo quedará registrado en la tabla de incidencias para futuras consultas.

Serán factores importantes de cara a su estudio en las estadísticas y a obtener un índice de la calidad de detección del sistema SIEM.

En ambos casos el campo es de tipo booleano y formado por un carácter 'S'/'N'.

La razón para la elección de un tipo cadena de 1 carácter en lugar de un tipo booleano puro es la misma que en el caso del campo *csirt*.

- ✓ **Fecha de cierre de la incidencia (closing_date):** por último y como su propio nombre indica, este campo recogerá la fecha de cierre de la respectiva incidencia. Al igual que en el caso de *detect_date*, se dejará en formato numérico invertido (AAAAMMDDHHmm) de cara a poder realizar comparaciones de fechas, lo cual será muy útil en el apartado de Análisis. Por tanto, limitado a 12 caracteres.

- **Gestión de personal:** el ámbito de la gestión de personal en esta plataforma web tiene dos vertientes: la gestión del personal responsable de Seguridad de la Información habilitado para acceder de manera autenticada a la plataforma, y la conformación y seguimiento de Equipos de Respuesta asociados a los incidentes de mayor severidad (CSIRT's). Por tanto, se mantendrán dos tablas separadas, una para el control del personal, y otra para la conformación de Equipos de Respuesta.

La tabla con la información del personal incluye los siguientes datos (tabla *STAFF*):

- ✓ **Nombre de usuario (user):** código formado por 9 caracteres alfabéticos: 3 primeros caracteres del nombre + 3 primeros caracteres de cada uno de los apellidos.
- ✓ **Nombre (name):** limitado a 20 caracteres.
- ✓ **Apellidos (surname):** limitado a 30 caracteres.
- ✓ **Situación (status):** 1 carácter indicando: [A]ctivo, [B]aja temporal, baja [D]efinitiva o [V]acaciones.
- ✓ **Dirección de correo electrónico (email):** limitado a 64 caracteres.

La tabla con la información de los CSIRT's incluye los siguientes datos (tabla *CSIRT*):

- ✓ **ID CSIRT (id):** código numérico de 6 cifras que identifica de manera unívoca cada Equipo. Se compone de: 4 dígitos para el año de creación, y 2 dígitos restantes para el número de Equipo dentro del año en curso. Aunque el personal que lo integre pueda en algún momento volver a coincidir en un equipo, cada CSIRT es distinto y conformado explícitamente para dar solución a una incidencia concreta, de ahí que se identifique de manera unívoca, algo fundamental de cara a la trazabilidad.
- ✓ **ID incidencia (id_incid):** código de identificación de la incidencia motivo por la cual se ha conformado el Equipo.
- ✓ **Personal que integra el Equipo (team):** cadena de caracteres que recoge los nombres de usuario de los 3 integrantes del Equipo. El jefe del equipo es el que figura en primer lugar. Como el nombre de usuario es un código alfabético fijo de 9 caracteres, no se hace necesario introducir separadores entre los 3 nombres. Campo limitado a 27 caracteres alfabéticos.

- ✓ **Fecha y hora de creación (team_date):** fecha y hora de generación del CSIRT. Cadena con formato:

[DD]/[MM]/[AAAA] [HH]:[mm]

Por tanto, limitada a 16 caracteres.

- Gestión de Conocimiento: en relación a este apartado, además del registro de las incidencias, se hace necesario un registro de su resolución final. Ello permitirá mantener un conocimiento de las incidencias ocurridas con anterioridad, permitiendo reducir tanto la aparición como el impacto de nuevas incidencias potenciales. Para desarrollarlo de la manera más eficiente posible, la BBDD soteria se implementa de tal manera que pueda albergar la información de todo el ciclo de vida de las incidencias, incluida la relativa a su cierre, conclusiones y la referencia a los posibles informes finales.

Por tanto y, en resumen, la BBDD soteria será única, ya que albergará igualmente la información relativa a la gestión de Conocimiento: cierre, conclusiones finales, documentos e informes anexos, resoluciones, métodos y procedimientos aplicados, etcétera. Ello permite que se desarrollen todos los servicios necesarios a través de una única BBDD.

El servicio de gestión de Conocimiento se encuentra dividido en dos secciones:

- ✓ Incidencias por categoría: ofrece un compendio clasificado por categorías (tipo) de incidencias según la clasificación que ofrece la Guía CCN-STIC 804, de Implantación del ENS. Su objetivo es aglutinar el histórico de las medidas de protección aplicadas a lo largo de la vida de las incidencias que se encuentren ya cerradas y, por tanto, solucionado el problema que atendían. De esta manera se puede analizar caso a caso cómo se han ido aplicando las medidas de protección, cómo se han ido solucionando los inconvenientes encontrados, etcétera.

Para desarrollar esta funcionalidad el procedimiento será consultar todas aquellas incidencias que se encuentren cerradas y que sean del mismo tipo buscado. De dichas incidencias, se extraerán los campos *pm_info*, *details* y *reports*, pues son lo que ofrecen información de interés de cara a utilizarla como referencia en la resolución de nuevas incidencias.

Por último, se ordena y se maqueta HTML la información de cada incidencia para ir mostrando en forma de lista, estableciendo algún tipo de separador entre la información de una incidencia y la siguiente.

- ✓ Incidencias notificadas: ofrece el listado de incidencias contenido en la tabla NOTIFIED, es decir, la recopilación de incidencias de mayor severidad (Crítica y Alta) actualmente en activo (Abiertas o en Cuarentena). El objetivo es ofrecer un lugar donde consultar las incidencias de mayor severidad que se encuentran pendientes de resolver. Son, por tanto, las incidencias donde más se tiene que centrar el personal responsable de Seguridad de la Información en cada momento.

Para desarrollar esta funcionalidad basta con generar el listado de incidencias recogidas en la tabla INCIDENTS que coincidan con los siguientes criterios: severidad Crítica o Alta, estado Abierta o Cuarentena.

- Gestión de notificaciones: se hace necesario disponer de una tabla que mantenga el registro de aquellas incidencias de severidad más elevadas (en concreto, Crítica o Alta) que hayan supuesto notificación al responsable de la incidencia (o al Equipo de Respuesta, si cuenta con uno). La tabla se denominará NOTIFIED y consta de los siguientes campos:

- ✓ **Identificación de la incidencia (id):** valor entero de 8 dígitos.

- ✓ **Bandera del artículo 33 del RGPD (rgpd):** como su propio nombre indica, se trata de una bandera o flag de control que indica si a la incidencia le afecta el

artículo 33 del RGPD, es decir, debe ser notificada a la AEPD. Tipo booleano, es decir, un carácter ‘S’/‘N’.

Si se observa, los tipos booleanos, normalmente True/False, en este caso se han representado mediante un carácter. Ello se debe a consideraciones de eficiencia a la hora de programar y respecto al almacenamiento. Por un lado, cuando realizas una consulta a una BBDD, el resultado te viene dado en forma de lista (mono o multidimensional), incluyendo caracteres adicionales como paréntesis, corchetes, comillas, etcétera. Extraer el dato de interés y hacerlo para cada caso concreto es algo altamente ineficiente. Al declararlo como cadena (aunque sea de un único carácter), se puede emplear el método *.find()*, así como cualquier otro método aplicable a cadenas caracteres. De esta manera y como se puede observar a lo largo del código Python desarrollado, basta con ejecutar el método *resultado.find('S')* para poder operar en consecuencia, facilitando en gran medida la programación, especialmente evitando tener que extraer el dato booleano para procesarlo a continuación. Además del ejemplo expuesto, quizá el más claro y habitual en el desarrollo de este trabajo, el trabajar con cadenas también posibilita aplicar los métodos asociados a las mismas, sin tener que realizar una conversión previa: *str(variable)*. Por otro lado: declarar, asignar valor, almacenar (tanto en la BBDD como en el código) y trabajar en el código una variable de tipo cadena de un único carácter siempre ocupará menos espacio que un tipo booleano puro. Por tanto y, en definitiva, **los tipos booleanos en este trabajo se declaran como de tipo cadena de un solo carácter ‘S’/‘N’**.

Un detalle importante a tener en cuenta en relación con las medidas de protección, es su dependencia de la valoración del sistema. Según el nivel de seguridad como se haya valorado el sistema (guía CCN-STIC 803, de Valoración de los sistemas), se aplicarán unas medidas de protección u otras. En el contexto de este trabajo y su posible aplicación, su uso está orientado al ámbito de las AA.PP. y, más en concreto, al ámbito de su aplicación en el MINISDEF, lo cual implica trabajar tanto con datos sensibles, como pueden ser datos de carácter personal o información clasificada, por lo que se simplifica la elección de las medidas de protección, al considerarse los **sistemas donde se podría aplicar como de nivel de seguridad Alto**. Además, debido al ámbito en que se aplica, se regirá por el ENS y las guías y recomendaciones originadas en el CCN.

Por otro lado, otro aspecto a considerar, de gran importancia, es el **mantener la consistencia de los datos de las incidencias, evitar los cambios de datos fundamentales y, ante todo, evitar la pérdida de trazabilidad**. Cuando se trabaja en el ámbito de la gestión de incidencias, en el caso de que una incidencia se haya quedado bloqueada durante largo tiempo o precise cambios en datos fundamentales de la misma, la política que suele seguirse es abrir una nueva incidencia haciendo referencia a la anterior, se inserta en el campo de detalles de ambas incidencias cualquier información relativa a la relación entre ambas, y se cierra la incidencia antigua. Dos escenarios típicos de ejemplo podrían ser los siguientes:

- Se desea poner al día el sistema de gestión de incidencias e intentar cerrar aquellas que tengan más de dos años de antigüedad. Supóngase la incidencia 20150013, de comienzos del año 2015, la cual sigue bloqueada en estado de cuarentena a la espera de un software compatible con el nuevo SO utilizado en el sistema.
En ese caso, y siempre que sea viable, es decir, que se tenga constancia de que se obtendrá dicho software, lo más razonable es abrir una nueva incidencia indicando en los detalles de la misma el histórico y la referencia a la incidencia antigua. Este ejemplo, de hecho, está basado en casos reales, y suele ser una situación habitual de cara a cerrar antiguas incidencias que continúen bloqueadas por cualquier motivo.
- Otro ejemplo podría estar relacionado con la clasificación de la incidencia. El campo *type* de la tabla *INCIDENTS* (o *id* de la tabla *ENS*) es fundamental en el sentido de que determina el ámbito de la Seguridad de la Información afectado, y las medidas de protección aplicables. Supóngase que, al dar de alta la incidencia, los indicios apuntan a que está enmarcada en el punto 5.1.5 *PROTECCIÓN FRENTE A INCENDIOS*, sin

embargo, conforme se analiza y avanza en la atención de la incidencia, se determina que realmente debe estar clasificada como *5.1.6 PROTECCIÓN FRENTE A INUNDACIONES*. Bien, lo más socorrido en estos casos es pensar que se soluciona tan fácilmente como cambiar la clasificación de la incidencia, o lo que es lo mismo, cambiar el campo *INCIDENTS.type*. Sin embargo, no es tan trivial, pues cada clasificación lleva asociadas unas medidas de protección aplicables, es posible que algunas de ellas ya se hayan aplicado, incluso consideraciones a tener en cuenta anotadas en las observaciones de cada medida de protección. Por tanto, intentar solucionarlo sin más que cambiar la clasificación de la incidencia provocaría problemas de consistencia de los datos y de coherencia en el seguimiento de la incidencia **impidiendo su trazabilidad, aspecto fundamental en el ámbito de la Seguridad de Información y de cara a la Auditabilidad**.

De nuevo, al igual que en el ejemplo anterior, la solución pasa por abrir otra incidencia con la nueva clasificación pretendida, y dejar claro en los detalles de la misma la relación con la incidencia anterior, y el motivo de su apertura. De igual manera, la incidencia anterior, antes de cerrarse, debe dejar claramente reflejado el motivo de su cierre anticipado y la relación con la incidencia que le sustituye.

De ahí que **sólo se permita modificar algunos campos de las incidencias a lo largo de su ciclo de vida**. Se deja como línea de trabajo futura determinar con rigurosidad qué datos se podrían modificar y cuáles no, manteniendo, claro, la consistencia de la BBDD y **siempre que no se vean afectadas la trazabilidad, y la seguridad del sistema**.

A la hora del cierre de una incidencia, se deberá estar seguro que se incluye toda aquella información y configuración de datos de la incidencia que se consideren de interés, pues, **para mantener la consistencia de la BBDD y la coherencia, una vez cerrada una incidencia no admite modificación**.

Para hacer más eficiente y ágil la experiencia de usuario, a la hora de trabajar con la plataforma, los listados (mostrados mediante tablas) de las consultas contendrán una parte fundamental de los datos. Para visualizar la información completa de una entrada (incidencia) en el listado, se seleccionará dicha entrada, lo cual llevará a la interfaz web a través de la cual se desarrolla el servicio de gestión de incidentes de Seguridad de la Información, donde se puede consultar de manera detallada y editar la información de la incidencia.

Hay que tener presente que se trabaja con información operativa relacionada con seguridad, por lo que su tratamiento debe ser eficiente y proteger frente a corrupción o fugas de datos. Así mismo, se precisará una validación robusta de cada entrada de datos para evitar el uso de caracteres no permitidos o reservados, ya sea por error o de manera deliberada.

La información contenida en la base de datos se considera sensible, por lo que debe preservarse su confidencialidad. En el caso de que deba transmitirse de manera remota, deberá realizarse de manera cifrada.

3.3.2 Diseño conceptual

Una vez expuestos los requisitos, se pasa a desarrollar el diseño conceptual, lo cual ofrece una representación de los recursos de información y sirve de paso intermedio facilitando el diseño lógico del sistema que dé solución a las necesidades planteadas. En el marco de este trabajo se utilizará el modelo Entidad-Asociación, o Entidad-Relación, debido a que se trabaja con datos estructurados.

Por tanto, se seguirán los siguientes pasos:

- Identificar las entidades.
- Identificar las asociaciones (relaciones).
- Identificar y asociar los atributos con las entidades y asociaciones.
- Determinar los dominios de los atributos (campos).

- Determinar los atributos que actuarán como clave principal (PK $\equiv$ Primary Key) y como clave externa (FK $\equiv$ Foreign Key), en cada relación.
- Eliminar posibles redundancias.

A partir de la información detallada en la especificación de requisitos, y siguiendo los pasos descritos se obtiene el siguiente Diagrama Entidad-Relación (Diagrama E-R):

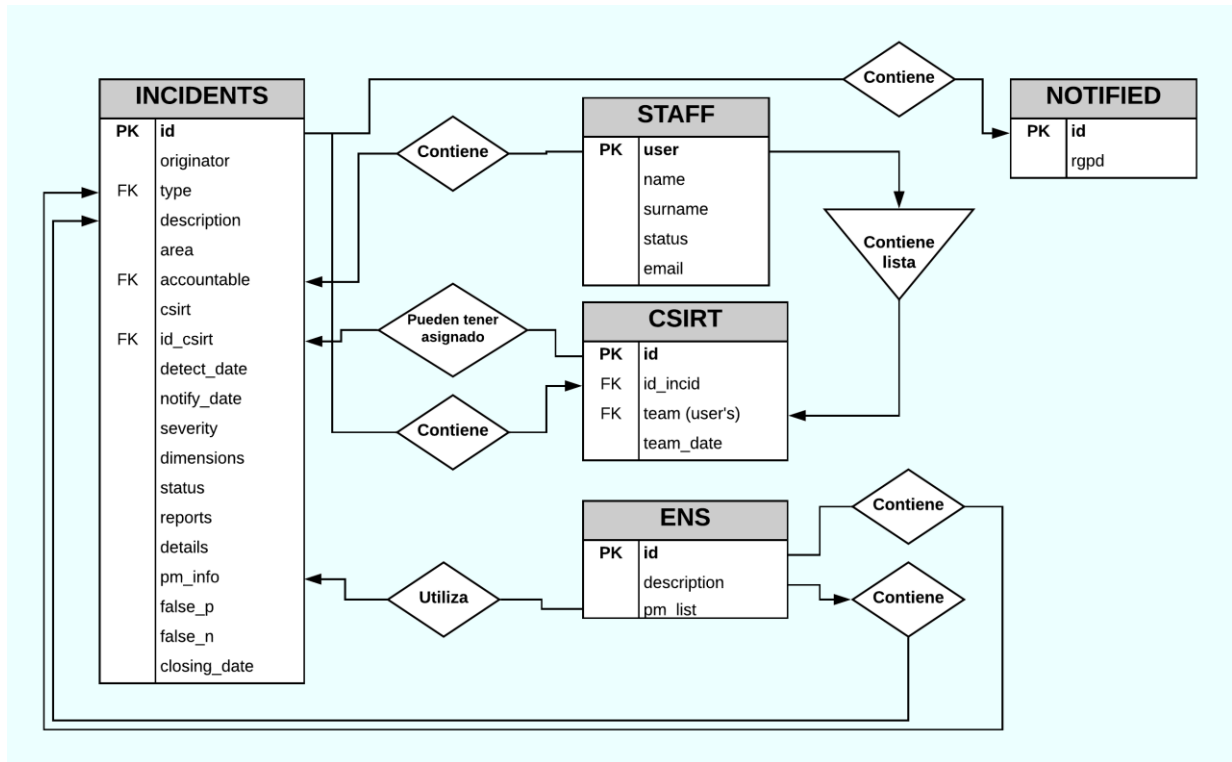


Figura 3-3. Diagrama E-R.

3.3.3 Diseño lógico

Una vez establecido el Diagrama E-R del sistema, el siguiente paso consistirá en transformar dicho esquema conceptual de tal manera que se adapte a la representación de relaciones correspondiente. Debido a que se trabajará con datos estructurados, el diseño lógico se desarrollará siguiendo el modelo relacional. El resultado es el siguiente:

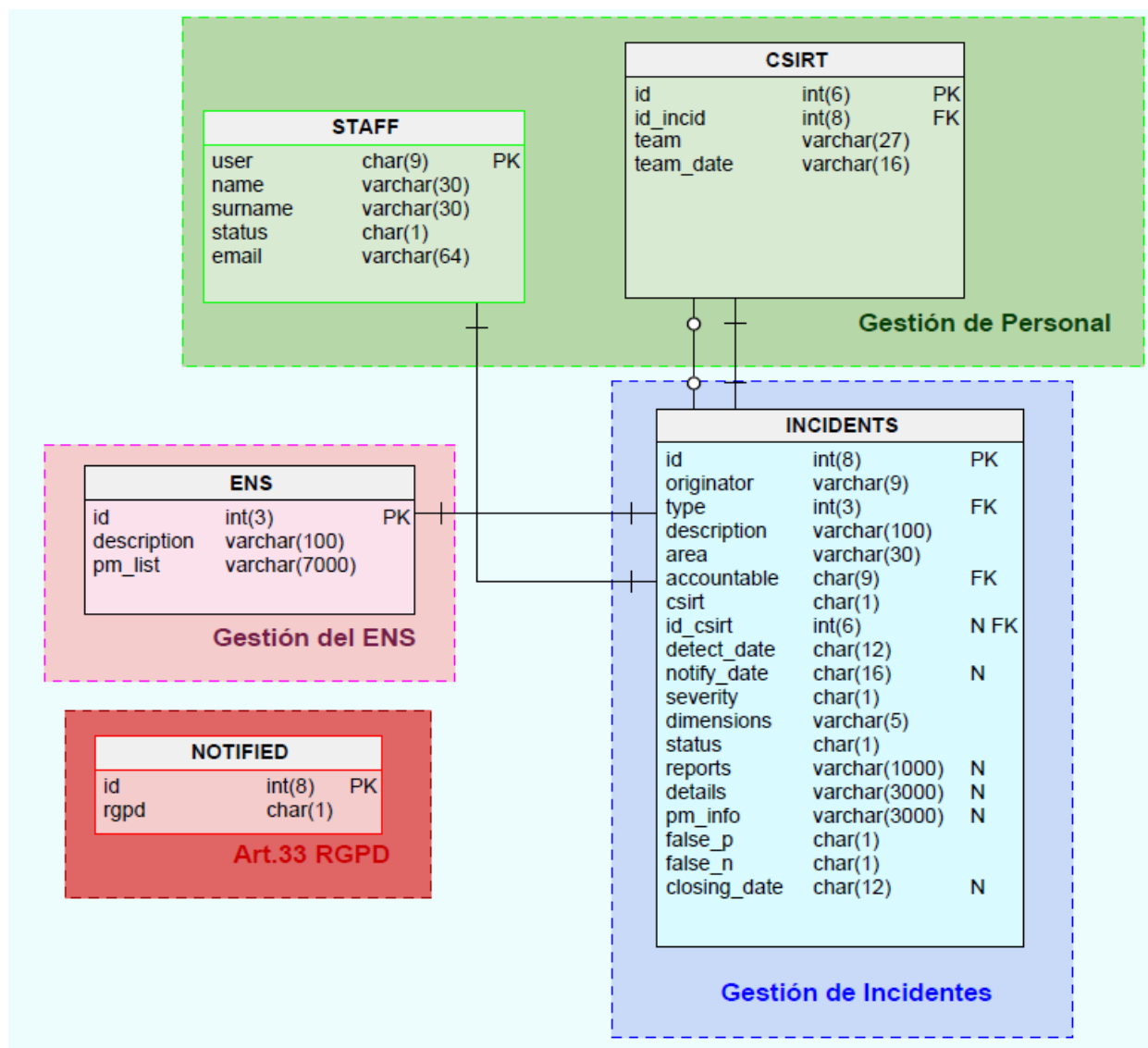


Figura 3-4. Modelo Relacional.

Merece la pena comentar acerca de la configuración de las referencias, pues es un aspecto muy importante de cara a mantener la consistencia de la BBDD. En el próximo apartado se explican los motivos al hablar de *Integridad referencial*. Siguiendo el criterio expuesto en dicho apartado, las referencias se han configurado de la siguiente manera:

- **CSIRT_INCIDENTS**: la clave primaria **id** de la tabla **CSIRT** se utiliza en la tabla **INCIDENTS** como **id_csirt**. En esta ocasión no hay riesgo de provocar inconsistencia en los datos, pues ambos datos se declaran como fundamentales, por lo que no admiten modificación.
Por otro lado, en este caso la cardinalidad se establecerá en 0..1, pues una incidencia puede tener asociado 1 CSIRT, o no tener asociado ninguno.
- **INCIDENTS_CSIRT**: la clave primaria **id** de la tabla **INCIDENTS** se utiliza en la tabla **CSIRT** como **id_incid**. Al igual que en el caso anterior, no hay riesgo de provocar inconsistencia en los datos, pues ambos datos se declaran como fundamentales, por lo que no admiten modificación. Por otro lado, en este caso la cardinalidad se establecerá en 1..1, ya que la conformación de un CSIRT se realiza y se asocia de manera explícita para dar solución a una incidencia concreta de severidad Crítica, es decir, siempre existe y solo se asocia un CSIRT a una incidencia, por lo que la relación es 1 a 1.

- STAFF_INCIDENTS: La clave primaria *user* de la tabla STAFF se utiliza en la tabla INCIDENTS como *accountable*. Al igual que ocurría en el caso de la referencia STAFF_CSIRT y por los mismos motivos, se permite modificar un nombre de usuario y ello genera la actualización en cascada, pero no se permite eliminar usuarios de la tabla STAFF.
- ENS_INCIDENTS: la clave primaria *id* de la tabla ENS se utiliza en la tabla INCIDENTS como *type*. Tal como se expuso y motivó en el apartado 3.3.1 *Especificación de requisitos*, ambos campos ($ENS.id = INCIDENTS.type$), no son modificables, por lo que se evita la posible inconsistencia de los datos.

3.3.4 Normalización e Integridad

Mediante este proceso se identifican y eliminan aquellas anomalías de diseño en las relaciones construidas. Para ello se definen un conjunto de formas normales o restricciones de diseño. Se trata en definitiva de un conjunto de condiciones o reglas que deben cumplir las relaciones para evitar dichas anomalías y reducir los problemas de lógica. Las anomalías más típicas en el diseño de BBDD que se deben evitar son:

- La redundancia de los datos.
- Problemas de actualización de datos en las tablas.
- Problemas de integridad de los datos.

La primera de ellas, relativa a la redundancia de datos, depende exclusivamente del diseño. En este caso y una vez revisado el diseño, solo habría un detalle a tener en cuenta. Se trata de los campos *ENS.pm_list* e *INCIDENTS.pm_info*. Ambos campos de tablas distintas tienen una fuerte relación. Sin embargo, su contenido es fundamentalmente distinto. Mientras que *ENS.pm_list* recoge el conjunto de medidas de protección propuestas por la guía CCN-STIC 804 en forma de campo de texto, el campo *INCIDENTS.pm_info* contiene información estructurada, a saber: las medidas de protección, la bandera de si se han aplicado o no, y observaciones para cada medida de protección. Por tanto, se verifica que el diseño no sufre de redundancia innecesaria.

Los siguientes problemas más típicos, tanto los relativos a la actualización como a la integridad de los datos, dependen tanto del diseño como de la operación sobre la base de datos. Desde el punto de vista del diseño, se debe desarrollar de tal manera que se simplifique la actualización de los datos y se posibilite aplicar mecanismos de verificación de la integridad de los datos durante su operación y almacenamiento. En realidad, los problemas principales respecto a estos aspectos suelen originarse en sistemas distribuidos, los cuales requieren mecanismos adicionales para garantizar la consistencia de los datos. En el caso de este trabajo, el despliegue y operación se realizarán de manera centralizada, por lo que se evitará la complejidad y problemas asociados a los sistemas distribuidos.

A continuación, se comprueba si el diseño propuesto para este trabajo cumple las 3 primeras formas normales para el diseño de BBDD relacionales, creadas por Edgar F. Codd [17]:

- Primera Forma Normal (1FN): se dice que una relación está en 1FN cuando cada atributo sólo toma un valor del dominio subyacente, decir, no existen registros o tuplas con el contenido del mismo atributo coincidente. El ejemplo más trivial es una relación con los datos de personal, y que exista la coincidencia de que dos hermanos sean empleados de la misma organización. En ese caso, el contenido del atributo o campo *Apellidos* será idéntico en ambos casos.

Realmente, es una circunstancia que se produce en la mayoría de sistemas de BBDD y suele ser inevitable. En estos casos lo que hay que hacer es **evitar fijar esos atributos como campos clave**, ya que no identifican de manera unívoca a cada registro de la relación.

- Segunda forma normal (2FN): se dice que una relación está en 2FN si todos los atributos no clave dependen por completo de la clave primaria. El problema de esta regla se plantea cuando la clave de una tabla es compuesta, y uno de los campos no clave depende exclusivamente de uno de los campos claves, pero no del resto de campos clave de la composición. En el caso de este trabajo, no se presenta dicha circunstancia.
- Tercera forma normal (3FN): se dice que una relación está en 3FN si no existe ningún atributo no principal que dependa transitivamente de alguna clave primaria, es decir, que no existan atributos no principales que dependan funcionalmente de otros atributos no principales. Como se puede observar en la descripción de los campos y la conformación de cada tabla, esta circunstancia tampoco se produce en el diseño del presente trabajo.

Otro aspecto a tener en cuenta es si en el diseño desarrollado se puede hablar indistintamente de relaciones y tablas para referirse al mismo concepto. Para que ello pueda darse, las tablas deben cumplir las siguientes condiciones:

- Cada columna, atributo o campo debe tener su nombre único.
- No puede haber dos filas, registros o tuplas iguales: no se permiten los duplicados.
- Todos los datos en una columna deben ser del mismo tipo.

En el caso del diseño de la BBDD desarrollado para este trabajo, se cumplen las tres condiciones, por lo que de ahora en adelante se utilizarán indistintamente los términos relaciones o tablas.

Por último, se aplican las siguientes restricciones de integridad de datos, las cuales permiten preservar la consistencia y corrección de los datos almacenados en la BBDD:

- Datos requeridos: algunas columnas de la BBDD deben contener un valor de datos válido en cada fila, es decir, no se permite que todas las columnas contengan valores *NULL*. Como se observa en el Modelo Relacional expuesto en el apartado anterior, solo se permiten que algunos campos sean nulos (*Nullable* == *N*). El resto de campos (la mayoría) obligatoriamente han de contener datos válidos.
- Chequeo de validez: cada columna de la BBDD debe tener un dominio asignado, es decir, un conjunto de valores válidos para esa columna. De nuevo, como se observa en el Modelo Relacional, todos los campos tienen asignado un dominio.
- Integridad referencial: cada clave externa (*Foreign Key* == *FK*) en la BBDD relacional enlaza cada fila de la tabla hijo, la cual contiene la clave externa, con la fila de la tabla padre, la cual contiene el valor de clave primaria (*Primary Key* == *PK*) correspondiente. Como se observa en el Modelo Relacional, se cuenta con 4 referencias que enlazan claves primarias y externas. Se deben adoptar las medidas necesarias de tal manera que se asegure que las relaciones entre entidades (referencias) de la BBDD se preserven durante las actualizaciones. Ejemplo: si una entidad padre que tiene asociada una entidad hija desaparece, se debe actualizar el contenido de la clave externa de tal manera que no contenga una referencia inexistente. Viendo el ejemplo gráficamente sobre el Modelo Relacional: si un registro de la tabla *CSIRT* desaparece, y el contenido de su clave principal *CSIRT.id* se alberga en algún registro *INCIDENTS.id_csirt*, el contenido de la clave externa *INCIDENTS.id_csirt* debe actualizarse (a 0, en este caso). Para intentar mantener la consistencia de la BBDD, no se permitirá la modificación ni el borrado de datos que se consideran fundamentales, y que puede provocar la pérdida de trazabilidad. Siguiendo con el ejemplo, **una vez creada la incidencia, no se permitirá la modificación de datos fundamentales que puedan afectar a la trazabilidad en la gestión de la misma, en este caso, *CSIRT.id*.**

La siguiente tabla recoge los campos declarados como datos fundamentales:

Tabla	Campo
INCIDENTS	id
	originator
	type
	description
	area
	detect_date
	notify_date
	closing_date
CSIRT	id
	id_incid
	team_date
STAFF	user
	name
	surname
	email
ENS	id
	description
	pm_list

Tabla 3-1. Campos declarados como datos fundamentales.

- Integridad de entidad: la clave primaria de cada tabla debe contener un valor único en cada fila, diferente de los valores de todas las filas restantes. De esta manera se podrá identificar de manera unívoca a cada registro de la tabla. Lo cual se cumple por parte de la BBDD soteria.

3.3.5 Diseño físico

Como último paso en el diseño de la BBDD, se realiza el diseño físico. Se trata de obtener la implementación, lo más eficiente posible, a partir del resultado del esquema lógico. Es decir, la implementación del Modelo Relacional, en este caso.

La implementación dependerá del lenguaje utilizado y del sistema gestor de BBDD elegido. En este caso se emplean las siguientes características de la BBDD:

- **Lenguaje: Structured Query Language (SQL).**
- **Sistema Gestor de Bases de Datos (SGBD / DBMS): MariaDB.**

Una vez fijado el lenguaje y el SGBD, y a partir del Modelo Relacional diseñado, se pasa a codificar la generación de la nueva BBDD, la creación del usuario para la ejecución de las consultas, el otorgamiento de permisos al usuario, la generación de las tablas y, según el caso, el relleno inicial de los datos de las tablas. Para este trabajo se generarán algunos registros para cada tabla de cara a poder realizar las pruebas y verificar la funcionalidad de todos los apartados de la plataforma.

A continuación, se describen los archivos desarrollados que forman parte de la generación de la BBDD, y relleno de datos (se recomienda su visionado desde la herramienta gratuita Notepad++):

- MGSTICS_TFM_create_FULLL.sql: contiene el código SQL completo para crear la BBDD, crear el usuario de acceso a la BBDD, otorgar los permisos de acceso, creación de las tablas, inserción de datos iniciales de prueba en cada tabla y la declaración de claves foráneas. Cargando este archivo a través de la herramienta *mysql* de línea de comandos para la conexión con el gestor de BBDD MariaDB, se tiene una versión funcional completa de la BBDD, preparada para poder realizar todo tipo de pruebas. La tabla *NOTIFIED* no requiere cargar datos iniciales, ya que se va rellenando automáticamente al arrancar la plataforma conforme se detectan nuevas incidencias de severidad Crítica o Alta mediante el script Python de ejecución automática *notify.py*.
- MGSTICS_TFM_drop_FULLL.sql: contiene el código SQL para eliminar las claves foráneas, las tablas, el usuario de acceso y la propia BBDD soteria.
- 1_staff_table.sql: código SQL para cargar los datos de la tabla STAFF.
- 2_ens_table.sql: código SQL para cargar los datos de la tabla ENS.
- 3_csirt_table.sql: código SQL para cargar los datos de la tabla CSIRT.
- 4_incidents_table.sql: código SQL para cargar los datos de la tabla INCIDENTS.
- Relleno_BBDD.py: script Python para generar automáticamente los datos de prueba a insertar en las tablas ENS, CSIRT e INCIDENTS. La tabla STAFF es muy sencilla, por lo que pueden generarse datos de prueba manualmente.

Mención especial tiene la problemática existente en las dependencias de datos entre distintos campos, en concreto entre los campos *INCIDENTS.id_csirt* y *CSIRT.id* por un lado; y entre *CSIRT.id_incid* e *INCIDENTS.id*, por otro. Para entenderlo de manera rápida, el problema se reduce al dicho popular: “¿qué fue antes, el huevo o la gallina...? El problema surge porque ambas parejas de datos son coetáneos, es decir, se intentan generar y registrar al mismo tiempo en sus respectivas tablas. Como el gestor de BBDD detecta que es posible que no exista el otro dato cuando se está generando uno de ellos, es por lo que devuelve el error al definir las claves foráneas en tiempo de creación de la BBDD. La solución pasa por no declarar la dependencia en tiempo de creación de las tablas (aunque se contemple por diseño), y controlar programáticamente la inserción de los datos en sus respectivos registros en tiempo de operación. El problema explicado de manera sencilla es el siguiente:

- Cuando pretendes registrar una nueva incidencia que lleva asociado un CSIRT, ¿qué datos introduces en el campo *INCIDENTS.id_csirt*...?
- Cuando estás conformando un nuevo CSIRT, ¿qué dato introduces en el campo *CSIRT.id_incid*...?

La solución en estos casos pasa por los siguientes pasos:

- No declarar la dependencia de los campos en tiempo de generación de la BBDD.
- En el caso concreto de este trabajo, al registrar una nueva incidencia que lleve asociado la conformación de un CSIRT, llegará un momento en que debe rellenarse el campo *INCIDENTS.id_csirt*. Como aún no está generado, lo que se hace es lanzar primero la generación de un nuevo CSIRT que atienda esa incidencia. En este caso, el registro de un

nuevo CSIRT sí se puede completar ya que sí se conoce el *CSIRT.id incid* (la identificación de la incidencia es conocida al empezar a generar la misma).

- Una vez completado el registro del nuevo CSIRT, ya se conoce el *CSIRT.id* que se registrará en el campo *INCIDENTS.id_csirt*, permitiendo completar el alta de la incidencia.
- No se requiere control adicional de cambio de estos dos campos (*CSIRT.id* e *INCIDENTS.id_csirt*), ya que, tal como se exponía en los apartados 3.3.1 *Especificación de requisitos* y 3.3.4 *Normalización e Integridad*, ambos se consideran datos fundamentales, por lo que no se permite su modificación o eliminación.

De esta manera, **mantener la consistencia de los datos se mantiene bajo control del programador**, en lugar de confiarlo al gestor de la BBDD, además de **permitir la trazabilidad de la gestión, aspecto fundamental en el ámbito de la Seguridad de Información y de cara a la Auditabilidad**.

3.4 Diseño de la interfaz web.

Para describir las partes principales de la interfaz y los recursos utilizados para su control se muestra a continuación la pantalla inicial de bienvenida de la plataforma:



Figura 3-5. Interfaz web general de acceso a los servicios de la plataforma Soteria.

La interfaz se encuentra integrada por los siguientes componentes:

- Marquesina superior: incluye el logo del CUD, el título, el nombre del usuario autenticado y el botón para salir del aplicativo.
- Marquesina inferior: incluye la denominación del Máster y la indicación de que se trata de un Trabajo de Fin de Máster.
- Marquesina lateral: incluye el menú lateral de acceso a los servicios, denominación de la plataforma, la marca de fecha y hora, el botón de acceso al índice general y un logo del autor.
- Cuerpo de la página: incluye a su vez dos partes:
 - Menú superior de acceso a los servicios en forma de pestañas.
 - Cuerpo principal de la interfaz donde se ofrecerá la información de cada servicio.

Las tecnologías utilizadas para el desarrollo de la interfaz web han sido:

- Componentes HTML: objetos *Fieldset* para la agrupación de elementos en la interfaz, botones de selección de distinto tipo, tablas, elementos de entrada de distinto tipo (*input*), inserción de imágenes e iconos, formularios, cuadros de texto, listas desplegables (*select*), etcétera.
- Plantillas web: albergan la plantilla para la generación de los interfaces web a través de los diferentes servicios que ofrece la plataforma. Son:
 - banner.html: plantilla web de bienvenida.
 - index.html: plantilla web principal, se emplea para la mayoría de servicios.
 - logout.html: plantilla web para mostrar al usuario el resultado de la salida.
 - manage_incident.html: plantilla web para la gestión de incidentes.
 - new_incident.html: plantilla web para el alta de nuevas incidencias.
 - nok.html: plantilla web para el aviso de error ante alguna acción del usuario.
- Hoja de estilos en cascada (CSS): se recoge a través del archivo *styles.css*. Se ha intentado parametrizar y asignar en la medida de lo posible los estilos desde dicho archivo, pero en algunos casos ha sido imposible, principalmente por compatibilidad de los componentes. En ese caso los estilos se han asignado directamente sobre los objetos html. En otros casos, como es el caso de la generación del contenido de la pestaña ENS, el estilo está definido adrede en el propio contenido para evitar que se modifique su apariencia de manera externa. De esta manera siempre se mostrará tal como se visualiza en la Guía CCN-STIC 804, de Implantación del ENS.
- Librerías y código Javascript:
 - jquery.min.js: librería de código abierto para el control de elementos de la interfaz, uso de variables, etc.
 - cambiarPestanna.js [18]: librería de código abierto para el control de navegación mediante pestañas.
 - clock.js [19]: librería de código abierto para la visualización del reloj en la interfaz.
 - /sweetalert.min.js [20]: librería de código abierto para la muestra de ventanas emergentes en la interfaz web.
 - Chart.min.js y utils.js [21]: librerías de código abierto para la generación de gráficas.
 - Código de desarrollo propio para el control de las gráficas, control de cambios en los elementos de la interfaz, habilitación/deshabilitación de elementos de la interfaz, asignación de valores, etcétera.
- Código interpretado para la plataforma de generación dinámica de páginas web utilizada (Flask): se verá en el subapartado 3.5 relativo a ello.

La extracción del nombre del usuario autenticado se realiza a partir de la información que guarda Google Authenticator en un determinado fichero del servidor. De esta manera, basta desarrollar un script shell que permita localizar dicho fichero recién creado y extraer el nombre del usuario, insertado justo al final del contenido del mismo. Esta funcionalidad se ha desarrollado mediante el script denominado *get_user.sh*, y su contenido puede consultarse en el *Anexo II: Scripts*. El sistema de autenticación mediante Google Authenticator se tratará en el apartado 3.8 *Seguridad*.

3.5 Generación dinámica de las páginas web y tareas automatizadas.

3.5.1 Plataforma de generación dinámica de páginas web.

Para la interconexión entre el lado del servidor y el lado del cliente se ha utilizado el Middleware Flask. Se trata de una plataforma software que permite la generación dinámica de páginas web desde la programación activa del servidor. Está escrito en Python, por lo que ofrece buena compatibilidad e integración a la hora de desarrollar la parte activa del servidor mediante código Python, como ha sido el caso de este trabajo.

Está basado en la especificación WSGI de Werkzeug. WSGI (Web Server Gateway Interface) es un término empleado para las funciones de redireccionamientos de los servidores web de las peticiones que reciben, a las aplicaciones o plataformas web correspondientes que las atienden. Se encuentran escritas en lenguaje Python.

El motor de plantillas (templates) que utiliza se denomina Jinja2.

En ambos casos, tanto la plataforma Flask como el motor de plantillas web Jinja2, se distribuyen bajo licencia BSD, por lo que se permite su uso en software no libre.

Utilizar este conjunto de recursos facilita la labor de desarrollo, pues permite centrar el desarrollo completo de la parte activa del servidor (procesado) en un archivo de programación Python.

Los recursos principales que se han utilizado de cara a la generación dinámica de las plantillas web han sido los siguientes:

- Paso de variables: constituye uno de los recursos principales, ya que permite pasar variables tras ser procesadas en el servidor al motor de plantillas, el cual insertará su contenido allí donde se referencie dicha variable en la plantilla web:
 - En el lado del servidor, la variable se pasa al generar la plantilla mediante la función `render_template()`. Si se observa el código principal de procesado del servidor, el archivo `Soteria.py`, aparecen varias llamadas a dicha función, por ejemplo:

```
return render_template(app.config['DEFAULT_TPL']+'index.html',  
                      current_user = session['current_user'],
```

...

`current_user = session['current_user']` constituye el paso de una variable, donde la denominación que empleará el motor de plantillas es la que aparece a la izquierda de la asignación, mientras que la parte derecha de la asignación es el valor que contendrá y que se insertará en la página web.

Siguiendo con el ejemplo, en la plantilla web, `index.html` en este caso, aparecerá:

```
{{ current_user }}
```

- En el lado del cliente, lo que recibe es la plantilla interpretada, es decir, en este caso, el contenido de la variable inserto en la página `.html` recibida.
A la hora de generar la página web final que se enviará al cliente, el motor de plantillas sustituye la variable por su contenido, por lo que lo que el cliente verá en este caso será:



Las variables sobre la plantilla web se referencian encerradas entre dobles `{{ }}`.

- Programación en la plantilla web: para mejorar la potencia a la hora de generar de manera dinámica la página web, el motor de plantillas permite insertar código interpretable en la

plantilla web. Lo más habitual suele ser, por ejemplo, para el control a la hora de generar una lista desplegable (select):

```
<select name="severity" id="severity">
  <option name="severity" value="B" {% if severity == 'B' %} selected="selected" {% endif %}>Baja</option>
  <option name="severity" value="M" {% if severity == 'M' %} selected="selected" {% endif %}>Media</option>
  <option name="severity" value="A" {% if severity == 'A' %} selected="selected" {% endif %}>Alta</option>
  <option name="severity" value="C" {% if severity == 'C' %} selected="selected" {% endif %}>Crítica</option>
</select><br/><br/>
```

Se puede observar cómo se utiliza sentencias de tipo `{% if %} / {% endif %}` para el control de selección de los elementos de la lista.

Ello aporta gran potencia y flexibilidad a la hora de generar la interfaz y mejorar la experiencia del usuario, pues se personaliza y automatiza la información en función de los datos de que se disponga.

Estos recursos han sido esenciales para mejorar la usabilidad y la navegación de la plataforma web.

Aunque se pueden conseguir resultados muy buenos y emplear características avanzadas con estos recursos, en realidad se trata de la parte sencilla del desarrollo. La dificultad realmente estriba en la programación activa del servidor, es decir, el procesado adecuado para que la información que llega al motor de plantillas y, en definitiva, la información que recibe el cliente, sea la correcta y libre de errores.

El proceso inverso, es decir, la captura de datos desde la interfaz web del cliente para su procesado en el servidor se realiza mediante el envío de formularios. Al seleccionar el usuario cliente un botón o una imagen que remite un formulario, los datos se recogen mediante el método configurado en el servidor. Los formularios y la petición de datos que recogen los mismos se pueden capturar mediante dos métodos: POST y GET. Para el desarrollo del presente trabajo se ha empleado el método POST.

A partir de ahí, es tan sencillo como utilizar los métodos para extraer el valor de los objetos enviados. Existen dos métodos: `request.form.get('variable')` y `request.form.getlist('variable')`. El primero se utiliza para leer el contenido de una variable de valor único. El segundo se emplea para el leer el contenido de una lista.

Como se observa, la interacción entre la programación activa del servidor en Python y el motor de plantillas web es relativamente sencilla. La dificultad consiste en el procesado correcto de la información.

3.5.2 Tareas automatizadas.

Una de las premisas que se ha intentado seguir a lo largo del desarrollo del presente trabajo es lograr automatizar todas aquellas tareas que lo permitan y sean de interés. En concreto, se han automatizado los siguientes procesos:

- Simulación del sistema SIEM: generación automática de incidencias simulando el comportamiento de un sistema SIEM. Se desarrolla mediante el script Python *siem.py*. La funcionalidad que incorpora se describe de manera resumida mediante los siguientes pasos:
 - Inicialización del acceso a la BBDD.
 - Generación de los valores de aquellos campos cuyo valor se conoce de antemano y serán, por tanto, de valor fijo en el momento de la creación de la incidencia: *originator*, *detect_date*, *status*, *false_p*, *false_n* y *closing_date*.
 - Generación del campo *id*, consultando previamente el valor máximo que existe en la tabla *INCIDENTS* para conservar la secuencia.
 - Generación de los campos *type* y *description*.

- Generación del campo *area*.
- Generación del campo *severity*, empleando un generador de números aleatorio para asignar la severidad según la distribución de probabilidad establecida, en este caso: Crítica: 5%, Alta: 10%, Media: 30% y Baja: 55%.
- Conformación de Equipo de Respuesta, aplicando también un generador de números aleatorio, con el siguiente criterio: probabilidad del 94% de conformar un CSIRT para incidencias de severidad Crítica.
- Generación del campo *dimensions*.
- Generación del campo *details*, mediante la selección aleatoria de una lista para incidencias en cuarentena.
- Generación del campo *pm_info* a partir del valor del campo *type* y la información del campo *ENS.pm_list* correspondiente.
- Por último, inserción de la nueva incidencia en la tabla *INCIDENTS*.

Para la ejecución periódica del script se emplea el gestor de programación de tareas CRON de Linux. El periodo de activación se puede regular, haciéndolo menor para las pruebas, por ejemplo. Lo normal es una frecuencia de 1 incidencia al día, en el peor de los casos. Para realizar pruebas rápidas se puede programar su activación cada hora:

@hourly python /var/www/Soteria/src/siem.py

- Servicio de notificaciones: se desarrolla mediante el script Python *notify.py*. El servicio automático de notificaciones, debido a su importancia y extensión, se expone en un subapartado propio a continuación.

3.5.3 Implementación del servicio de notificaciones.

Una vez planteados los condicionantes reflejados en el apartado 3.2.6 *Servicio de notificaciones*, se pasa a continuación a exponer **cómo se le ha dado solución** en la plataforma Soteria.

Para atender las incidencias que requieren Notificación, se han desarrollado los siguientes recursos:

- **Tabla NOTIFIED dentro de la BBDD Soteria**: compuesta de los campos *id* y *rgpd*. El campo *id* recogerá los identificadores de las incidencias de severidad Crítica y Alta de nueva creación. De esta manera se mantendrá registro de las incidencias de mayor severidad que han requerido Notificación. El campo *rgpd* recoge el flag* relativo a la posible vulneración de la seguridad de los datos personales, al amparo del artículo 33 del REGLAMENTO (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, tal como se expuso en el apartado 2.5 *Normativa y legislación*.

Una vez cerrada la incidencia, se debe eliminar de la tabla NOTIFIED, pues el objetivo de dicha tabla es servir de punto de consulta de las incidencias de mayor severidad que se encuentran aún abiertas o en cuarentena.

- **Fichero de script Python notify.py**: Desarrolla el servicio que comprueba si hay incidencias de severidad Crítica o Alta pendientes de notificar, las registra en la tabla NOTIFIED si fuera el caso, y las **notifica** mediante correo electrónico **al responsable** de la gestión de cada nueva incidencia que cumpla estas condiciones. En el caso de que la incidencia lleve asociada la conformación de un Equipo de Respuesta (CSIRT), **se notifica a los tres (3) miembros del equipo**. Además, **si la incidencia está categorizada de tipo 571 (DATOS DE CARÁCTER PERSONAL), es posible que suponga una violación de la seguridad de los datos**

personales, por lo que se refleja así y claramente en el correo de notificación, cumpliendo de esta manera con la normativa comunitaria (parcialmente, claro, ya que lo se genera es la notificación técnica: se completará cuando, finalmente, el responsable de la organización envíe la notificación legal a la AEPD).

- **Programación de ejecución periódica del script notify.py:** mediante la configuración del gestor de tareas automático de Linux (*CRON**) se pueden ejecutar actividades de manera periódica. Para ello, basta con ejecutar el comando *sudo crontab -e*, y añadir la siguiente línea:

```
*/1 * * * * python /var/www/Soteria/src/notify.py
```

De esta manera, **se ejecuta cada minuto la comprobación de nuevas incidencias de severidad Crítica o Alta que requieran Notificarse.**

Por otro lado, no debe dejarse de lado el artículo 34 del Reglamento europeo, en el sentido de que, si se estima que la posible violación de la seguridad de los datos personales puede entrañar un alto riesgo para los derechos y libertades de las personas físicas (afectados), se les debe comunicar también a éstos, lo antes posible, el incidente, tal como se introdujo en el apartado 2.5 *Normativa y legislación*. En realidad, esta parte, de cara a Soteria y el desarrollo de este trabajo, trasciende, es transparente, pues el alcance de la plataforma Soteria queda en la detección (y, por supuesto, ayuda a la subsanación) de la incidencia, notificando a los responsables de la gestión de la incidencia, de tal manera que se vaya escalando la notificación técnica hasta llegar al verdadero responsable del tratamiento de los datos personales: **el responsable de la organización**. De esta manera, y **contando con la mayor cantidad de información técnica que se tenga disponible a través de Soteria**, el responsable puede generar la notificación final (legal) de la brecha de seguridad (si afectase a los datos personales) a la AEPD en primer lugar y, de determinar que cabría aplicar también el artículo 34, notificar igualmente a los afectados. El escenario habitual y cargos por donde transcurriría la notificación de la incidencia hasta llegar al responsable último de la organización se reflejaba en las Figuras 3-1 y 3-2, según el caso.

En lo que respecta a la plataforma Soteria, bajando al detalle de la implementación, el script *notify.py* desarrolla los siguientes pasos:

- Carga las librerías necesarias e inicializa el acceso a la BBDD Soteria.
- Se buscan aquellas incidencias de severidad Crítica o Alta que se encuentren en estado Abierta o Cuarentena.
- Para cada una de las incidencias del paso anterior:
 - Se comprueba si ya se encuentran registradas en la tabla NOTIFIED. Si no lo están:
 - Se comprueba si está afectada por el Art.33 del RGPD y si tiene asociado o no un Equipo de Respuesta para atenderla.
 - Se registra en la tabla NOTIFIED.
 - Se componen el asunto y el cuerpo del texto del mensaje de notificación.
 - Se componen las direcciones de correo electrónico donde ejecutar la notificación: al responsable, si no dispone de CSIRT; o a los tres (3) componentes si la incidencia actual tiene conformado un CSIRT.
 - Envía el(los) correo(s) de notificación.

Aclarar que, por seguridad, no se envían todos los detalles de la incidencia por correo electrónico. La notificación incluye el aviso con la severidad, el tipo de incidencia y, si procede, el aviso de posible violación de la seguridad de los datos personales.

De esta manera, se cumplen los siguientes objetivos parciales de este apartado:

- Se cumple con la normativa legal vigente.

- Se notifica a los responsables de la incidencia, por lo que pueden atenderla a la mayor brevedad posible.
- Se automatiza el proceso de detectar las incidencias más graves generadas más recientemente, haciendo el trabajo más eficiente y facilitando la tarea al personal responsable de Seguridad de la Información.

3.6 Integración y puesta en marcha de la plataforma web.

La puesta en marcha de la plataforma requiere del despliegue e integración de los recursos software descritos en la Tabla 2-1, y que se reproduce aquí por comodidad:

Software	Versión
Sistema Operativo <i>Ubuntu Server Linux</i>	14.04.5 LTS
Servidor Web <i>Apache HTTP Server</i>	2.4.7
Módulos <i>python-setuptools</i> y <i>libapache2-mod-wsgi</i>	40.5.0, 3.4
Gestor de BBDD <i>MariaDB</i>	10.3.10
Programación activa del servidor mediante <i>Python</i>	2.7.15
Acceso programático a la BBDD mediante <i>mysql-connector-python</i>	8.0.13
Acceso a la BBDD mediante línea de comandos mediante <i>mysql</i>	15.1
Generación dinámica de páginas web mediante <i>Flask</i>	1.0.2
Planificador de tareas mediante <i>CRON</i>	Integrado en Linux

Tabla 3-2. Recursos software necesarios.

Una vez se dispone de esta relación de software instalado en el equipo, se pueden copiar los ficheros fuente de desarrollo: páginas web .html, código Python .py, hojas de estilos .css, ficheros de JavaScript .js, etcétera. Lo normal es crear una estructura estándar bajo el directorio */var/www*, y allí copiar cada archivo en la carpeta correspondiente. La estructura recomendada es la siguiente:

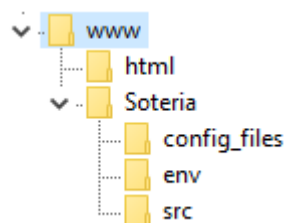


Figura 3-6. Estructura de directorios recomendada.

Comenzando de abajo hacia arriba, la distribución de archivos para cada directorio sería la siguiente:

- js: archivos JavaScript: *cambiarPestanna.js*, *Chart.min.js*, *clock.js*, *jquery.min.js*, *sweetalert.min.js* y *utils.js*.
- img: archivos imágenes e iconos.
- css: archivo de hojas de estilos: *styles.css*.
- default: archivos .html: *banner.html*, *index.html*, *logout.html*, *manage_incident.html*, *new_incident.html* y *nok.html*.

- **src:** archivos Python de programación activa del servidor, de librerías de apoyo, de configuración y de tareas automáticas: *config.py*, *data_valid.py*, *notify.py*, *siem.py*, *Soteria.py* y *Soteria_libs.py*.
- **Soteria:** archivo de configuración de la aplicación Flask *Soteria.wsgi*.

Para las primeras pruebas, se puede utilizar el servidor web propio que integra Flask, insertando en la última línea del archivo Python que desarrolla la parte activa del servidor, el siguiente código:

```
app.run(debug=True,host='0.0.0.0',port=5000)
```

Mediante la dirección `http://localhost:5000` se observa que se puede acceder al servidor web.

En este caso el fichero de configuración que emplea para la aplicación Flask es *config.py*, cuyo contenido puede consultarse en el *Anexo II: Scripts*.

El archivo *Soteria.wsgi* se hace necesario en el caso de utilizar un servidor web distinto al interno que ofrece la propia plataforma Flask. Se trata de un script de configuración que permite cargar una aplicación web a través de un servidor distinto a Flask. En concreto, el archivo utilizado para Soteria contiene el siguiente código de configuración:

```
#!/usr/bin/python
import sys
import logging
logging.basicConfig(stream=sys.stderr)
sys.path.insert(0,"/var/www/Soteria/src")

activate_this = '/var/www/Soteria/src/bin/activate_this.py'
execfile(activate_this, dict(__file__=activate_this))

from Soteria import app as application
application.secret_key = '[REDACTED]'
```

Figura 3-7. Fichero de configuración Soteria.wsgi.

Se ofrece también en el *Anexo II: Scripts*.

Las últimas dos líneas son las que permiten enlazar con la aplicación web desarrollada, contenida en el archivo principal *Soteria.py*. Un detalle importante a destacar es que, en dicho archivo, tendrá que configurarse la misma clave secreta (*application.secret_key*) para que se establezca la comunicación.

Los parámetros fundamentales de este archivo de configuración son:

- `sys.path.insert()`: permite designar la ruta de acceso a los fuentes.
- `activate_this`: indica el archivo para la activación del entorno donde se desarrolla la aplicación Flask.
- Importar la aplicación Flask, denominada `app` y asignar la misma clave secreta.

Por último, se hace necesario incluir una opción a nivel de configuración de la aplicación Flask, de tal manera que se fuerce que las cookies que se puedan intercambiar entre servidor y cliente se hagan siempre de manera segura(cifrada). Para ello se inserta la siguiente línea de código en el archivo Soteria.py, el cual contiene la declaración de la aplicación Flask:

```
app.config['SESSION_COOKIE_SECURE'] = True
```

De esta manera se activa el SECURE FLAG, asegurando que sólo se envían cookies mediante HTTPS.

La configuración y puesta en marcha de *Apache HTTP Server* se expone en el apartado 3.8 *Seguridad*, así como los recursos relativos a seguridad, su despliegue y configuración.

3.7 Acceso mediante computación en la nube.

Cargar la plataforma en la nube ofrece grandes ventajas que merece la pena aprovechar:

- Accesibilidad: la primera ventaja es que facilita en gran medida el desarrollo, ya que para acceder al uso y mantenimiento de la plataforma basta con disponer de acceso a Internet. De esta manera se evita tener que portar máquinas virtuales, o problemas con el control de las versiones.
- Gestión de imágenes: otra gran ventaja es que los proveedores de computación en la nube suelen ofrecer servicios para obtener imágenes rápidas del sistema, lo que permite disponer de backups en caso de que se presente algún inconveniente.
- Tutorización: por último, otra gran ventaja a tener en cuenta es que permite que el tutor pueda acceder e ir comprobando la marcha del desarrollo. De esta manera se evita tener que intercambiar máquinas virtuales o ficheros pesados.

Cabe señalar que la iniciativa para subirlo a la nube se debe, por un lado, a aprovechar las ventajas mencionadas respecto al desarrollo, para disponer de un sistema de backup y recuperación rápido, y para consulta del tutor, así como para la posible prueba durante la defensa del TFM si hubiera tiempo. Como se introdujo en el apartado 1.2 *Motivación*, el objetivo es que la plataforma Soteria se ejecute en una red privada. No obstante, debido a las ventajas que ofrece, merece la pena contar con este recurso durante el desarrollo y las pruebas.

3.7.1 Contratación de un servicio de máquina virtual en la nube

Hay que mencionar, antes de nada, que el autor de este trabajo ya contaba con una instancia EC2 (Elastic Cloud Computing, servicio de máquinas virtuales) de Amazon Web Services (en adelante, AWS), por lo que no se ha hecho necesario contratar nuevos servicios. La opción elegida, no obstante, con respecto al proveedor, hubiera seguido siendo AWS, por experiencia, calidad, oferta de servicios y precios.

Los pasos necesarios para poder disponer de una instancia EC2 en AWS serían:

- Despliegue de una instancia EC2 de AWS y asignación de IP fija.
- Despliegue de la estructura de archivos necesaria: la forma de proceder es idéntica a la vista en el apartado anterior: se crea la estructura de directorios recomendada y se copian los archivos a sus respectivos directorios.
- Instalación de paquetes y librerías de software: la forma de proceder es idéntica a la vista en el apartado anterior: se instala el software necesario que se refleja en la Tabla 3-2.
- Adquisición de un certificado digital para comunicaciones seguras mediante SSL. Este aspecto se desarrolla en el siguiente subapartado, pues se incluye junto con el dominio.
- Configuración segura de Apache2: se expondrá en el capítulo 3.8 *Seguridad*.

A continuación, se detallan dichos pasos, a modo de referencia:

Entrar a la consola de administración de AWS (previo registro) y acceder al servicio EC2 desde el menú Services:

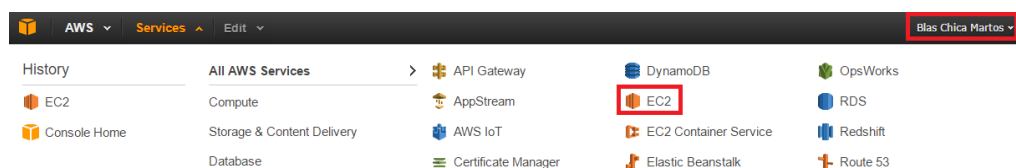


Figura 3-8. Despliegue de una instancia EC2 de AWS (A).

Seleccionar la región Ireland en el menú desplegable superior derecho, a la derecha del nombre de registro, y, a continuación, Launch Instance:

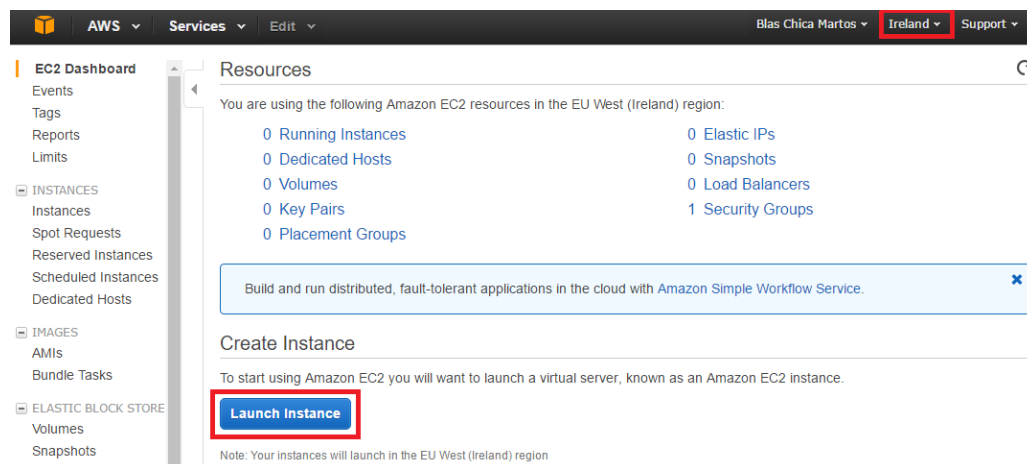


Figura 3-9. Despliegue de una instancia EC2 de AWS (B).

De los sistemas operativos ofrecidos, seleccionar Ubuntu Server 64 bits:

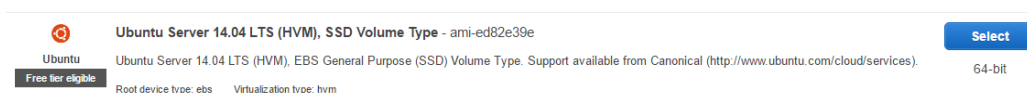


Figura 3-10. Despliegue de una instancia EC2 de AWS (C).

A continuación, seleccionar una imagen de tipo t2.micro, pues ofrece suficiente potencia para lo que se necesita, y se incluye dentro del paquete gratuito el primer año:

	Family	Type	vCPUs	Memory (GiB)
☐	General purpose	t2.nano	1	0.5
☒	General purpose	t2.micro Free tier eligible	1	1

Figura 3-11. Despliegue de una instancia EC2 de AWS (D).

Seguidamente, se ofrecerá un resumen de la configuración elegida, y se recomendará aplicar alguna política de seguridad. Es muy recomendable limitar el acceso a la dirección IP del desarrollador antes de tener garantizada la seguridad del servidor y abrirlo al público (imprescindible antes de tener habilitado HTTPS):

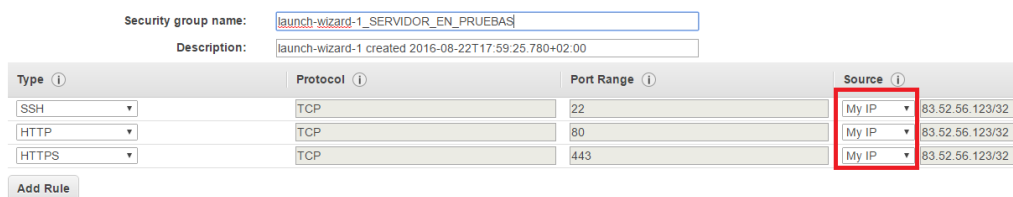


Figura 3-12. Despliegue de una instancia EC2 de AWS (E).

A continuación, seleccionar Launch:

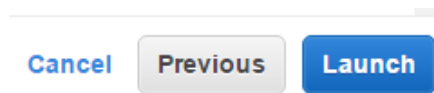


Figura 3-13. Despliegue de una instancia EC2 de AWS (F).

En el siguiente paso se generará una clave privada para poder utilizarla en algún sistema de login remoto seguro (SSH) como PuTTY, por ejemplo. Es imprescindible generar y descargar dicha clave para poder acceder posteriormente a la instancia. Para ello, seleccione “Create a new key pair” e indique un nombre en la casilla siguiente. Seguidamente, seleccione “Download Key Pair”:

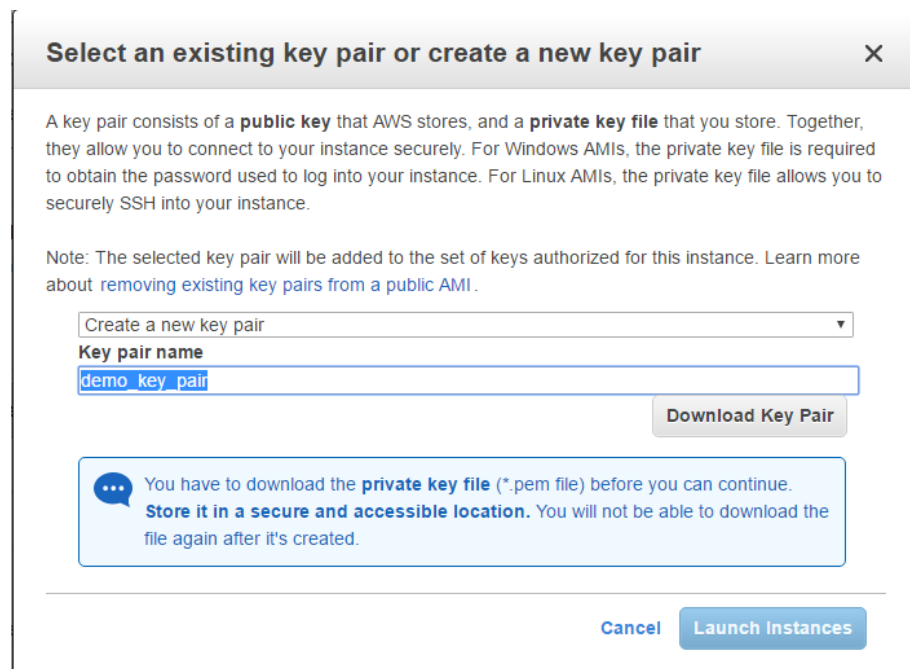


Figura 3-14. Despliegue de una instancia EC2 de AWS (G).

Una vez se asegure de haber descargado el archivo .pem con la clave privada, se puede seleccionar “Launch Instances”.

Una vez pulsado sobre “Launch Instances”, aparecerá una pantalla informándole de que se está generando la instancia. En breve minutos la tendrá disponible para su uso:

Launch Status

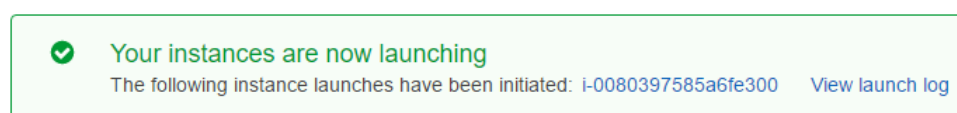


Figura 3-15. Despliegue de una instancia EC2 de AWS (H).

Pasados unos minutos, a través del menú *Services* → *EC2* → *Instances* podrá acceder a la información de la instancia:

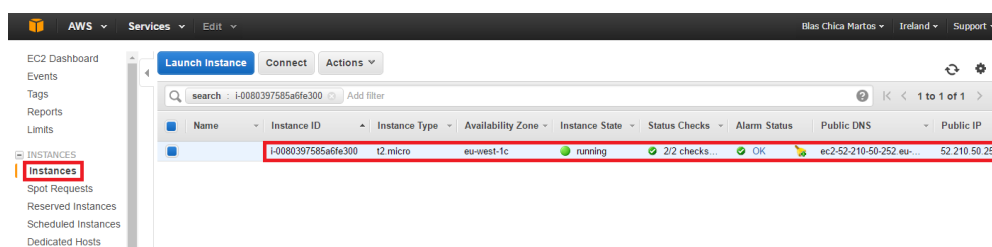


Figura 3-16. Despliegue de una instancia EC2 de AWS (I).

Una vez se dispone de la instancia corriendo, se puede acceder utilizando la clave privada mediante cualquier programa de login remoto seguro que admita SSH. Por facilidad y eficiencia, se recomienda utilizar la herramienta gratuita PuTTY.

De cara a las pruebas iniciales, en este punto ya se debería contar con una máquina virtual funcional, a la que se puede acceder, cargar el software, copiar los archivos del desarrollo, configurar todo convenientemente y poder echar a andar la plataforma Soteria.

Aunque no es imprescindible para los primeros pasos del desarrollo, se recomienda utilizar el servicio *Elastic IP* de AWS, el cual permite asignar una dirección IP fija a la instancia EC2. Será necesario para el siguiente paso cuando se desee adquirir y utilizar un nombre de dominio.

3.7.2 Contratación de un dominio de Internet propio

Para poder acceder de manera ágil y cómoda a la plataforma web desarrollada y cargada en la instancia EC2 de AWS, se hace necesario realizarlo mediante un nombre de dominio. Para ello se requiere contar con algún proveedor que ofrezca la posibilidad de contratar nombres de dominio, o utilizar algún servicio como <https://freedns.afraid.org/> para acceder a subdominios gratuitos.

Para este trabajo se ha aprovechado que el autor ya contaba con servicios contratados a través del proveedor 1&1, ahora 1&1 IONOS (<https://www.ionos.es/>). El servicio de dominios que ofrece este operador presenta la ventaja de incluir un Certificado SSL por cada dominio contratado. Además, los certificados SSL que ofrecen se encuentran firmados por una Autoridad de Certificación, evitando los inconvenientes que presentan algunos navegadores con los certificados autofirmados.

Aprovechando estas circunstancias, se ha contratado el dominio **soteria.es**, accesible una vez configurado convenientemente a través de <https://soteria.es>. Las características del certificado SSL y su configuración se muestran en el siguiente apartado relativo a Seguridad.

Algunas partes de este subapartado están basadas en la referencia [22].

3.8 Seguridad.

Debido al objetivo principal de este trabajo y la información que se manejará, **este apartado supone uno de los núcleos fundamentales del TFM.**

El diseño e implementación de la plataforma debe llevarse a cabo de tal manera que se ofrezcan las siguientes garantías en materia de Seguridad de la Información:

- **Acceso autenticado de usuarios:** se debe garantizar que solo accede el personal de seguridad responsable y habilitado para tareas de gestión de incidentes de seguridad de la información.
- **Confidencialidad:** se debe garantizar la confidencialidad de los datos manejados, habida cuenta de que se manejan datos sensibles, incluidos datos de carácter personal.
- **Cumplimiento de la normativa legal vigente:** ello tiene dos ámbitos:
 - **ENS:** debido al ámbito de aplicación pretendido, se hace necesario cumplir con el ENS, en especial en lo relativo a medidas de protección y notificación al CCN de

aquellas incidencias de Seguridad de la Información que tengan un impacto significativo en la Seguridad de la Información manejada y en los servicios prestados.

- **RGPD:** se deberá tener en cuenta el nuevo Reglamento General de Protección de Datos, en el sentido de que la plataforma maneja datos personales y lo que ello supone en el caso de detectar una fuga de datos y la obligatoriedad de notificar el incidente.

Respecto a la normativa legal vigente y la funcionalidad desarrollada para asegurar su cumplimiento, ya se ha cubierto a lo largo de los subapartados anteriores.

En base a estos preceptos, a lo largo de los siguientes subapartados se desarrollan las medidas de seguridad diseñadas e implementadas de cara a ofrecer dichas garantías.

3.8.1 Acceso autenticado y gestión de usuarios

El objetivo principal es garantizar que solo acceden usuarios legítimos y habilitados para la gestión de incidentes de seguridad de la información de la organización.

En una primera aproximación, se valoró la posibilidad de implementar un sistema de autenticación basado en el protocolo *Open Authorization (OAuth)* [14], el cual permite compartir de manera segura información parcial (en este caso de autenticación) de la cuenta alojada en un proveedor del estilo de Google, Facebook, Microsoft, Twitter o LinkedIn. Este sistema se puede complementar con el registro y verificación de la cuenta de correo electrónico utilizada para la autenticación, por ejemplo. Es un sistema relativamente sencillo de implementar y seguro si se trabajan todas las conexiones sobre HTTPS. Ya se ha utilizado previamente para otros desarrollos, y hay que reconocer que es un esquema que funciona bien para la mayoría de sistemas web con acceso público, de hecho, es muy habitual verlo en la actualidad en los apartados de login de numerosas páginas web y organizaciones. El problema principal que presenta este esquema es precisamente el acceso público: su funcionamiento requiere el acceso a un proveedor externo, lógicamente, a través de Internet, lo cual puede ser un gran impedimento para ciertos entornos de trabajo. La pretensión de este trabajo es que pueda ser utilizado en un entorno de información clasificada, ya sea a nivel de la Administración General del Estado, o bien, en concreto, en el ámbito del Ministerio de Defensa. Estos sistemas suelen estar dotados de fuertes medidas de seguridad y, entre las restricciones más habituales, se encuentra que deben ser sistemas corporativos aislados, redes cerradas, sin conexión a redes abiertas (Internet).

Como solución alternativa, se ha diseñado un sistema que permite la autenticación desde la propia red interna de la organización. Para ello se implementa un sistema de doble factor de autenticación, donde se requiere del usuario que pretende acceder la siguiente información:

- **Autenticación mediante contraseña:** cada cuenta de usuario se encuentra protegida por contraseña, por lo que se requerirá en primer lugar que el usuario se autentique introduciendo el nombre de su cuenta y la contraseña correspondiente. En este caso, se utiliza el sistema de web login integrado en el propio servidor web de Apache. Utilizar este sistema y configurarlo desde el apartado *VirtualHost* de Apache (en secciones *<Directory>*), hace más ágil la navegación, ya que evita tener que comprobar que el usuario que accede es válido para cada uno de los recursos solicitados al servidor. Ello se debe a que permite definir directivas de configuración para cada directorio (con sus respectivos subdirectorios), es decir, comunes para todos los recursos accesibles del site web. Se configura mediante la directiva *AuthType* [23]. Conviene aclarar que existen dos métodos: el mencionado mediante configuración de secciones *<Directory>*, y mediante ficheros *.htaccess* [24]. Se recomienda encarecidamente emplear el primer método, ya que emplear *.htaccess* puede ralentizar en gran medida el servidor web, ya que supone el acceso al fichero con las credenciales para cada recurso solicitado.

- **Autenticación mediante un segundo factor:** en esta ocasión se ha elegido autenticación mediante la introducción de un PIN de 6 dígitos a través de la herramienta Google Authenticator, y utilizando un algoritmo de generación de números PIN basado en tiempo. Además, se configurará de tal manera que solo admita la introducción de un número PIN válido en cada ciclo de generación de un nuevo código PIN, es decir, cada 30 segundos. De esta manera se evitarán ataques de repetición basados en las técnicas de Man-In-The-Middle. Este sistema también se integra a través del fichero de configuración de Apache, en el apartado *VirtualHost*.

La siguiente figura recoge el esquema del sistema de autenticación diseñado e implementado para este desarrollo:

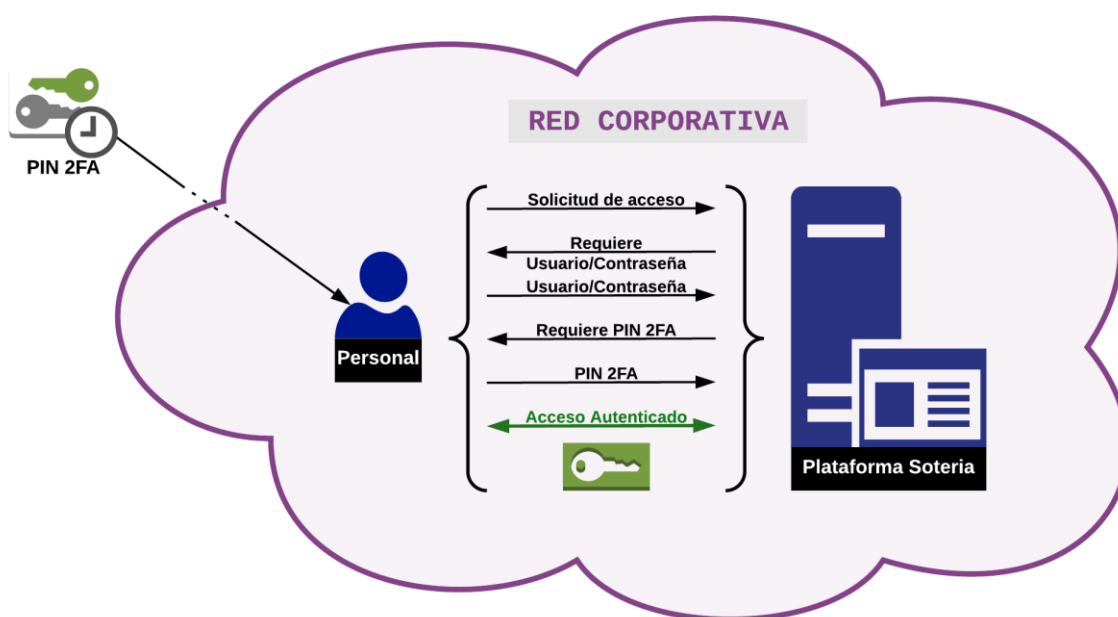


Figura 3-17. Esquema de Autenticación.

Este esquema permite establecer un sistema de autenticación de doble factor muy eficiente y seguro. Además, se evita el acceso al exterior de la red corporativa.

Según la clasificación del sistema y las restricciones que se impongan, se podría dar el caso de que se admita acceso remoto seguro vía VPN. Esta funcionalidad se ofrece, por ejemplo, en la red de acceso de propósito general WAN-PG del MINISDEF, la cual ofrece la posibilidad de acceder a la Extranet de la WAN-PG de manera remota mediante autenticación vía tarjeta electrónica del MINISDEF, empleando sistema de criptografía de clave pública (PKI), y autenticación de usuario mediante contraseña. En el caso de que la plataforma Soteria se incluyera en el catálogo de servicios accesible vía Extranet, el personal de seguridad podría acceder de manera remota y segura desde cualquier punto con acceso a Internet.

Como medida de seguridad adicional, se evitará ofrecer cualquier tipo de información de la plataforma web de manera pública. Hay que tener en cuenta que se trata de una herramienta de gestión específica de seguridad, cuyo acceso debe estar restringido al personal responsable, por lo que no tiene sentido, ni sería recomendable, ofrecer una cara pública de la aplicación web. Para conseguir este objetivo, se ha implementado el sistema de autenticación de tal manera que cuando se intenta acceder por primera vez a la plataforma se exige, en primer lugar, la autenticación del usuario. **Mientras no se produzca una autenticación exitosa de un usuario permitido, no se tiene acceso a los recursos de la plataforma.** De esta manera, al intentar acceder lo primero que aparece es una ventana de petición

de datos de autenticación mediante nombre de usuario y contraseña. Al final del presente apartado se pueden observar las distintas capturas de pantalla para el acceso a la plataforma.

Además de dificultar la tarea a los posibles atacantes, este sistema de doble factor de autenticación presenta una gran ventaja: como se sabe, la autenticación habitual mediante usuario y contraseña tiene el riesgo de mantener los datos de la sesión en local, a través en este caso del navegador cliente. Esto hace que no sea posible, debido a cómo funciona el protocolo HTTP (sin estado) y a que es el navegador es el que cachea las credenciales, controlar el logout de manera programática, ya sea desde el servidor, o incluso desde el lado del cliente (insertando código JavaScript, por ejemplo). De hecho, conforme se han ido actualizando los navegadores web clientes, en la actualidad ni siquiera admiten utilizar métodos alternativos como puede ser el intentar autenticarse con un usuario tipo *dummy* (usuario no real sin acceso a recursos del servidor) del tipo *logout:logout_password*. Si se sigue el enlace ofrecido en la referencia [25], se bucea detenidamente en <https://stackoverflow.com> (sin duda, la mejor fuente para intentar resolver problemas de tipo programático), o se buscan cadenas como “logout basic http authentication”, “htaccess logout”, etcétera, se observará que la mayoría de soluciones propuestas son intentos no formales de dar solución al problema, pero formalmente este problema no tiene solución. Las soluciones no formales propuestas, algunas muy imaginativas como la expuesta anteriormente de intentar volver a loguearse con un usuario tipo dummy, solo funcionan con algunas versiones antiguas de determinados navegadores. Después de probar gran cantidad de soluciones de este tipo, se puede concluir que no existe una solución formal, válida y universal (válida para todos los navegadores) para este problema. Aquí es donde la autenticación mediante el segundo factor (Google Authenticator) aporta una gran ventaja adicional, ya que soluciona este problema: en este caso, no se guarda la cookie de sesión en local, sino que se almacena en el servidor. Ello ofrece dos medidas adicionales de seguridad: por un lado, atacar e intentar acceder a un servidor suele ser más complejo y costoso que el ataque a un cliente (no reviste gran dificultad acceder a las cookies de los clientes). Por otro lado, permite que se pueda controlar la gestión del acceso desde el servidor. Esto es útil y necesario, tal como se ha expuesto, de cara a realizar el logout (desautenticación) segura del usuario, de tal manera que, una vez haya salido el usuario, si intenta volver a acceder, aunque el navegador no requiera de nuevo el usuario y contraseña al quedar guardados en local, sí es necesario superar de nuevo el segundo factor de autenticación, es decir, en este caso, volver a introducir un PIN válido del sistema Google Authenticator para dicha cuenta. Con ello se soluciona el problema de las cookies locales controladas por el navegador cliente, y la imposibilidad de realizar formalmente un desautenticación utilizando el método de web login integrado en Apache. En cualquier caso, siempre se recomienda, y así se indica en el proceso de desautenticación, borrar los datos de navegación (que incluye las cookies) o, al menos, cerrar el navegador, tras realizar el logout de la plataforma. De esta manera se obliga a superar de nuevo los dos factores de autenticación.

En resumen, si el usuario seleccionó el botón de  **Salir** desautenticación para volver a acceder requiere autenticarse de nuevo. Si el usuario salió correctamente y siguió las recomendaciones de seguridad, tendrá que volver a autenticarse mediante ambos factores: usuario y contraseña + el PIN de Google Authenticator. En caso contrario, tendrá que introducir solamente el PIN. **En cualquier caso, se impide el acceso directo a la sesión sin autenticarse de nuevo mediante algún método.**

El diseño del sistema de autenticación impide, además, cruzar las cuentas de los usuarios, es decir, si un usuario ha realizado logout, solo el mismo usuario puede volver a entrar insertando el PIN correspondiente a su cuenta. No se acepta como válido un PIN correspondiente a otra cuenta.

Recordar, además, como norma general, nunca guardar las credenciales en local cuando lo solicite el navegador.

Por último, se incorpora también una medida de seguridad en relación a un problema habitual en los navegadores web: el botón de retroceso. De no controlarse bien, un atacante podría volver a tener acceso a los recursos de la plataforma web. Para evitarlo, se incluye código JavaScript gracias al cual

se impide volver a la página principal de la plataforma (o cualquier página web de la plataforma desde la que se seleccionó salir).

Para la gestión de las cuentas de usuario existirá una máquina aislada y dedicada. Esta máquina tendrá el tratamiento de información clasificada de alto grado de seguridad, con las medidas de protección que ello supone: solo podrá utilizarse en una sala de seguridad, se custodiará en un armario de seguridad (con la certificación adecuada), se restringirá el acceso al personal responsable de la gestión de cuentas de los usuarios de seguridad, y solo dispondrá de conectividad con unidades USB controladas (filtradas por número de serie) a través de un único puerto USB habilitado. Albergará el software mínimo imprescindible para la gestión de cuentas y el bastionado del equipo.

El proceso de alta de nuevo usuario se realizará de la siguiente manera:

- **Primer paso:** el primer paso será generar la cuenta según el nombre de usuario del nuevo personal incorporado, según el formato estándar previsto: 3 primeros caracteres del nombre y apellidos respectivamente, 9 caracteres en total. Estas cuentas, son importantes ya que permitirán recuperar la cuenta de Google Authenticator en el caso de que ocurra algún inconveniente (las credenciales se registran en el fichero oculto `.google_authenticator` de la carpeta personal de cada usuario). Por seguridad, dichos ficheros también se copiarán en la carpeta `/home/users/"nuevo usuario"` correspondiente a cada usuario.

La generación de la cuenta se realizará mediante el comando en la consola de linux: `sudo adduser "nuevo usuario"`, siguiendo las indicaciones expuestas a continuación:

- a) password: igual al nombre de usuario.
- b) volver a insertar la password.
- c) Full Name: indicar el nombre completo de la persona.
- d) Room Number: número de oficina donde tiene el puesto de trabajo, si tuviera asignado número.
- e) Work Phone: número de contacto corporativo.
- f) Home Phone: número de contacto personal (opcional).
- g) Other: se utilizará para indicar el cargo/puesto que ocupa en la organización.
- h) Verificar la información y confirmar introduciendo "Y".

Dependiendo de la versión instalada del SO Linux (ES/EN) estas entradas aparecerán en inglés o en español, pero el sentido de cada entrada es el mismo.

Se le requerirá al usuario la introducción de una contraseña (clave personal maestra), con las siguientes restricciones:

- ✓ Longitud mínima: 12 caracteres.
- ✓ Presencia obligada de caracteres alfanuméricos.
- ✓ Mínimo un carácter alfabético en mayúscula.
- ✓ Mínimo un carácter especial.

De esta manera se controlará que la clave cuente con suficiente robustez, una medida de seguridad fundamental. Se deja a criterio de la organización que implemente este sistema la **frecuencia** que establezca **de actualización de las contraseñas**. Este es otro factor clave, pues una baja frecuencia es inherentemente peligrosa, pero una elevada frecuencia puede interferir de manera excesiva en la comodidad de los usuarios, pudiendo tener también sus riesgos al intentar evitar dicha dificultad: anotación de contraseñas en lugares poco seguros, adopción de patrones a la hora de seleccionar la contraseña, etc.

Ésta será también la **clave maestra del usuario** para la autenticación mediante usuario y contraseña web login en la plataforma web, por lo que debe recordarla, no compartirla y no anotarla en ningún lugar que no ofrezca un nivel adecuado de seguridad.

A continuación, se ingresa con la cuenta de dicho usuario y se accede a su carpeta personal mediante los siguientes comandos:

- a) *sudo su "nuevo usuario"* (solicita de nuevo la contraseña del usuario).
- b) *cd /home/"nuevo usuario"*

• **Segundo paso:** el siguiente paso es generar la clave secreta y el código QR correspondiente mediante la herramienta Google Authenticator: ejecutando el comando *google-authenticator*.

Las opciones a seleccionar durante la ejecución de *google-authenticator* serán:

- a) Autenticación mediante tokens generados en base al tiempo: por tanto, se seleccionará la opción "y". En cuanto se introduce la respuesta ("y"), se puede observar que se ofrece la nueva clave secreta y el código QR correspondiente para Google Authenticator. Aunque se puede hacer posteriormente, **se recomienda en este punto que el usuario escanee el código QR para agregar la nueva cuenta a su aplicación cliente de Google Authenticator en el móvil**. Por otro lado, se recomienda que el personal encargado de gestionar el alta del usuario capture el código QR, junto con la clave secreta, y los guarde en la carpeta personal del usuario. Ello sería útil en caso de necesitar de nuevo configurar el acceso en la aplicación cliente. Como medida adicional de seguridad, estos archivos no deberían salir del ordenador aislado de gestión de usuarios, y debería quedar bajo la custodia del personal responsable de la gestión de usuarios.
- b) Actualizar el fichero *.google_authenticator* personal del nuevo usuario. Por tanto, se seleccionará la opción "y".
- c) Limitamos la repetición en tiempo de la autenticación consecutiva (cada 30 segundos), ya que **solo se permite un intento de acceso por cada nuevo token generado**. Ello mejora la seguridad al reducir la probabilidad de éxito de ataques de tipo Man-In-The-Middle mediante repetición. Requiere mantener sincronizados la aplicación cliente y la aplicación instalada en el servidor web, eso sí. Por tanto, se seleccionará la opción "y".
- d) En esta opción se da la posibilidad del uso de un token anterior y un token posterior al actual, es decir, el usuario podría conseguir autenticarse empleando alguno de 3 tokens posibles. Esta opción iría en contra de la restricción anterior. Además, 30 segundos es margen suficiente para la sincronización entre la herramienta cliente Google Authenticator del usuario y la herramienta Google Authenticator instalada en el servidor web. Normalmente la desincronización suele ser de pocos segundos, además desde la herramienta cliente se permite al usuario volver a sincronizar de manera sencilla la base de tiempos (*Configuración / Corrección de la hora en códigos*). Por tanto, se seleccionará la opción "n".
- e) Limitar intentos de acceso a un máximo de 3 por cada 30 segundos. Realmente esta opción ya está recogida en la opción c): donde, de hecho, se limitaba a 1 intento cada 30 segundos (por cada generación de nuevo token). Por tanto, realmente no sería necesaria. En cualquier caso, se seleccionará la opción "y".

En el caso de que no se haya realizado tras el paso a), es fundamental no olvidar que **el usuario debe registrar el acceso en la aplicación cliente Google Authenticator del**

móvil, ya sea introduciendo manualmente la clave secreta, o bien escaneando el código QR correspondiente.

- **Tercer Paso:** solo si no se ha realizado en el punto anterior: a través del código QR generado en el punto anterior y teniendo previamente instalada la herramienta gratuita Google Authenticator en un teléfono móvil, el usuario añadirá el sistema de generación de códigos pin de 6 dígitos, basado en tiempo, escaneando dicho código QR de manera visual. Si fuera necesario, como alternativa se podría realizar introduciendo de manera manual la clave secreta asociada al código QR, pero preferiblemente se realizará escaneando el código.

Por otro lado, es también recomendable en este momento que el personal responsable de la gestión de cuentas capture la pantalla y registre el código QR. Ello permitirá salvaguardar en el sistema las credenciales de los usuarios, tanto en texto como gráficamente. Para ello, llegado el momento, es tan sencillo como pulsar el botón de “Imprimir Pantalla” desde el teclado, tratando de que se capture correctamente la zona del código QR y, a ser posible, también la clave secreta, la cual aparece justo debajo del código. Cuando aparezca la ventana con la captura para guardar el archivo, guardarlo en la carpeta de nueva creación `/home/users/“nuevo usuario”`. Si se planteasen problemas de permisos de acceso a dicha carpeta, se puede guardar temporalmente en otra carpeta con acceso, e inmediatamente moverla desde la línea de comandos a la carpeta correspondiente.

A continuación, se muestra una captura de ejemplo de código QR durante el proceso de gestión de alta de nuevo usuario:



Figura 3-18. Código QR y Clave Secreta Google Authenticator de una cuenta de usuario.

- **Cuarto Paso:** el cuarto paso consiste en generar las credenciales del usuario para incorporarlo al archivo `apache_credentials`. El contenido de este archivo es el que se emplea para la autenticación mediante usuario y contraseña web login. Dichas credenciales y su incorporación al fichero mencionado se realizan mediante la herramienta `htdigest`. Como es lógico y por motivos de seguridad, lo que se incorpora al fichero es el hash de la contraseña, nunca la contraseña en claro. El formato del comando es el siguiente:

htdigest “PATH apache_credentials” “server” “user”

Es decir, como parámetros se indican: la ruta al fichero `apache_credentials`, el nombre del servidor (en el caso de este trabajo: `soteria.es`), y el nombre del nuevo usuario.

Se requerirá al usuario de nuevo la introducción de la contraseña, por duplicado.

- **Quinto Paso:** en el siguiente paso se registra el token, añadiéndolo al fichero de credenciales *tokens.json*. Se utilizará para el segundo factor de autenticación, es decir, para la solicitud de un PIN válido. Al igual que el fichero *apache_credentials*, se trata de un fichero localizado en la carpeta de la herramienta *Apache_2FA*. El proceso en este caso se realiza de manera manual, editando y añadiendo las credenciales correspondientes al fichero. El formato de cada entrada en el fichero es el siguiente:

“nuevo usuario”: “clave secreta Google Authenticator”

Es decir, es tan sencillo como indicar el nombre del nuevo usuario y la clave secreta mostrada al ejecutar la herramienta *google-authenticator* del Segundo Paso (aparece justo debajo del código QR a escanear).

- **Sexto Paso:** como último paso para el registro y alta del usuario, el personal responsable de la gestión de cuentas de usuarios de seguridad registrará el nuevo nombre de usuario y sus credenciales para web login y Google Authenticator en la máquina que alberga el servidor web de acceso a la plataforma de gestión de incidentes de seguridad de la información. Para ello, se añadirán las credenciales correspondientes al nuevo usuario en los archivos *apache_credentials* y *tokens.json* de la carpeta donde se haya instalado la herramienta *Apache_2FA* en el servidor. La instalación y configuración de las herramientas necesarias, así como los ficheros que se manejan, se detallan en el *Anexo III: Instalación del software esencial*.

Para facilitar la gestión del alta de nuevos usuarios, **se ha desarrollado el script para shell de Linux *set_new_user.sh*, el cual automatiza todo el proceso de gestión del alta de manera continua**, así como actualiza los ficheros de credenciales correspondientes. De esta manera, al personal responsable de la gestión de cuentas solo le resta copiar los archivos *apache_credentials* y *tokens.json* al servidor que alberga la plataforma web. El contenido de dicho script también se puede localizar en el *Anexo II: Scripts*.

Para las pruebas de verificación de este trabajo, la máquina que alberga el servidor y la máquina desde la que se gestionan las cuentas coinciden, por lo que con la ejecución del script shell desarrollado se completa el proceso de alta. Queda en manos de la organización que implemente este sistema establecer un procedimiento para ingresar de forma segura las credenciales de los usuarios en el servidor (normalmente se realiza a través de un ordenador Aduana*).

Este proceso se exigirá para todo aquel personal responsable de la seguridad de la información de la organización, incluido el personal responsable de la gestión de cuentas.

A lo largo de todo este proceso se puede apreciar un detalle importante: aunque alguna información de autenticación puede ser de carácter personal y se tiende a pensar que debe estar en posesión del usuario, como se sabe, el factor humano es el eslabón más débil en toda la cadena de seguridad (defensa en profundidad). El hecho de que determinada información se mantenga custodiada en los sistemas centrales de la organización reduce significativamente la posibilidad de filtración de información de autenticación y, en definitiva, reduce los problemas de seguridad asociados. Además, el que dicha información se custodie en la organización obliga al usuario a depender de ella y notificar cualquier incidente que pudiera haber. Por contra, si se ofrece al usuario toda la información personal para restaurar la autenticación por sí mismo, se podría dar el caso de que el propio usuario intente solventar un incidente, como puede ser la filtración del código QR, de la clave secreta, o la pérdida/robo del móvil. Normalmente y en la inmensa mayoría de los casos, **el usuario en estas circunstancias tendería a ocultar el incidente, sin que haya por tanto registro de la incidencia** en la organización, ni se puedan tomar las medidas de seguridad que correspondan, o añadir a la base de conocimiento. En resumen, va en detrimento de la seguridad de la organización. Habrá que extremar, por tanto, la precaución a la hora de la protección del factor humano. Por todo ello es por lo que se

registran las credenciales de Google Authenticator de los usuarios, y se custodian en el ordenador aislado de gestión de cuentas.

Por otro lado, y aunque el proceso así detallado parece extenso, una vez automatizado por el personal responsable de la gestión de cuentas, no debería llevar más de 5-10 minutos de reloj por cada nuevo proceso de alta. Tiempo asumible teniendo en cuenta el nivel de seguridad que se ofrece. **Con el script desarrollado para automatizar el proceso de alta de un nuevo usuario, la secuencia apenas lleva 3 minutos de reloj.** No se incluye la transferencia segura de credenciales al servidor web, pues dependerá del procedimiento establecido.

Respecto a la autenticación de los usuarios en la plataforma web, el proceso se dividirá en dos pasos de fácil manejo, cada uno correspondiente a un factor de autenticación diferente:

- **Primer Paso:** acceso a la plataforma Soteria a través de la dirección IP o dominio del servidor web. Si el acceso se realiza desde dentro de la red corporativa, se podría acceder mediante una dirección IP privada fija. Para las pruebas de este trabajo, se ha adquirido un dominio de acceso público, por lo que se puede acceder mediante la URL: <https://soteria.es>.

Tal como se expuso al comienzo del presente apartado, por seguridad, no se puede acceder a los recursos de la plataforma hasta no haberse autenticado en el sistema, por lo que lo primero que se presenta es la ventana para la autenticación mediante usuario y contraseña:

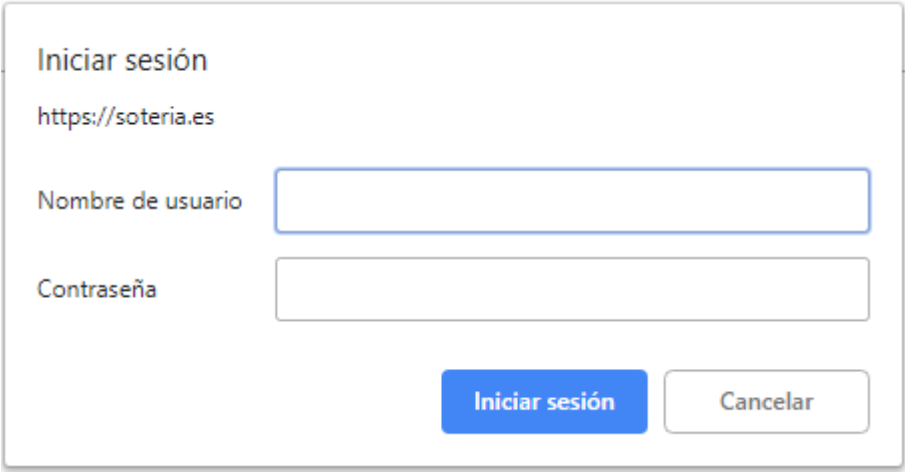
El formulario de inicio de sesión tiene un título "Iniciar sesión" en azul. Debajo, se muestra la URL "https://soteria.es". Hay dos campos de entrada: "Nombre de usuario" y "Contraseña", ambos con bordes azules. En la parte inferior derecha, hay dos botones: "Iniciar sesión" (azul) y "Cancelar" (gris).

Figura 3-19. Autenticación mediante usuario y contraseña.

- **Segundo Paso:** autenticación mediante PIN. Una vez superada la autenticación mediante usuario y contraseña, se solicita al usuario el segundo factor de autenticación, en este caso, el PIN (token) de 6 dígitos de Google Authenticator correspondiente a su cuenta:

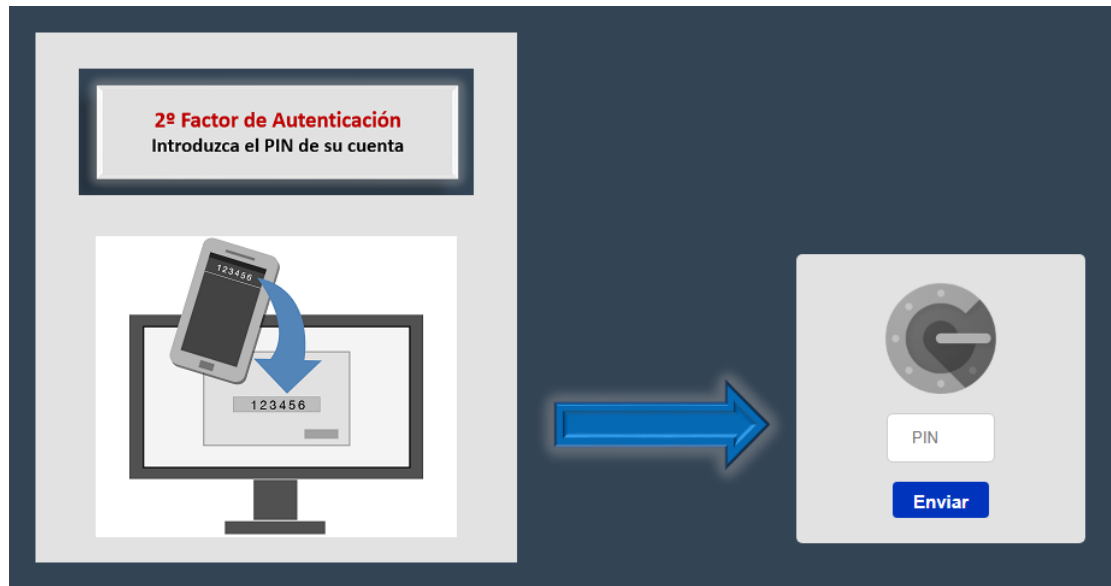


Figura 3-20. Autenticación mediante PIN.

El usuario que pretende acceder deberá extraer dicho dato de su aplicación cliente Google Authenticator instalada en el móvil.

Solo en el caso de haber superado ambos retos de autenticación, se tendrá acceso a la interfaz web general de la plataforma:



Figura 3-21. Usuario autenticado.

Sobre la esquina superior derecha de la interfaz, además del botón para salir del aplicativo, se mostrará en todo momento el nombre del usuario autenticado, lo cual es un factor importante de cada a la trazabilidad, tanto en el uso de los servicios, como en el acceso a los datos.

3.8.2 Confidencialidad

Asegurar la confidencialidad en la plataforma Soteria es uno de los pilares fundamentales para su seguridad y para el desempeño operacional de la misma. Por ello se hace necesario contar con algún sistema que asegure la confidencialidad en el acceso.

Debido a que el acceso a los servicios se realiza vía web, la forma de asegurar dicho acceso en este caso consiste en emplear el protocolo HTTPS y el uso de un certificado de seguridad SSL.

Respecto al certificado digital, se trata de la prueba que necesitan los clientes que se conecten al servidor de cara a poder establecer una confianza con el mismo e intercambiar datos de manera segura, ya que demuestra la autenticidad del servidor.

Existen dos versiones:

- Certificado digital firmado por una Autoridad de Certificación (CA).
- Certificado digital autofirmado.

Cada una de las versiones tiene sus ventajas y sus inconvenientes. La principal ventaja de un certificado firmado por CA es que ya se encuentra avalado por una CA, especialmente si se trata de una CA de reconocido prestigio. La ventaja del certificado autofirmado es que no precisa del acceso a una CA por parte del cliente en el proceso de negociación de la conexión segura, evitando además ataques del tipo Man In The Middle (MITM). La desventaja de los certificados autofirmados es que no se encuentran avalados por una CA, por lo que algunos navegadores muestran un aviso de advertencia al cliente, incluso pueden negar el acceso como acción predeterminada, como ocurre con Mozilla Firefox.

Cuando se planteó qué hacer sobre el asunto, se analizó los pros y los contras de cada versión. Salvando el problema del posible ataque MITM, resuelto mediante el certificado intermedio (ofrece al cliente durante la negociación de la conexión segura la ruta a la CA que valida el certificado digital del servidor), la opción más segura y fiable, especialmente de cara a facilitar la experiencia a los usuarios, es la de contar con un certificado firmado por CA. El problema que planteaba esta opción era el coste relativamente elevado que suponía adquirir un certificado, si se realiza la compra de manera aislada. Como se introdujo en el subapartado 3.7.2 *Contratación de un dominio de Internet propio*, la adquisición del dominio para el servidor web, soteria.es, incluía el poder expedir y utilizar un certificado SSL. Por lo que la adquisición resolvió ambas necesidades al mismo tiempo: contar con un nombre de dominio, y contar con un certificado digital. El certificado en este caso se encuentra firmado por DigiCert (<https://www.digicert.com/es/>):

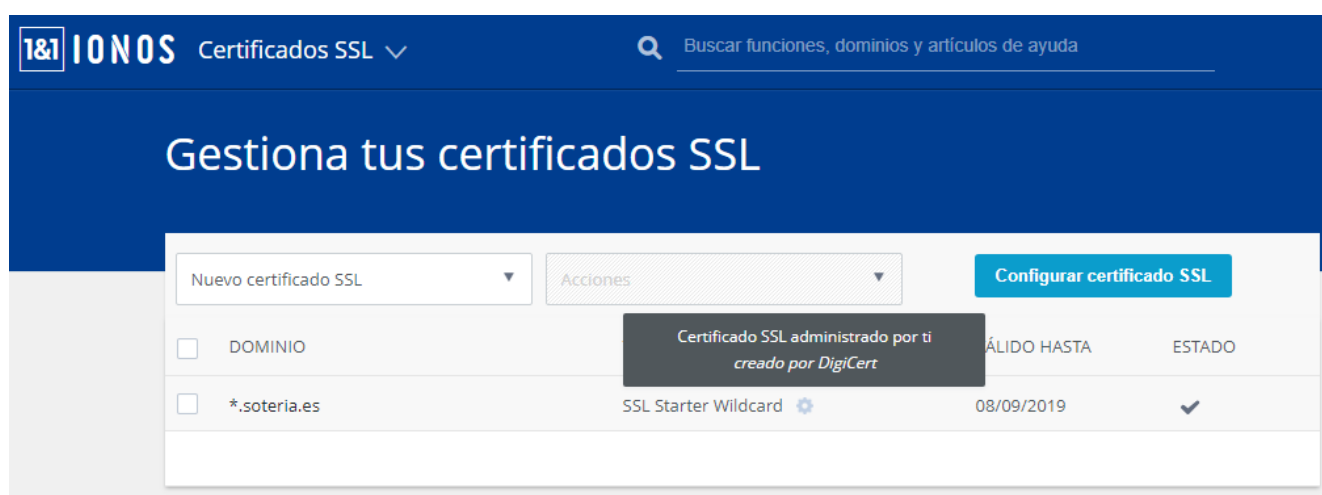


Figura 3-22. Certificado SSL asociado al dominio soteria.es.

El certificado consta de tres archivos:

- Archivo con la clave privada: *soteria.es_private_key.key*.
- Certificado en sí, o clave pública del servidor: *soteria.es_ssl_certificate.cer*.
- Certificado intermedio: *soteria.es_ssl_certificate_INTERMEDIATE.cer*.

Dicho todo esto, insistir en que se ha implementado y elegido esta opción para facilitar el desarrollo y la comprobación del funcionamiento de la plataforma mediante acceso público. **En el caso pretendido de que se aplique sobre una red privada, la solución pasaría irremediablemente por emitir y utilizar un certificado autofirmado.** La confianza en este caso residiría en que se trata de un acceso de ámbito cerrado, por lo que no se precisa la verificación por parte de un tercero (CA).

Respecto a la configuración y habilitación del acceso HTTPS en Apache2, precisa, por un lado, tener disponible el módulo `mod_ssl`, el cual permite al servidor encriptar las comunicaciones. Para activar dicho módulo se puede ejecutar la siguiente orden desde la consola:

```
sudo a2enmod ssl
```

Por otro lado, se precisa realizar la configuración mediante el archivo `.conf` correspondiente. Apache2 ofrece un archivo de configuración por defecto denominado `default-ssl.conf`, el cual puede encontrarse en la ruta `/etc/apache2/sites-available/`. Antes de realizar ningún cambio, conviene realizar una copia de dicho archivo y asignarle el nombre de dominio del servidor, en el caso de este trabajo:

```
cd /etc/apache2/sites-available
sudo cp default-ssl.conf soteria.es-ssl.conf
```

A continuación, ya puede editarse el archivo mediante `nano`, por ejemplo:

```
sudo nano soteria.es-ssl.conf
```

Apache2 utiliza lo que denomina *Virtual Hosts* para la configuración de los accesos. Con ello se refiere a la configuración para los distintos servicios, o, lo que es lo mismo, para el acceso a los distintos puertos. En el caso de HTTPS, el puerto utilizado es el 443, de ahí que la primera entrada del archivo que se observe sea `<VirtualHost _default_:443>`. Observar, así mismo, como antes se comprueba la presencia del módulo de seguridad `mod_ssl` en el sistema: `<IfModule mod_ssl.c>`.

Lo que interesa editar en concreto del archivo `soteria.es-ssl.conf` son las siguientes entradas:

- `ServerName`: se refiere al nombre de dominio del servidor, por lo que se insertará:

```
ServerName soteria.es
```
- `ServerAlias`: se refiere a una segunda denominación para el nombre de dominio del servidor, normalmente agregando `www.` al inicio:

```
ServerAlias www.soteria.es
```

- `ServerAdmin`: contacto con el administrador de la página web:

```
ServerAdmin bchimar@outlook.es
```
- `WSGIScriptAlias`: se trata del acceso al archivo de configuración `.wsgi`, expuesto en el subapartado 3.6 *Integración y puesta en marcha de la plataforma web*:

```
WSGIScriptAlias / /var/www/soteria/soteria.wsgi
```

- `Directory`: indica la ruta a la carpeta de archivos fuente de la página web:

```
<Directory /var/www/soteria/src>
```

```
Require all granted
```

```
</Directory>
```

La entrada `Require all granted`, indica que no se realice filtrado por dirección IP, es decir, se permite el acceso desde cualquier dirección.

- **SSLProtocol:** mediante esta entrada se especifican los protocolos SSL habilitados. Esta parte es fundamental de cara a la seguridad, ya que, por ejemplo, las versiones 2 y 3 del protocolo SSL es de conocimiento público que en la actualidad son inseguras, por lo que se deshabilitan:

SSLProtocol All -SSLv2 -SSLv3

- **SSLHonorCipherOrder:** si se establece a on, permite que sea el servidor el que seleccione el cifrador durante la negociación de la conexión segura, en lugar de dejarlo en manos del cliente. De esta manera se asegura poder elegir un cifrador robusto, que no presente debilidades publicadas:

SSLHonorCipherOrder on

- **SSLCipherSuite:** permite indicar el conjunto de cifradores disponibles para utilizar en la negociación de las conexiones seguras. En este caso se han insertado los cifradores recomendados desde: <https://www.ssllabs.com>.

- **SSLCertificateFile:** indica la ruta al archivo que contiene el certificado digital del servidor web:

/etc/ssl/certs/soteria.es_ssl_certificate.cer

- **SSLCertificateKeyFile:** indica la ruta al archivo que contiene la clave privada asociada al certificado digital. Imprescindible para que el servidor se pueda autenticar ante la Autoridad de Certificación (CA) a la hora de validar el certificado:

/etc/ssl/private/soteria.es_private_key.key

- **SSLCertificateChainFile:** indica la ruta al archivo que contiene el certificado intermedio:

/etc/ssl/certs/soteria.es_ssl_certificate_INTERMEDIATE.cer

Los tres archivos relativos al certificado deben ser copiados en los directorios correspondientes según configuración del servidor Apache2:

- Certificado digital en /etc/ssl/certs/.
- Clave privada en /etc/ssl/private/.
- Certificado intermedio en /etc/ssl/certs/.

Una entrada adicional, pero importante desde el punto de vista de la seguridad, es activar la opción HSTS: HTTP Strict Transport Security. Una vez que se habilite el acceso mediante HTTPS (puerto 443), el acceso vía HTTP (80) quedará deshabilitado. Para posibilitar que los usuarios que hayan indicado en el navegador *http://...*, en lugar de *https://...*, puedan seguir accediendo, se precisa, o bien realizar una redirección, o bien activar la opción HSTS. La segunda opción es la más recomendada. Para ello, basta añadir la siguiente entrada a la configuración del Virtual Host que se acaba de editar:

Header always set Strict-Transport-Security "max-age=94608000; includeSubDomains"

Básicamente, la opción HSTS indica al navegador del cliente que accede, que las comunicaciones se realizarán de manera segura sobre HTTPS, y que no se intercambiarán datos mediante HTTP. Mediante la opción “*max-age*” se indica el periodo, en segundos, que tendrá vigencia la opción HSTS. Se recomienda indicar un valor elevado. En este caso se asignan 3 años de duración.

Ya sólo queda reiniciar el servidor Apache2:

sudo service apache2 reload

sudo service apache2 restart

Mediante *reload* se comprueba y carga la nueva configuración, y mediante *restart* se reinicia el servidor.

Con todo ello, ya se tendría configurado el servidor Apache2 para utilizar el acceso mediante HTTPS. Se puede probar introduciendo en la barra de direcciones del navegador <https://soteria.es>, o simplemente soteria.es.

Una vez aplicadas las medidas de seguridad y con el servidor en marcha, se puede utilizar algún servicio que analice el grado de seguridad que ofrece el sistema.

En esta ocasión se ha empleado la herramienta de análisis de seguridad disponible de manera gratuita a través de la dirección <https://www.ssllabs.com/ssltest/>. El resultado es el siguiente:

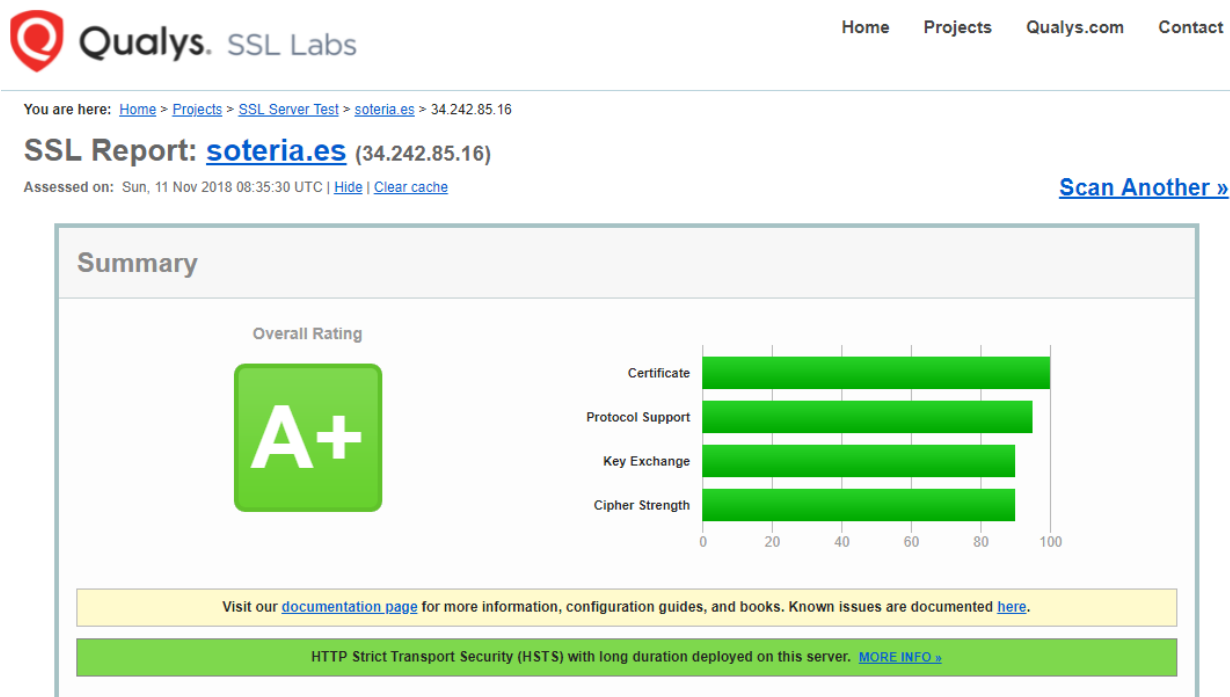


Figura 3-23. Test de seguridad aplicado sobre soteria.es.

Notar que, si se realiza la prueba, se observará que se intenta realizar tanto sobre IPv4 como sobre la dirección de IPv6. El resultado inicialmente indica “*Warning: Inconsistent server configuration*”, debido a que la seguridad no está configurada para IPv6. El dominio y el certificado utilizado se aplican sobre la dirección IPv4 34.242.85.16. Si se selecciona sobre ella en la ventana de resultados, se llega a la información que se ofrece en la Figura 3-22, así como información extendida sobre el certificado utilizado, los protocolos y cifradores habilitados, etcétera.

Se puede concluir que **la configuración ha sido correcta y se ha obtenido un nivel de seguridad muy adecuado.**

Algunas partes de este subapartado están basadas en la referencia [22].

3.9 Funcionalidades adicionales y problemáticas encontradas

Mediante este subapartado se recogen todos aquellos detalles y funcionalidades adicionales que hayan sido contempladas en el diseño y en la implementación, pero no se haya podido poner de manifiesto al describir el desarrollo de los servicios.

- **Optimización:** la elección de un navegador se torna algo fundamental en los servicios web. Optimizar el desarrollo de manera universal para cualquier navegador web que se utilice por parte de los clientes es algo difícil de lograr, si no imposible. Incluso los navegadores

más avanzados y con mejor soporte a veces tienen problemas para visualizar determinado contenido. En ocasiones algún navegador es posible que ni siquiera funcione, por lo que siempre se considera una buena recomendación el disponer de varios navegadores instalados para disponer de alternativa.

De cara al desarrollo del presente trabajo, se ha consultado la siguiente estadística disponible a través de <https://www.w3counter.com/globalstats.php>:

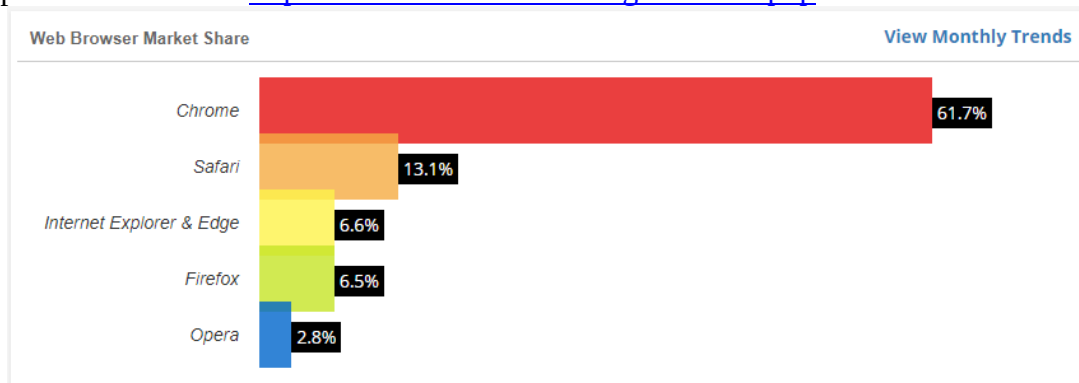


Figura 3-24. Estadísticas de uso de los navegadores más populares.

Por tanto, el presente desarrollo se ha optimizado para el acceso a través del navegador Chrome de Google.

- **Accesibilidad:** este factor se ha tenido en cuenta de cara a favorecer la navegación y el trabajo diario con la plataforma del personal responsable de la Seguridad de la Información.

Se han seguido las recomendaciones del W3C (World Wide Web Consortium - Web Accessibility Initiative: <https://www.w3.org/WAI>). En concreto: Web Content Accessibility Guidelines (WCAG) 2.1, 05 June 2018.

No obstante, hay que tener presente que este trabajo es susceptible de ser desplegado dentro de la AGE, incluso específicamente dentro del MINISDEF, por lo que es muy poco probable que la interfaz necesite ser adaptada a personas con capacidades reducidas, como puede ser con dificultad de visión o audición. De ahí que las adaptaciones se reduzcan principalmente al uso y contraste de colores de la interfaz web.

Para el desarrollo de este factor se ha consultado el siguiente test de contraste:

<https://www.joedolson.com/tools/color-contrast.php>

- **Automatización:** aunque suele significar mayor complejidad a la hora del diseño y la implementación del software, ofrece grandes ventajas en tiempo de operación: facilidad de uso, ahorro en tiempo, reduce posibles errores por parte de los operarios, etcétera. Es por ello que se han intentado automatizar todas aquellas tareas y control de la interfaz web que ha sido posible.
- **Pestaña ENS:** su preparación no ha sido sencilla, ya que requería trasponer el contenido de dicha guía, en su apartado 5 de medidas de protección, a la maquetación HTML adecuada para que se pudiera visualizar a través de la interfaz web manteniendo la apariencia tal como se refleja en la Guía CCN-STIC 804. Era un objetivo laborioso, pero necesario como herramienta de referencia esencial para el personal responsable de Seguridad de la Información. Por tratarse de una referencia fundamental para este trabajo, se ha decidido integrar directamente en la plataforma, en lugar de proporcionarse en forma de acceso al documento original.
- **Escalado de una incidencia:** se ha integrado como anotación en el campo de detalles debido a que se ha incorporado como funcionalidad adicional en un estado muy avanzado del desarrollo. Integrarlo como un campo de la tabla INCIDENTS y lo que ello supone

respecto al rediseño y la reimplementación, hubiera imposibilitado finalizar el trabajo a tiempo. Se deja, por tanto, como línea futura de trabajo.

- Cierre de una incidencia: por considerarse un hito importante en el ciclo de vida de la misma, incluirá la anotación correspondiente en el campo details de la misma, al margen de registrarse la fecha de cierre en el campo *INCIDENTS.closing_date*.
- Variables globales y navegación entre pestañas: han supuesto un esfuerzo importante, incluso una reestructuración completa del código principal del servidor.
 - Respecto a las variables globales: en general, su uso debe restringirse en la medida de lo posible en cualquier lenguaje de programación utilizado. En este caso además se hacía necesario debido a la forma en que se ejecutan este tipo de servicios: mediante procesos e hilos. Ello hace que las variables globales tengan poca utilidad al intercambiar información entre distintos controladores Flask, o incluso entre distintas peticiones POST dentro de un mismo controlador. Las tres soluciones posibles eran:
 - Utilizar variables de ámbito local, lo que obligaba a incluir el código dentro de un mismo controlador.
 - Intercambiar los datos a través de la BBDD, creando alguna tabla de apoyo adicional, lo cual, programáticamente, significa reducir el rendimiento.
 - Utilizar variables de sesión: es la solución más elegante y eficiente, pero el problema que tiene esta aproximación es que cuenta con un espacio reducido en memoria y no puede utilizarse para grandes bloques de datos. Se ha utilizado, por ejemplo, para obtener el nombre de usuario y mostrarlo en cada plantilla web utilizada (*session['current_user']*).
 - Navegación mediante pestañas: se ha tornado dificultoso coordinar la programación activa del servidor con la navegación por pestañas, ya que este último recurso está basado en código JavaScript que se ejecuta de lado del cliente. El problema principal que planteaba era poder mantener el contenido de manera independiente en cada pestaña, de tal manera que el usuario pueda cambiar de pestaña en pestaña como si fueran servicios e interfaces independientes.

Ante esta problemática, la solución adoptada finalmente ha sido el empleo de variables locales y el uso de un único controlador principal para el procesamiento *index()*. Se siguen utilizando distintas plantillas web (*index.html*, *manage_incident.html* y *new_incident.html*), pero el procesamiento se realiza desde un único controlador. Las variables globales quedan restringidas a las partes fijas del aplicativo web: contenido de la pestaña ENS, generación de la maquetación HTML de los interfaces web, etcétera.

- Actualización de la BDD: a la hora de trabajar con BBDD mediante este conjunto de recursos utilizado, es recomendable emplear la bandera *mariaadb_connection.autocommit = True*, con ello se actualiza de manera efectiva la BBDD cada vez que se realiza una modificación sobre sus datos, permitiendo que se refresquen los datos en las consultas posteriores y evitando los problemas de la memoria caché.
- Política de seguridad: Hay que tener en cuenta que el diseño e implementación dependen en gran medida de las políticas de seguridad y de operación que tenga establecidas la organización donde se aplique. Se ha intentado, en base a la experiencia, tener en cuenta diferentes detalles operacionales, pero ese criterio no necesariamente tiene por qué ser fijo, ni el mejor. Como ejemplo paradigmático, se puede indicar el de no permitir que se modifique la severidad de una incidencia que fue inicialmente categorizada como crítica, y a la que se le asignó un equipo de respuesta. Otros criterios diferentes e igualmente válidos

podrían ser el que se pueda modificar la severidad de una incidencia, sea cual sea su categorización inicial; o que se pueda modificar únicamente si el originador fue el sistema SIEM.

Una gran ventaja del diseño interno o a medida es que se pueden ajustar todos estos criterios a conveniencia de la organización, en función de las políticas de Seguridad y Operacional.

4 VERIFICACIÓN

4.1 Descripción del apartado

Mediante este apartado se pretende realizar un conjunto de pruebas que permitan verificar cada una de las funcionalidades proyectadas en el diseño.

Así mismo, el desarrollo de este apartado servirá igualmente como manual de usuario, de tal manera que constituya una referencia válida para que los usuarios recién incorporados cuenten con un método de aprendizaje rápido.

A continuación, se muestra la interfaz inicial de bienvenida que aparece una vez el usuario se ha autenticado correctamente:



Figura 4-1. Interfaz inicial de acceso a la plataforma Soteria.

Muestra una descripción rápida de los servicios que ofrece la plataforma.

Para poder acceder a los servicios se hace necesario iniciar la plataforma a través del botón que se observa en dicha página de bienvenida.

Las pruebas y verificación se llevarán a cabo recorriendo la interfaz web del aplicativo en cada uno de sus apartados y subapartados, probando cada aspecto de la implementación. El punto de partida será el conjunto de servicios que ofrece la plataforma, representado mediante los menús superior y lateral que pueden observarse en la interfaz:

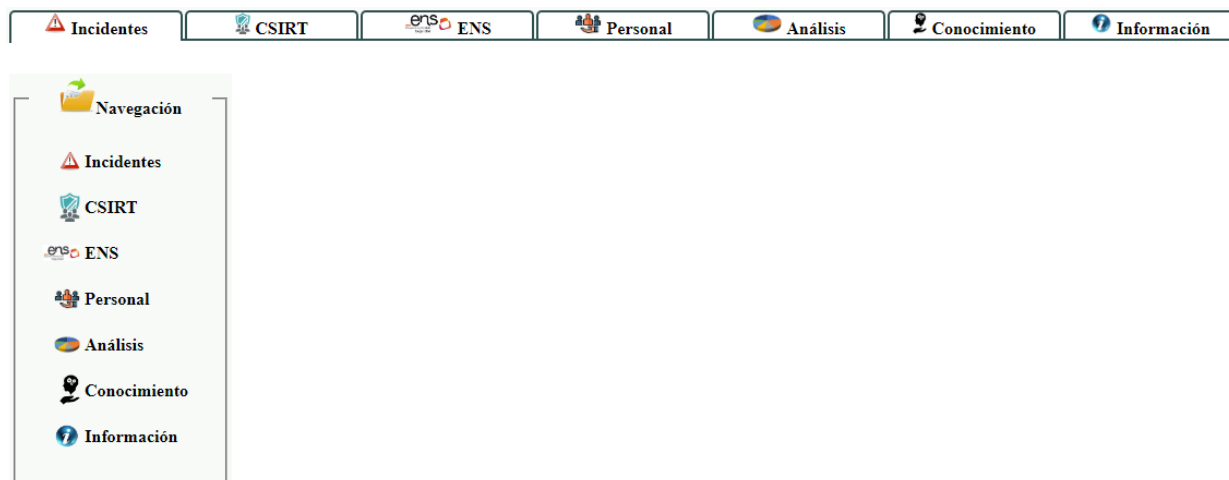


Figura 4-2. Menú superior y lateral de acceso a los servicios de la plataforma.

Como se observa, el acceso a los servicios se encuentra ordenado de izquierda a derecha en el menú superior y de arriba abajo en el menú lateral, en el mismo orden.

A lo largo de los siguientes subapartados se irán recorriendo los servicios disponibles, probando cada aspecto de la funcionalidad.

4.2 Servicio de gestión de incidencias

Mediante este servicio se ofrece el acceso a la gestión de incidentes de Seguridad de la Información. Constituye el núcleo principal del trabajo.

Una vez seleccionado, se ofrece la siguiente interfaz de trabajo:

The image shows the 'Incidentes' (Incidents) section of the web application. At the top is the same horizontal menu bar as in Figure 4-2. Below it is a large search form titled 'Seleccione los criterios de consulta' (Select the search criteria). The form contains several input fields and dropdown menus: 'ID:' (text box), 'Detección: Fecha de inicio:' (text box with 'dd/mm/aaaa' placeholder), 'Fecha de fin:' (text box with 'dd/mm/aaaa' placeholder), 'Estado:' (dropdown), 'Severidad:' (dropdown), 'Dimensiones de seguridad afectadas:' (checkboxes for C, I, D, A, T and an 'AND' dropdown), 'Originador (ID de usuario):' (text box), 'Responsable (ID de usuario):' (text box), 'Tipo de incidencia (código ENS):' (text box), 'Área afectada:' (dropdown), 'CSIRT:' (dropdown), 'CSIRT_ID:' (text box), and radio buttons for 'Falso positivo' and 'Falso negativo'. A magnifying glass icon is at the bottom center of the form. To the right of the form is a button labeled 'Alta de Incidencia' (Incident Entry) with a green plus icon.

Figura 4-3. Interfaz de búsqueda y alta de incidencias.

Para poder realizar la gestión de una incidencia se hace necesario en primer lugar poder localizarla. Por tanto, la interfaz inicial para la gestión de incidentes será un formulario de consulta donde se podrá ordenar la búsqueda de incidencias a través de diversos campos.

Por otro lado, se incorpora el botón de acceso a la interfaz para la gestión del alta de incidencias. Se verá más adelante.

Esta interfaz, además, será la que se muestre por defecto tras iniciar el acceso a los servicios de la plataforma Soteria.

Las pruebas, por tanto, consistirán en realizar búsquedas estableciendo diferentes criterios. Las posibilidades son muy elevadas, pues se ha implementado de tal manera que permita la búsqueda compleja mediante la composición de los diferentes criterios que se establezca, por ejemplo, que la fecha de detección sea posterior a 10/10/2018 y que cuenten con CSIRT asignado. El ofrecer esta posibilidad permite afinar la búsqueda y centrarse solo en aquellas incidencias que cumplan dichos criterios. Como es lógico, no se pueden probar aquí todas las combinaciones posibles, pero sí se puede probar de manera individual la búsqueda simple por cada uno de los campos, y un determinado número de búsquedas compuestas, en las cuales se utilice, al menos, alguno de los campos. Con ello se verificará que el motor de fusión de consultas funciona correctamente. No obstante, se probará también alguna búsqueda compuesta que emplee un elevado número de campos.

Las primeras pruebas, por tanto, serán la búsqueda simple mediante la configuración de un valor en cada campo. Las figuras muestran cada consulta realizada y el resultado de la misma:

Seleccione los criterios de consulta

ID:

Detección: Fecha de inicio: Fecha de fin:

Estado:

Severidad:

Dimensiones de seguridad afectadas: ☐ C ☐ I ☐ D ☐ A ☐ T

Originador (ID de usuario):

Responsable (ID de usuario):

Tipo de incidencia (código ENS):

Área afectada:

CSIRT: CSIRT_ID:

☐ Falso positivo ☐ Falso negativo



Resultado de la consulta:

ID	Originador	Clasificación ENS	Descripción	Área	Responsable	CSIRT	ID_CSIRT
 20180123	SIEM	515	5.1.5 [MPIF.5] ...	Escuadrón #3	juamarmor	N	0

Figura 4-4. Búsqueda de incidencia por su IDentificación.

Como se observa, se muestra una tabla con el resultado de la consulta. En esta ocasión aparece solo una incidencia ya que se estaba buscando directamente mediante su ID.

De ahora en adelante se representará gráfica y únicamente el campo utilizado en la parte de consulta, y los campos ID y el afectado en la parte de resultado.

En el caso de tablas de resultados con elevado número de entradas, se seleccionarán únicamente las primeras a modo de ejemplo.

Detección: Fecha de inicio: Fecha de fin:

Resultado de la consulta:

ID	Detección
 20180093	10/10/2018 21:44
 20180094	15/10/2018 11:23
20180095	17/10/2018 11:39
20180096	20/10/2018 20:18
20180097	21/10/2018 23:11
20180098	22/10/2018 21:52
 20180099	27/10/2018 08:44
 20180100	29/10/2018 08:43
20180121	01/11/2018 20:56
 20180122	01/11/2018 20:57
20180123	01/11/2018 23:00

Figura 4-5. Búsqueda por fecha de Detección.

Estado:

Resultado de la consulta:

ID	Estado
 20170021	U
 20170071	U
 20180005	U
 20180009	U
 20180038	U
 20180046	U
 20180051	U
 20180072	U
 20180098	U
 20180100	U
 20180121	U
 20180123	U
 20180124	U
 20180125	U
 20180126	U

Figura 4-6. Búsqueda por Estado.

Severidad: Alta ▼

Resultado de la consulta:

ID	Severidad
20150003	A
20150030	A
20150040	A
20150049	A
20150056	A
20150059	A
20150085	A
20150092	A
20150093	A
20150095	A
20150096	A
20150099	A

Figura 4-7. Búsqueda por Severidad.

Dimensiones de seguridad afectadas: ☒ C ☒ I ☐ D ☐ A ☐ T AND ▼**Resultado de la consulta:**

ID	Dimensiones
20150005	CIDA
20150006	CID
20150009	CIDAT
20150012	CIAT
20150023	CIT
20150032	CIA
20150041	CIDT
20150042	CIA
20150043	CIDT
20150046	CIDAT

Figura 4-8. Búsqueda mediante Dimensiones de Seguridad. Selector AND.

Como se observa en la anterior figura, en esta ocasión se ha elegido el selector AND, por lo que se mostrarán todas aquellas incidencias en las que hay afectadas todas las dimensiones marcadas. A continuación, se repite la misma búsqueda, pero con el selector OR para mostrar la diferencia:

Dimensiones de seguridad afectadas: ☒ C ☒ I ☐ D ☐ A ☐ T OR ▼

Resultado de la consulta:

ID	Dimensiones
 20150001	IAT
 20150002	C
 20150003	I
 20150005	CIDA
 20150006	CID
 20150007	IAT
 20150008	CT
 20150009	CIDAT
 20150011	I
 20150012	CIAT

Figura 4-9. Búsqueda mediante Dimensiones de Seguridad. Selector OR.

Como se observa, con el selector OR se localizan las incidencias que tengan afectadas cualquiera de las dimensiones de seguridad marcadas.

Originador (ID de usuario): blachimar

Resultado de la consulta:

ID	Originador
 20150086	blachimar
 20160114	blachimar
 20180051	blachimar
 20180134	blachimar
 20180135	blachimar
 20180136	blachimar
 20180207	blachimar
 20180208	blachimar
 20180209	blachimar
 20180210	blachimar

Figura 4-10. Búsqueda por Originador.

Responsable (ID de usuario):

Resultado de la consulta:

ID	Responsable
 20150007	blachimar
 20150020	blachimar
 20150036	blachimar
 20150059	blachimar
 20150081	blachimar
 20160003	blachimar
 20160048	blachimar
 20160078	blachimar
 20160111	blachimar
 20160127	blachimar

Figura 4-11. Búsqueda por Responsable.

Tipo de incidencia (código ENS):

Resultado de la consulta:

ID	Clasificación ENS
 20150050	571
 20150077	571
 20150113	571
 20160026	571
 20160044	571
 20160088	571
 20160104	571
 20170100	571
 20170128	571
 20180023	571

Figura 4-12. Búsqueda por Tipo de incidencia (Clasificación del ENS).

Área afectada:

Resultado de la consulta:

ID	Área
 20150005	Escuadrón #1
 20150018	Escuadrón #1
 20150046	Escuadrón #1
 20150050	Escuadrón #1
 20150057	Escuadrón #1
 20150064	Escuadrón #1
 20150065	Escuadrón #1
 20150094	Escuadrón #1
 20150108	Escuadrón #1
 20150113	Escuadrón #1

Figura 4-13. Búsqueda por Área afectada.

CSIRT:

Resultado de la consulta:

ID	CSIRT
 20150026	S
 20150065	S
 20150088	S
 20150105	S
 20160027	S
 20160040	S
 20160047	S
 20160049	S
 20160096	S
 20160111	S

Figura 4-14. Búsqueda según tenga asignado o no un Equipo de Respuesta la incidencia.

CSIRT_ID:

Resultado de la consulta:

ID	ID_CSIRT
 20180010	201801

Figura 4-15. Búsqueda por IDentificación de Equipo de Respuesta.

☒ Falso positivo

Resultado de la consulta:

ID	Falso Positivo
 20150011	S
 20150018	S
 20150028	S
 20150032	S
 20150034	S
 20150038	S
 20150042	S
 20150045	S
 20150047	S
 20150053	S

Figura 4-16. Búsqueda de falsos positivos.

☒ Falso negativo

Resultado de la consulta:

ID	Falso Negativo
 20150006	S
 20150019	S
 20150060	S
 20150108	S
 20150131	S
 20160042	S
 20160083	S
 20160123	S
 20160124	S
 20160127	S

Figura 4-17. Búsqueda de falsos negativos.

Una vez comprobado que las consultas individuales funcionan correctamente, pasamos a realizar diversas pruebas mediante consultas combinadas de distintos campos, cuidando que cada campo participe, al menos, una vez en las pruebas (con la excepción de los campos de identificación de incidencias y de Equipos de Respuesta, pues solamente tienen utilidad para buscar incidencias concretas).

Detección: Fecha de inicio: 01/08/2018 Fecha de fin: 31/10/2018
Estado: Cuarentena ▼

Resultado de la consulta:

ID	Originador	Clasificación ENS	Descripción	Área	Responsable
 20180072	SIEM	532	5.3.2 [MPEQ.2] ...	Escuadrón #1	danjimcue
 20180098	marestrom	511	5.1.1 [MP.IF.1] ...	Apoyo al Personal	marestrom
 20180100	SIEM	524	5.2.4 [MP.PER.4]...	Escuadrón #2	mikzucsav

Figura 4-18. Consulta compuesta: fecha de Detección + Estado.

En la figura anterior se puede comprobar el resultado de la primera búsqueda compuesta, en este caso limitando a un periodo de tres meses la fecha de detección, y para aquellas incidencias que se encuentren actualmente en cuarentena.

Para la siguiente búsqueda se consultarán aquellas incidencias en estado Abierta, de severidad Alta y donde se encuentre afectada la dimensión de seguridad de Disponibilidad:

Estado:

Severidad:

Dimensiones de seguridad afectadas: ☐ C ☐ I ☒ D ☐ A ☐ T

Resultado de la consulta:

ID	Originador	Clasificación ENS	Descripción	Área	Responsable
 20180076	SIEM	511	5.1.1 [MP.IF.1] ...	Global	lucvelrub
 20180099	mikzucsav	581	5.8.1 [MP.S.1] P...	Abastecimiento	framinest
 20180135	blachimar	544	5.4.4 [MP.COM.4]...	Escuadrón #1	marestrom

Figura 4-19. Consulta compuesta: Estado + Severidad + Dimensiones.

Para la siguiente búsqueda se realizará una consulta compleja donde se indicará un periodo para la detección de seis meses, el sistema SIEM como originador de las incidencias y además que sean de un determinado tipo:

Detección: Fecha de inicio: Fecha de fin:

Originador (ID de usuario):

Tipo de incidencia (código ENS):

Resultado de la consulta:

ID	Originador	Clasificación ENS	Descripción	Área	Responsable
 20180057	SIEM	571	5.7.1 [MP.INFO.1...	Escuadrón #3	marestrom

Figura 4-20. Consulta compuesta: fecha Detección + Originador + Tipo.

Como se observa, conforme más se afina la configuración de la búsqueda, más se reducen las posibilidades y, por tanto, los resultados.

En la siguiente búsqueda se consultarán aquellas incidencias cuya responsabilidad corresponda al usuario *blachimar*, el área afectada sea *Secretaría* y haya requerido la conformación de un Equipo de Respuesta:

Responsable (ID de usuario):

Área afectada:

CSIRT:

Resultado de la consulta:

ID	Originador	Clasificación ENS	Descripción	Área	Responsable	CSIRT	ID_CSIRT
 20160111	SIEM	551	5.5.1 [MP.SI.1] ...	Secretaría	blachimar	S	201606

Figura 4-21. Consulta compuesta: Responsable + Área + CSIRT.

Severidad:

Dimensiones de seguridad afectadas: ☐ C ☐ I ☐ D ☒ A ☒ T

☒ Falso positivo

Resultado de la consulta:

ID	Originador	Clasificación ENS	Descripción	Área	Responsable	Dimensiones	Falso Positivo
 20170030	SIEM	517	5.1.7 [MP.IF.7] ...	Automóviles	rafnadpar	CIDAT	S

Figura 4-22. Consulta compuesta: Severidad + Dimensiones + Falso positivo.

En la última consulta de prueba se buscan aquellas incidencias originadas por el sistema *SIEM*, cuyo responsable sea el usuario *blachimar* y que hayan resultado ser un falso negativo:

Originador (ID de usuario):

Responsable (ID de usuario):

☒ Falso negativo

Resultado de la consulta:

ID	Originador	Clasificación ENS	Descripción	Área	Responsable	Falso Negativo
 20160127	SIEM	582	5.8.2 [MPS.2] P...	Escuadrón #2	blachimar	S

Figura 4-23. Consulta compuesta: Originador + Responsable + Falso negativo.

Para comprobar que las consultas se están realizando correctamente, se puede ejecutar en paralelo la consulta desde la línea de comandos de acceso a la BBDD. En el caso de la última consulta:

```
ubuntu@ip-172-31-33-131: ~
ubuntu@ip-172-31-33-131:~$ mysql -u root -p
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 24909
Server version: 10.3.10-MariaDB-1:10.3.10+maria~trusty-log mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use soteria;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [soteria]> select id from INCIDENTS where originator='SIEM' and accountable='blachimar' and false_n='S';
+-----+
| id    |
+-----+
| 20160127 |
+-----+
1 row in set (0.001 sec)

MariaDB [soteria]>
```

Figura 4-24. Consulta compuesta desde línea de comandos.

Como se observa, en ambos casos se acota el resultado a la incidencia con ID 20160127.

A lo largo de las pruebas se puede comprobar igualmente que **las entradas se encuentran validadas**, no siendo posible insertar caracteres que no sean apropiados para cada campo.

Una vez comprobado que se pueden realizar consultas compuestas de manera correcta, el siguiente paso será seleccionar una de las incidencias de la tabla que ofrece el resultado de la consulta, y acceder al servicio de vista detallada y edición de incidencias (*manage_incident*). Supóngase, por ejemplo, la consulta que aparece en la Figura 4-19. Si se selecciona la incidencia con ID 20180099, se obtiene el siguiente resultado:

Datos básicos

ID: 20180099 Escalar: ☐

Originador: Mike Zuckerberg Saverin

Clasificación ENS: 581

Área: Abastecimiento

Responsable: Francisco Javier Miñambres Estero ▼

CSIRT: N CSIRT ID: 0

Fecha detección: 27/10/2018 08:44

Fecha notificación: 27/10/2018 08:48

Severidad: Alta ▼

Dimensiones de seguridad:
☐ C ☐ I ☒ D ☐ A ☒ T

Estado: Abierta ▼

☐ Falso positivo ☐ Falso negativo

Actualizar

Información ampliada

Descripción: 5.8.1 [MPS.1] PROTECCIÓN DEL CORREO ELECTRÓNICO (E-MAIL)

MEDIDAS DE PROTECCIÓN		
Código	Aplicado	Observaciones
609	Sí ▼	Se puede aplicar en su lugar la siguiente medida sustitutiva: bla bla bla. Medida sustitutiva aplicada. Aplicada correctamente.
		Se puede aplicar en su lugar la siguiente medida sustitutiva: bla bla bla.

Detalles

Se inician las acciones para la resolución de la incidencia. Para poder aplicar la medida de protección tal se ha hecho necesario reiniciar el servidor pascual. Realizando pruebas de estabilidad.

Informes

¿Nuevo informe? => inserte URL:

Figura 4-25. Servicio de consulta detallada y edición de incidencias.

El siguiente paso será comprobar que, en el caso de necesitar actualizar algunos datos a lo largo del ciclo de vida de la incidencia, se realiza de manera correcta. En esta ocasión no se hace necesario ir probando la modificación de todos aquellos campos que admitan edición. Basta con hacer cambios en todos ellos y comprobar que, efectivamente, se han actualizado correctamente. Por tanto, tras introducir los cambios el resultado es el siguiente:

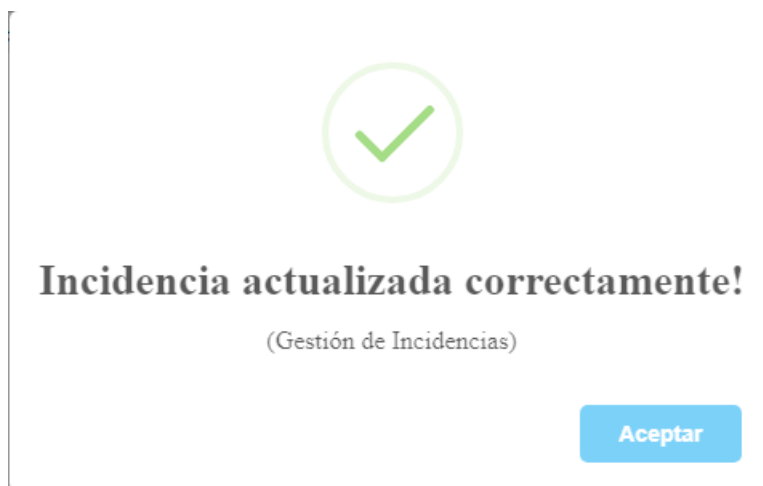


Figura 4-26. Ventana emergente de aviso de la edición correcta de una incidencia.

Lo primero que aparece es una ventana emergente para avisar de la actualización correcta de la incidencia. Si se vuelve a entrar en la vista detallada de la incidencia, se puede comprobar que, efectivamente, se han actualizado los datos:

Datos básicos

ID: 20180099 Escalar: ☐

Originador: Mike Zuckerberg Saverin

Clasificación ENS: 581

Área: Abastecimiento

Responsable: Blas Chica Martos

CSIRT: N CSIRT ID: 0

Fecha detección: 27/10/2018 08:44

Fecha notificación: 27/10/2018 08:48

Severidad: Media

Dimensiones de seguridad:
☐ C ☐ I ☒ D ☐ A ☐ T

Estado: Cuarentena

☐ Falso positivo ☐ Falso negativo

Actualizar

Información ampliada

Descripción: 5.8.1 [MPS.1] PROTECCIÓN DEL CORREO ELECTRÓNICO (E-MAIL)

MEDIDAS DE PROTECCION

Código	Aplicado	Observaciones
609	No	Se puede aplicar en su lugar la siguiente medida substitutiva: bla bla bla. La medida substitutiva requiere desplegar el software XXX.
610	Sí	Aplicada correctamente.

Detalles

Se inician las acciones para la resolución de la incidencia. Para poder aplicar la medida de protección tal se ha hecho necesario reiniciar el servidor pascual. Realizando pruebas de estabilidad.

09/11/2018: se reduce la severidad a Media, se actualizan las dimensiones de seguridad a D, se pasa a cuarentena debido a la espera del despliegue del software XXX, se aplica la medida de protección 610 y se añade el informe new_report_01.pdf.

09/11/2018: se cambia el responsable de la incidencia Francisco Javier Miñambres Estero por Blas Chica Martos.

Informes

new_report_01.pdf:
https://soteria.es/reports/new_report_01.pdf

¿Nuevo informe? => inserte URL:

Figura 4-27. Incidencia tras la modificación de todos sus campos editables.

Se puede comprobar que todos sus campos editables han sufrido variación respecto al estado anterior de la incidencia, y se reflejan correctamente. Para poder verificarlo, se realiza la consulta de los campos que han sufrido variación desde la línea de comandos de conexión a la BBDD:

```
MariaDB [soteria]> select accountable,severity,dimensions,status,pm_info,details,reports from INCIDENTS where id=20180099;
```

accountable	severity	dimensions	status	pm_info	details	reports
blachimar	M	D	U	609\$\$\$Se puede aplicar en su lugar la siguiente medida substitutiva: bla bla bla. La medida substitutiva requiere desplegar el software XXX.==610\$\$\$Aplicada correctamente.==611\$\$\$No se puede aplicar la recomendación sobre: bla bla bla. Se admite aplicación parcial. Parcialmente aplicada.==613\$\$\$Se puede aplicar en su lugar la siguiente medida substitutiva: bla bla bla. Medida substitutiva aplicada. Aplicada correctamente.==	Se inician las acciones para la resolución de la incidencia. Para poder aplicar la medida de protección tal se ha hecho necesario reiniciar el servidor pascual. Realizando pruebas de estabilidad. 09/11/2018: se reduce la severidad a Media, se actualizan las dimensiones de seguridad a D, se pasa a cuarentena debido a la espera del despliegue del software XXX, se aplica la medida de protección 610 y se añade el informe new_report_01.pdf. 09/11/2018: se cambia el responsable de la incidencia Francisco Javier Miñambres Estero por Blas Chica Martos.	https://soteria.es/reports/new_report_01.pdf

Figura 4-28. Verificación del contenido de los campos modificados.

Se verifica que, efectivamente, se han registrado los cambios establecidos.

Merece la pena destacar lo que refleja la incidencia modificada con respecto al campo Responsable (*accountable*). Si se observa el campo de Detalles (*details*), se aprecia que aparecen dos entradas con fecha 09/11/2018. La primera es precisamente la que se ha introducido de manera manual, donde el personal responsable de seguridad de la información refleja los cambios más importantes que vayan sucediendo a lo largo de la vida de la incidencia. Sin embargo, aparece una segunda entrada con la misma fecha, donde se refleja el cambio de Responsable de la incidencia. En este caso, la inserción ha sido automática, ya que **el responsable se considera un elemento crítico de una incidencia, especialmente en lo relativo a trazabilidad**, por lo que se automatiza su modificación para que quede reflejado en los detalles de la incidencia, lo refleje o no en manual el usuario.

Una última funcionalidad que faltaría por comprobar es respecto al escalado de la incidencia. Al igual que ocurría en el caso del Responsable, al ser el escalado también un hito importante a lo largo de la vida de la incidencia, se registra de manera automática en el campo detalles. En este caso únicamente se refleja la fecha de escalado, no se puede indicar nada más ya que se desconocen a priori los motivos para ello. Lo normal es que el operario que va a realizar el escalado indique en el campo de detalles los motivos para ello:

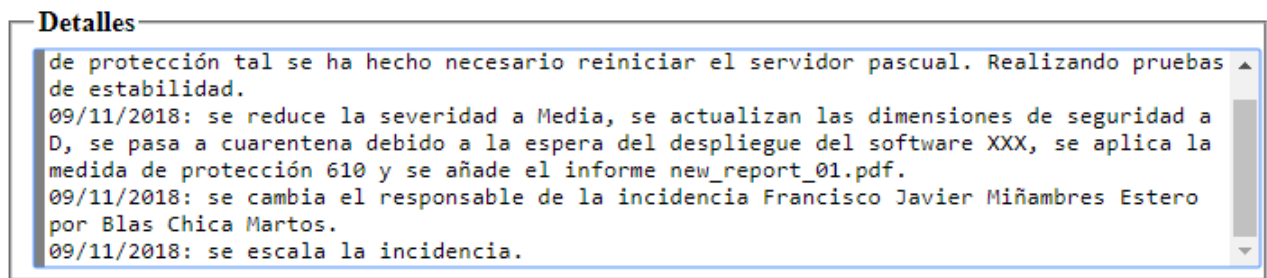


Figura 4-29. Inserción automática del registro del escalado de la incidencia.

De nuevo, accediendo a la BBDD desde línea de comandos se verifica el contenido del campo *details*:

```
MariaDB [soteria]> select details from INCIDENTS where id=20180099;
| details
|
| Se inician las acciones para la resolución de la incidencia. Para poder aplicar la medida de protección tal se ha hecho necesario reiniciar el
| servidor pascual. Realizando pruebas de estabilidad.
| 09/11/2018: se reduce la severidad a Media, se actualizan las dimensiones de seguridad a D, se pasa a cuarentena debido a la espera del despliegue
| e del software XXX, se aplica la medida de protección 610 y se añade el informe new_report_01.pdf.
| 09/11/2018: se cambia el responsable de la incidencia Francisco Javier Miñambres Estero por Blas Chica Martos.
| 09/11/2018: se escala la incidencia. |
```

Figura 4-30. Verificación de inserción automática del escalado en el campo *details*.

Tanto el **cambio de Responsable**, como del **Escalado** de la incidencia, por ser **aspectos críticos**, suponen además notificación a los afectados. Se verá en el apartado dedicado al servicio de notificaciones.

Por último, se verifican las banderas relativas a si se trata de un falso positivo o un falso negativo. Se ha preferido dejar para el final ya que, para hacer una demostración lo más realista posible, la detección de un falso positivo quiere decir, en definitiva, que se trata de una falsa alarma, por lo que supone indicarlo en el campo detalles y Cerrar la incidencia. Se prueba primero el marcado de un falso negativo:

Incidentes | **CSIRT** | **ENS** | **Personal** | **Análisis** | **Conocimiento** | **Información**

Datos básicos

ID: 20180099 Escalar: ☐

Originador: Mike Zuckerberg Saverin

Clasificación ENS: 581

Área: Abastecimiento

Responsable: Blas Chica Martos

CSIRT: N CSIRT ID: 0

Fecha detección: 27/10/2018 08:44

Fecha notificación: 27/10/2018 08:48

Severidad: Media

Dimensiones de seguridad:
☐ C ☐ I ☒ D ☐ A ☐ T

Estado: Cuarentena

☐ Falso positivo ☒ Falso negativo

Actualizar

Información ampliada

Descripción: 5.8.1 [MPS.1] PROTECCIÓN DEL CORREO ELECTRÓNICO (E-MAIL)

MEDIDAS DE PROTECCIÓN

Código	Aplicado	Observaciones
609	No	Se puede aplicar en su lugar la siguiente medida sustitutiva: bla bla bla. La medida sustitutiva requiere desplegar el software XXX.
		Aplicada correctamente.

Detalles

Se inician las acciones para la resolución de la incidencia. Para poder aplicar la medida de protección tal se ha hecho necesario reiniciar el servidor pascual. Realizando pruebas de estabilidad.

09/11/2018: se reduce la severidad a Media, se actualizan las dimensiones de seguridad a D, se pasa a cuarentena debido a la espera del despliegue del software XXX, se aplica la medida de protección 610 y se añade el informe new_report_01.pdf.

09/11/2018: se cambia el responsable de la incidencia Francisco Javier Miñambres Estero por Blas Chica Martos.

Informes

new_report_01.pdf:
https://soteria.es/reports/new_report_01.pdf

¿Nuevo informe? => inserte URL:

Figura 4-31. Incidencia marcada como falso negativo.

```

MariaDB [soteria]> select false_n from INCIDENTS where id=20180099;
+-----+
| false_n |
+-----+
| s       |
+-----+
1 row in set (0.000 sec)

```

Figura 4-32. Verificación del marcado como falso negativo.

Por último, se marca la incidencia como falso positivo, lo que supone el cierre de la misma:

Figura 4-33. Incidencia marcada como falso positivo y Cierre de la misma.

Al cerrar una incidencia se inserta en el campo de detalles de manera automática la fecha de cierre. Verificando los datos a través del acceso a la BBDD mediante línea de comandos:

```

MariaDB [soteria]> select false_p,status from INCIDENTS where id=20180099;
+-----+-----+
| false_p | status |
+-----+-----+
| s       | c      |
+-----+-----+
1 row in set (0.000 sec)

```

Figura 4-34. Verificación del marcado como falso positivo y cierre de la incidencia.

Respecto al alta manual de nuevas incidencias, se accede a dicho servicio a través del menú principal de gestión de incidencias:

Seleccione los criterios de consulta

ID:

Detección: Fecha de inicio: Fecha de fin:

Estado:

Severidad:

Dimensiones de seguridad afectadas: ☐ C ☐ I ☐ D ☐ A ☐ T

Originador (ID de usuario):

Responsable (ID de usuario):

Tipo de incidencia (código ENS):

Área afectada:

CSIRT: CSIRT_ID:

☐ Falso positivo ☐ Falso negativo





Figura 4-35. Acceso al servicio de alta manual de nuevas incidencias.

La interfaz de alta de incidencias es la siguiente:

Inserte los datos de la nueva incidencia

ID:

Estado*:

Severidad*:

Dimensiones de seguridad afectadas*: ☐ C ☐ I ☐ D ☐ A ☐ T

Responsable (ID de usuario)*:

Tipo de incidencia (código ENS)*:

Área afectada*:

CSIRT: CSIRT_ID:



***Campos obligatorios**

Figura 4-36. Interfaz para el alta manual de incidencias.

Antes de pasar a generar una incidencia de prueba, cabe destacar algunas consideraciones de interés:

- Si se observa la figura anterior, se inserta automáticamente el número para la identificación de la nueva incidencia. Para obtener este número, se comprueba cuál es la identificación de mayor valor que existe actualmente en la tabla *INCIDENTS*, seleccionando por tanto el siguiente valor. Este campo además no es editable, de esta manera se mantiene la secuenciación y coherencia de la BBDD. En resumen, es un campo controlado programáticamente para evitar pérdida de secuenciación y que se quede numeración de por medio sin utilizar.

Además, se controla la numeración para el cambio de año, ya que los cuatros primero dígitos del campo *ID* de una incidencia reflejan el año de creación de la misma.

- Los campos marcados con * son de obligada cumplimentación, no se pueden dejar en blanco. Este hecho se controla programáticamente y, en el caso de hacer caso omiso, se avisa al usuario y se le insta a insertar de nuevo los datos de manera correcta:

Rellene los campos obligatorios, por favor!

Figura 4-37. Mensaje de aviso en caso de no cumplimentar todos los datos necesarios.

- Los campos para introducir los datos se encuentran validados. Ello quiere decir que no admiten caracteres que no sean los apropiados al tipo de información que recoge cada uno. En caso contrario, se indica el siguiente mensaje de aviso:



Figura 4-38. Mensaje de aviso en caso de insertar caracteres no permitidos.

- Los campos *CSIRT* y *CSIRT_ID* tienen un tratamiento especial, ya que un Equipo de Respuesta únicamente puede conformarse para incidencias de severidad Crítica. Por tanto, quedan deshabilitados mientras no se seleccione dicha severidad:

Inserte los datos de la nueva incidencia

ID:

Estado*:

Severidad*:

Dimensiones de seguridad afectadas*: ☒ C ☒ I ☐ D ☐ A ☐ T

Responsable (ID de usuario)*:

Tipo de incidencia (código ENS)*:

Área afectada*:

CSIRT: CSIRT_ID:



***Campos obligatorios**

Figura 4-39. Deshabilitados CSIRT y CSIRT_ID hasta seleccionar severidad Crítica.

Una vez se selecciona severidad Crítica, se observa que se ofrece la posibilidad de que se establezca un CSIRT:

Inserte los datos de la nueva incidencia

ID:

Estado*:

Severidad*:

Dimensiones de seguridad afectadas*: ☒ C ☒ I ☐ D ☐ A ☐ T

Responsable (ID de usuario)*:

Tipo de incidencia (código ENS)*:

Área afectada*:

CSIRT: CSIRT_ID:



***Campos obligatorios**

Figura 4-40. Se habilitan CSIRT y CSIRT_ID al seleccionar severidad Crítica.

Al igual que ocurría en el caso de la identificación de incidencias, en el caso de seleccionar Sí en el campo CSIRT, se inserta automáticamente el identificador para el nuevo Equipo de Respuesta, y no admite edición, manteniendo la secuenciación y coherencia de la tabla CSIRT, en este caso:

CSIRT: CSIRT_ID:

Figura 4-41. Inserción automática del identificador del nuevo Equipo de Respuesta.

Por último, en el caso de que durante la creación de la incidencia se vuelva a reducir la severidad a un nivel inferior a Crítica, se deshabilitan de nuevo los campos CSIRT y CSIRT_ID, además de cambiarse automáticamente el estado del campo CSIRT a No:

Severidad*: Alta ▼

CSIRT: No ▼ CSIRT_ID: 201815

Figura 4-42. Se deshabilitan CSIRT y CSIRT_ID al volver a reducir la severidad.

Una vez expuestos todos estos condicionantes para asegurar una correcta recogida de datos, se expone a continuación el alta de una nueva incidencia. Para el ejemplo, se seleccionarán los siguientes datos:

Inserte los datos de la nueva incidencia

ID: 20180216

Estado*: Abierta ▼

Severidad*: Crítica ▼

Dimensiones de seguridad afectadas*: ☒ C ☒ I ☐ D ☐ A ☐ T

Responsable (ID de usuario)*: blachimar

Tipo de incidencia (código ENS)*: 571

Área afectada*: Global ▼

CSIRT: Si ▼ CSIRT_ID: 201815



***Campos obligatorios**

Figura 4-43. Generación manual de una nueva incidencia.

El proceso concluye indicándose el registro correcto de la nueva incidencia mediante una ventana emergente:

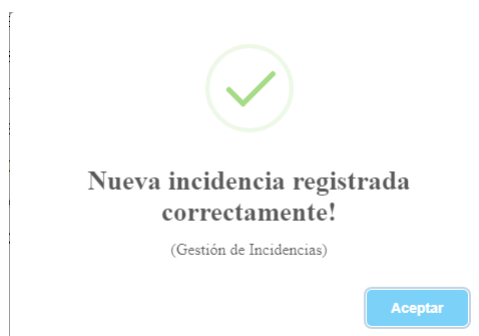


Figura 4-44. Ventana emergente informando del registro correcto de la nueva incidencia.

Otro detalle a observar es que, una vez insertada una nueva incidencia, el sistema permanece en la ventana de alta de alta de incidencias, en el caso de que el usuario desee seguir insertando más incidencias. Además, se cuida de actualizar la secuenciación de los identificadores de la nueva incidencia y del posible nuevo Equipo de Respuesta:

ID: 20180217

CSIRT_ID: 201816

Figura 4-45. Control de secuencia para nuevas altas.

Por último, solamente queda comprobar que, efectivamente, se ha registrado correctamente el alta de la nueva incidencia. Para ello, se sigue el proceso expuesto al comienzo de este subapartado: se consulta la nueva incidencia (buscando por ID → 20180216), y se selecciona de la tabla de resultados para acceder al despliegue detallado de sus datos:

The screenshot shows a web interface with a top navigation bar containing tabs: Incidentes, CSIRT, ENS, Personal, Análisis, Conocimiento, and Información. The 'Incidentes' tab is active. On the left, the 'Datos básicos' section displays the following information: ID: 20180216 (highlighted with a red box), Escalar: [checkbox], Originador: Blas Chica Martos, Clasificación ENS: 571, Área: Global, Responsable: Blas Chica Martos (dropdown), CSIRT: S CSIRT ID: 201815, Fecha detección: 09/11/2018 10:27, Fecha notificación: 09/11/2018 10:28, Severidad: Crítica (dropdown), Dimensiones de seguridad: [checkbox] C [checkbox] I [checkbox] D [checkbox] A [checkbox] T, Estado: Abierta (dropdown), and radio buttons for Falso positivo and Falso negativo. An 'Actualizar' button is at the bottom. The right panel, 'Información ampliada', shows the description: 5.7.1 [MP.INFO.1] DATOS DE CARÁCTER PERSONAL. Below this is a table for 'MEDIDAS DE PROTECCIÓN' with columns 'Código', 'Aplicado', and 'Observaciones'. The first row shows '539', 'No' (dropdown), and an empty field. Below the table are sections for 'Detalles' and 'Informes'. At the bottom right, there is a link: ¿Nuevo informe? => inserte URL: [text area].

Figura 4-46. Consulta detallada de la nueva incidencia generada manualmente.

Como último paso en la verificación, se comprueba mediante el acceso a la BBDD desde línea de comandos la nueva incidencia insertada:

```
MariaDB [soteria]> select * from INCIDENTS where id=20180216;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id      | originator | type | description | area | accountable | csirt | id_csirt | detect_date | notify_date |
| severity | dimensions | status | reports | details | pm_info | false_p | false_n | closing_date |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 20180216 | blachimar | CI | 5.7.1 [MP.INFO.1] DATOS DE CARÁCTER PERSONAL | Global | blachimar | S | 201815 | 201811091027 | 09/11/2018
10:28 | C | A | | 539$$$N==540$$$N== | N | N | NULL |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.000 sec)
```

Figura 4-47. Consulta de la nueva incidencia mediante conexión directa a la BBDD.

Comentar que el alta de una incidencia de severidad Crítica supone la notificación al responsable, o a todo el Equipo de Respuesta, como es el caso. De nuevo, este aspecto se verificará en el apartado dedicado al servicio de notificaciones.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de gestión de incidencias de Seguridad de la Información.**

4.3 Servicio de gestión de Equipos de Respuesta (CSIRT)

El acceso al servicio de gestión de equipos de respuesta se realiza a través de la pestaña correspondiente de la interfaz principal de la plataforma web. El aspecto es el siguiente:

GESTIÓN DE EQUIPOS DE RESPUESTA

ID	INCIDENCIA	Equipo de Respuesta	Conformación	Activo
201501	20150026	García Delgado, Arturo Jiménez Cuenca, Daniel Estepa Romero, María	12/03/2015 18:27	No
201502	20150065	Estepa Romero, María Nadal Parera, Rafael Sevilla Ovejita, Carmen	23/06/2015 21:49	No
201503	20150088	Miñambres Estero, Francisco Javier Sevilla Ovejita, Carmen García Delgado, Arturo	30/08/2015 13:47	No
201504	20150105	Cano Maldonado, Pedro Santos Melvar, Silvia Ígor Nelleró, Ángel	12/10/2015 14:57	No
201601	20160027	Tenorio Carrasco, Manuel Vélez Rubio, Lucía Cano Maldonado, Pedro	16/03/2016 11:23	No
201602	20160040	Cano Maldonado, Pedro Miñambres Estero, Francisco Javier Tenorio Carrasco, Manuel	19/04/2016 16:50	No
201603	20160047	Sevilla Ovejita, Carmen Ígor Nelleró, Ángel Tenorio Carrasco, Manuel	05/05/2016 10:56	No
201604	20160049	Cano Maldonado, Pedro Marchal Mora, Juan Estepa Romero, María	14/05/2016 01:44	No
201605	20160096	Tenorio Carrasco, Manuel García Delgado, Arturo	18/09/2016 11:23	No

Edición de Equipos

CSIRT: 201804 ▼

Componente 1 (Responsable):
Estepa Romero, María ▼

Componente 2:
Jiménez Cuenca, Daniel ▼

Componente 3:
Nadal Parera, Rafael ▼

ACTUALIZAR

Figura 4-48. Interfaz de gestión de Equipos de Respuesta.

Como se observa, está integrado por dos apartados:

- Tabla con los datos principales de los Equipos de Respuesta: se incluye una bandera de *Activo*, informando si el CSIRT se encuentra actualmente activo, es decir, la incidencia sigue abierta; o bien se ha cerrado ya, quedando por tanto el Equipo de Respuesta Inactivo.
- Edición de Equipos de Respuesta: permite la modificación de aquellos equipos de respuesta que se encuentren activos. Lógicamente, no tiene sentido intentar modificar la composición de un Equipo de Respuesta una vez pase a inactivo, es decir, una vez se cierre la incidencia que atiende dicho equipo. Eso además provocaría problemas de trazabilidad.

Las acciones que permite son, por tanto:

- La consulta de la conformación de todos los Equipos de Respuesta, tanto los activos actualmente, como el histórico de los mismos.
- La edición de los Equipos de Respuesta actualmente en activo.

A continuación, se va a verificar que, efectivamente, se permite la modificación en la composición de un Equipo de Respuesta, y lo que ello supone.

Del listado de Equipos editable (los que se encuentra en activo), se selecciona cualquiera de ellos. Supóngase que se elige el que aparece en primer lugar con ID 201804. Supóngase además que el componente 2, identificado simuladamente como Daniel Jiménez Cuenca, por motivos logísticos u organizacionales, se decide que sea cambiado de dicho equipo. El resultado sería el siguiente:

Edición de Equipos

CSIRT: 201804 ▼

Componente 1 (Responsable):
Estepa Romero, Maria ▼

Componente 2:
Marchal Mora, Juan ▼

Componente 3:
Nadal Parera, Rafael ▼


ACTUALIZAR

Figura 4-49. Modificación de un componente de un Equipo de Respuesta.

Al ejecutar el cambio aparece en primer lugar una ventana emergente de aviso sobre el cambio:



Figura 4-50. Ventana emergente informando sobre el cambio realizado correctamente.

Si se vuelve a la tabla, se observa que se ha realizado el cambio correctamente:

201804	20180093	Estepa Romero, Maria Marchal Mora, Juan Nadal Parera, Rafael	10/10/2018 21:45	Si
--------	----------	--	------------------	----

Edición de Equipos

CSIRT: 201804 ▼

Componente 1 (Responsable):
Estepa Romero, Maria ▼

Componente 2:
Marchal Mora, Juan ▼

Componente 3:
Nadal Parera, Rafael ▼


ACTUALIZAR

Figura 4-51. La tabla de Equipos de Respuesta actualizada refleja el cambio.

Bien, este cambio es además un hecho de elevada importancia, porque supone que una persona deja de atender una incidencia, y otra persona ocupa su lugar. Para mantener la trazabilidad, cuando ocurren estos cambios se hace necesario dejarlos reflejados en la incidencia. Para ello, ante un cambio de componentes de Equipos de Respuesta se inserta automáticamente dicho cambio en el campo de detalles de la incidencia. Si se consulta la incidencia afectada en este caso, 20180093:

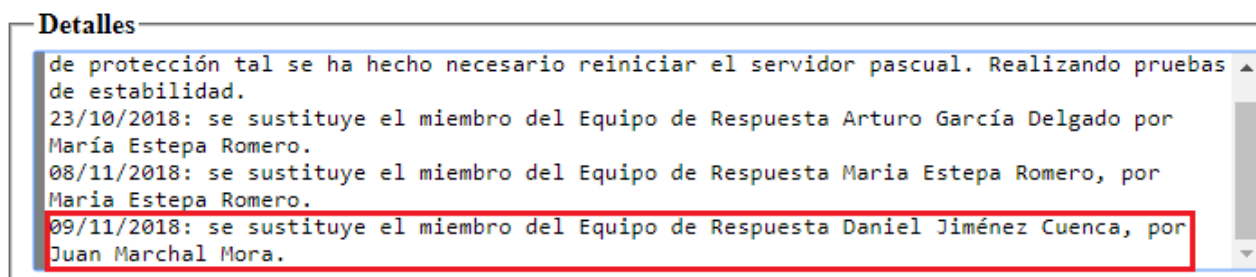


Figura 4-52. Registro en incidencia del cambio de componente en el Equipo de Respuesta.

Además, se tienen en cuenta las siguientes funcionalidades adicionales:

- Se evitan errores como intentar seleccionar más de una vez a una misma persona para formar parte de un mismo Equipo. En ese caso se mostrará una ventana emergente de aviso:



Figura 4-53. Ventana emergente de aviso de personal repetido.

- A la hora de mostrar el desplegable de personal seleccionable, se tiene cuidado de listar únicamente y poder seleccionar entre el personal que se encuentre en activo (según tabla *STAFF*).
- Al ser un cambio importante, se notifica a los tres nuevos miembros del Equipo. Se verá también en el subapartado dedicado al servicio de notificaciones.

El caso en que un componente de algún equipo sufra una baja temporal por asuntos médicos, por ejemplo, o una baja definitiva de la organización, algo factible que pueda suceder, por otro lado, se tratará en el apartado de gestión del personal.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de gestión de Equipos de Respuesta.**

4.4 Servicio de consulta del ENS

Se trata del servicio de consulta de la normativa aplicable del ENS, en concreto, relativo a las medidas de protección que contempla dicho esquema a través de su Guía CCN-STIC 804, de Implantación del ENS.

En este caso no se desarrolla funcionalidad adicional ni se requiere acción por parte del personal responsable de Seguridad de la Información. Se trata de un documento de consulta, fiel reflejo del apartado 5 de la mencionada Guía en lo relativo a Medidas de Protección.

La verificación en este caso consiste en comprobar que, efectivamente, se refleja la información tal cual aparece en la Guía CCN-STIC 804, apartado 5.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de consulta del ENS.**

4.5 Servicio de gestión de personal responsable de Seguridad de la Información

El servicio de gestión de personal está enfocado en los aspectos operativos de funcionamiento de la plataforma Soteria. Su acceso se realiza a través de la pestaña *Personal*, y tiene el siguiente aspecto:

Apellidos	Nombre	Usuario	Correo	Situación
Baños Zapata	Juan	juabanzap	juabanzap@soteria.es	Activo
Cano Maldonado	Pedro	pedcanmal	pedcanmal@soteria.es	Activo
Chica Martos	Blas	blachimar	blachimar@soteria.es	Activo
Espinosa Montero	Luis Miguel	luiespmo	luiespmo@soteria.es	Activo
Estepa Romero	Maria	marestrom	marestrom@soteria.es	Activo
Estrella Garrido	Javier	javestgar	javestgar@soteria.es	Activo
García Delgado	Arturo	artgardel	artgardel@soteria.es	Activo
Gates Wins	Bill	bilgatwin	bilgatwin@soteria.es	Activo
Gómez Martín	José Manuel	josgommar	josgommar@soteria.es	Activo
González Vázquez	David	davgonvaz	davgonvaz@soteria.es	Activo
Ígor Nellerro	Ángel	angigonel	angigonel@soteria.es	Activo
Jiménez Cuenca	Daniel	danjimcue	danjimcue@soteria.es	Activo
Marchal Mora	Juan	juamarmor	juamarmor@soteria.es	Activo
Martín Soria	José María	josmarsor	josmarsor@soteria.es	Activo
Miñambres Estero	Francisco Javier	framinest	framinest@soteria.es	Activo
Nadal Parera	Rafael	rafnadpar	rafnadpar@soteria.es	Activo
Santos Melvar	Silvia	silsanmel	silsanmel@soteria.es	Activo
Sevilla Ovejita	Carmen	carsevove	carsevove@soteria.es	Activo

Alta de nuevo usuario

Apellidos:

Nombre:

Situación:

Figura 4-54. Interfaz para la gestión del personal de Seguridad de la Información.

Se encuentra dividido en dos apartados:

- Tabla con los datos detallados del personal: permite consultar los detalles relativos a cada miembro del personal, así como la actualización de su situación.
- Alta de nuevo usuario: permite añadir personal de reciente incorporación.

Para la gestión efectiva y eficiente del personal se ofrecen los siguientes servicios adicionales:

- El paso de personal de situación *Activo* a cualquier otra situación, puede afectar a las tareas en las que estaba participando hasta el momento, en concreto, si se encontraba participando en un Equipo de Respuesta actualmente en activo, algo crítico. Por tanto, se verifica este hecho y, en caso de que así sea, se sustituye automáticamente de dicho Equipo por otro componente seleccionado aleatoriamente de entre el personal activo, y cuidando de no seleccionar por duplicado al mismo personal.

En la siguiente comprobación, se modificará el estado de una persona que actualmente se encontraba participando en un Equipo de Respuesta, para comprobar que, efectivamente, se refleja el cambio en el Equipo y en la Incidencia a la que se atiende.

Primero, se localiza en la pestaña de gestión de Equipos de Respuesta una persona que se encuentre actualmente participando en algún Equipo. Se elige por ejemplo a Chica Martos, Blas:

201705	20170090	Miñambres Estero, Francisco Javier Ígor Ñelleró, Ángel Chica Martos, Blas	06/09/2017 13:51	No
201706	20170093	Sevilla Ovejita, Carmen Cano Maldonado, Pedro Chica Martos, Blas	18/09/2017 03:26	No
201707	20170096	Tenorio Carrasco, Manuel Santos Melvar, Silvia Estepa Romero, Maria	23/09/2017 08:10	No
201801	20180010	Tenorio Carrasco, Manuel Jiménez Cuenca, Daniel Chica Martos, Blas	29/01/2018 13:55	No
201802	20180014	Vélez Rubio, Lucía Nadal Parera, Rafael Zuckerberg Saverin, Mike	12/02/2018 11:27	No
201803	20180071	Vélez Rubio, Lucía Cano Maldonado, Pedro Gómez Martín, José Manuel	01/08/2018 10:27	No
201804	20180093	Santos Melvar, Silvia Marchal Mora, Juan Sevilla Ovejita, Carmen	10/10/2018 21:45	Si
201805	20180100	Gates Wins, Bill Chica Martos, Blas Zuckerberg Saverin, Mike	29/10/2018 08:46	Si
201806	20180107	Gómez Martín, José Manuel Chica Martos, Blas Ígor Ñelleró, Ángel	22/11/2018 04:35	No
201807	20180133	Chica Martos, Blas Tenorio Carrasco, Manuel Miñambres Estero, Francisco Javier	02/11/2018 08:33	Si

Figura 4-55. Selección de personal participando en uno o varios Equipos de Respuesta.

Como se observa, dicho personal se encuentra participando actualmente en dos Equipos de Respuesta activos: 201805 y 201807.

A continuación, se pasa a la pestaña de gestión de personal y se cambia la situación de dicho personal a baja temporal, seleccionando el icono a su derecha para ejecutar la actualización:

GESTIÓN DE PERSONAL RESPONSABLE DE SEGURIDAD

Apellidos	Nombre	Usuario	Correo	Situación
Baños Zapata	Juan	juabanzap	juabanzap@soteria.es	Activo
Cano Maldonado	Pedro	pedcanmal	pedcanmal@soteria.es	Activo
Chica Martos	Blas	blachimar	blachimar@soteria.es	Baja temporal
Espinosa Montero	Luis Miguel	luiespmon	luiespmon@soteria.es	Activo
Estepa Romero	Maria	marestrom	marestrom@soteria.es	Baja definitiva
Estrella Garrido	Javier	javestgar	javestgar@soteria.es	Vacaciones
García Delgado	Arturo	artgardel	artgardel@soteria.es	Activo
Gates Wins	Bill	bilgatwin	bilgatwin@soteria.es	Activo
Gómez Martín	José Manuel	josgommar	josgommar@soteria.es	Activo
González Vázquez	David	davgonvaz	davgonvaz@soteria.es	Activo
Ígor Nellerro	Ángel	angigonel	angigonel@soteria.es	Activo
Jiménez Cuenca	Daniel	danjimcue	danjimcue@soteria.es	Activo
Marchal Mora	Juan	juamarmor	juamarmor@soteria.es	Activo

Figura 4-56. Cambio de situación del personal.

El resultado es el siguiente, y sirva además como comprobación de la actualización del personal:

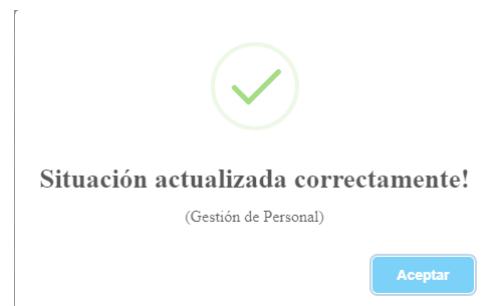


Figura 4-57. Mensaje informando sobre la actualización correcta de la situación.

Zarza Pérez	Josué	joszarper	joszarper@soteria.es	Activo
Zuckerberg Saverin	Mike	mikzucsav	mikzucsav@soteria.es	Activo
Zuera García	Esther	estzuegar	estzuegar@soteria.es	Activo
Chica Martos	Blas	blachimar	blachimar@soteria.es	Baja temporal
Hernández González	Abel	abegonher	abegonher@soteria.es	Baja temporal
López Fuentes	Eva	evalopfue	evalopfue@soteria.es	Baja temporal
Calvo Sotelo	Leopoldo	leocalst	leocalst@soteria.es	Baja definitiva
Rosado Montero	Adela	aderosmon	aderosmon@soteria.es	Baja definitiva
Carrión Vallejo	José	joscarval	joscarval@soteria.es	Vacaciones
González Blanco	Raúl	raugonbla	raugonbla@soteria.es	Vacaciones
López Garrido	Ana	analopgar	analopgar@soteria.es	Vacaciones

Figura 4-58. Actualización del personal en la tabla STAFF.

201705	20170090	Miñambres Estero, Francisco Javier Ígor Ñello, Ángel Chica Martos, Blas	06/09/2017 13:51	No
201706	20170093	Sevilla Ovejita, Carmen Cano Maldonado, Pedro Chica Martos, Blas	18/09/2017 03:26	No
201707	20170096	Tenorio Carrasco, Manuel Santos Melvar, Silvia Estepa Romero, Maria	23/09/2017 08:10	No
201801	20180010	Tenorio Carrasco, Manuel Jiménez Cuenca, Daniel Chica Martos, Blas	29/01/2018 13:55	No
201802	20180014	Vélez Rubio, Lucía Nadal Parera, Rafael Zuckerberg Saverin, Mike	12/02/2018 11:27	No
201803	20180071	Vélez Rubio, Lucía Cano Maldonado, Pedro Gómez Martín, José Manuel	01/08/2018 10:27	No
201804	20180093	Santos Melvar, Silvia Marchal Mora, Juan Sevilla Ovejita, Carmen	10/10/2018 21:45	Si
201805	20180100	Gates Wins, Bill Estepa Romero, Maria Zuckerberg Saverin, Mike	29/10/2018 08:46	Si
201806	20180107	Gómez Martín, José Manuel Chica Martos, Blas Ígor Ñello, Ángel	22/11/2018 04:35	No
201807	20180133	Vélez Rubio, Lucía Tenorio Carrasco, Manuel Miñambres Estero, Francisco Javier	02/11/2018 08:33	Si

Figura 4-59. Situación de los Equipos de Respuesta ante baja temporal.

Como se observa, el personal elegido ya no aparece en los Equipos activos.

Por otro lado, este cambio supone la notificación al nuevo miembro del Equipo. Se verá en el subapartado relativo al servicio de notificaciones.

Respecto al alta de nuevos usuarios, se realizan dos pruebas. En una primera se insertarán caracteres no admitidos en los campos de *Apellidos* y *Nombre* para comprobar que, efectivamente, ambos campos de entrada de datos se encuentran validados:

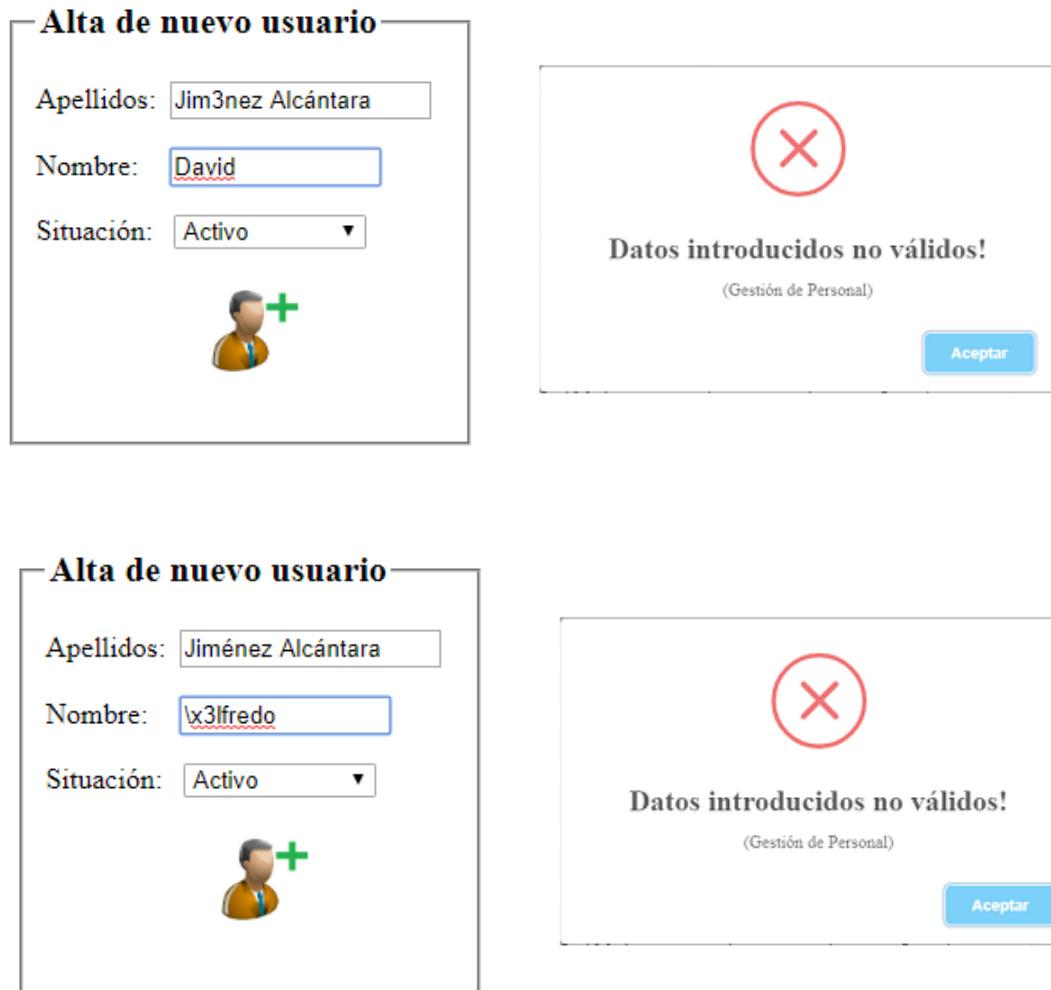


Figura 4-60. Comprobación de validación de la entrada.

Finalmente, se realiza un alta correcta y se comprueba que aparece añadida a la tabla de personal:



Figura 4-61. Alta de nuevo personal correcta, con mensaje emergente de confirmación.

GESTIÓN DE PERSONAL RESPONSABLE DE SEGURIDAD

Apellidos	Nombre	Usuario	Correo	Situación
Baños Zapata	Juan	juabanzap	juabanzap@soteria.es	Activo ▼ 
Cano Maldonado	Pedro	pedcanmal	pedcanmal@soteria.es	Activo ▼ 
Espinosa Montero	Luis Miguel	luiespmo	luiespmo@soteria.es	Activo ▼ 
Estepa Romero	Maria	marestrom	marestrom@soteria.es	Activo ▼ 
Estrella Garrido	Javier	javestgar	javestgar@soteria.es	Activo ▼ 
García Delgado	Arturo	artgardel	artgardel@soteria.es	Activo ▼ 
Gates Wins	Bill	bilgatwin	bilgatwin@soteria.es	Activo ▼ 
Gómez Martín	José Manuel	josgommar	josgommar@soteria.es	Activo ▼ 
González Vázquez	David	davgonvaz	davgonvaz@soteria.es	Activo ▼ 
Ígor Ñellerro	Ángel	angigonel	angigonel@soteria.es	Activo ▼ 
Jiménez Alcántara	Alfredo	alfjimalc	alfjimalc@soteria.es	Activo ▼ 
Jiménez Cuenca	Daniel	danjimcue	danjimcue@soteria.es	Activo ▼ 
Marchal Mora	Juan	juamarmor	juamarmor@soteria.es	Activo ▼ 
Martín Soria	José María	josmarsor	josmarsor@soteria.es	Activo ▼ 

Figura 4-62. El alta se refleja correctamente en la tabla del personal (STAFF).

El proceso lleva asociado también una notificación al personal recién incorporado, confirmando de esta manera que ha sido añadido a la BBDD de Soteria correctamente.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de gestión de personal responsable de Seguridad de la Información.**

4.6 Servicio de Análisis

Mediante el servicio de análisis se ofrecen diversas estadísticas y gráficas cuyo objetivo es el apoyo a la decisión del mando. Mediante este subapartado se ponen de manifiesto las distintas posibilidades que ofrece, seleccionando cada una de las opciones posibles y comprobando sus resultados.

La interfaz web del servicio es la siguiente:

Seleccione el tipo de información y el periodo

Datos relativos a:

☒ **Anual**
☐ **Mensual**

☐ **Intervalo:**

Inicio:
Fin:

Tipo de Gráfica:



Figura 4-63. Interfaz web del servicio de Análisis.

Como se observa en la figura anterior, se ofrece una lista desplegable donde se puede seleccionar sobre qué datos se desea realizar el análisis. Además, según el caso, se ofrece la posibilidad de aplicarlo sobre un intervalo anual, mensual (a lo largo de un año), o bien por intervalo definido de tiempo. A su vez, se podrán seleccionar diferentes tipos de gráficas para cada apartado. Según el tipo de datos elegidos y de cara a evitar problemas de visualización, se limitan ciertas partes de selección temporal y de tipo de gráfica.

A continuación, se muestran las estadísticas y gráficas que ofrece la plataforma, y se intentará comprobar su validez.

En primer lugar, se generan las estadísticas y gráficas relativas al número de incidentes de manera anual:

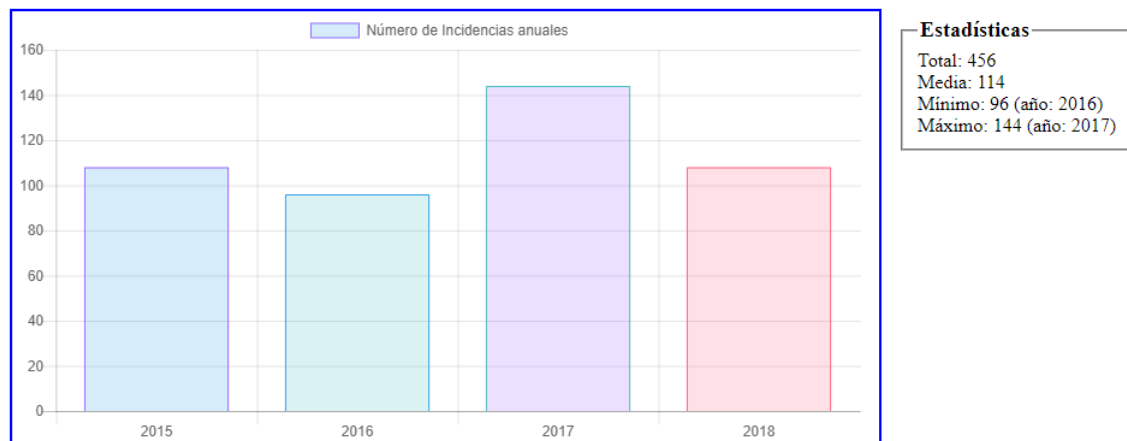


Figura 4-64. Número de incidencias por año.

Los números que indica la gráfica son (se muestran al pasar el punto del ratón sobre la barra correspondiente): 108, 96, 144 y 108, para los años 2015, 2016, 2017 y 2018, respectivamente. Para comprobarlo, se realiza el recuento conectándose a la BBDD desde la línea de comandos:

```
MariaDB [soteria]> select count(id) from INCIDENTS where id<20160000;
+-----+
| count(id) |
+-----+
|      108 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where id>20160000 and id<20170000;
+-----+
| count(id) |
+-----+
|       96 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where id>20170000 and id<20180000;
+-----+
| count(id) |
+-----+
|      144 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where id>20180000;
+-----+
| count(id) |
+-----+
|      108 |
+-----+
1 row in set (0.000 sec)
```

Figura 4-65. Recuento número de incidencias por año desde conexión directa a BBDD.

Como se puede observar, los números coinciden.

A continuación, se prueba generando las estadísticas y gráficas por mes para un mes concreto, por ejemplo, 2017:

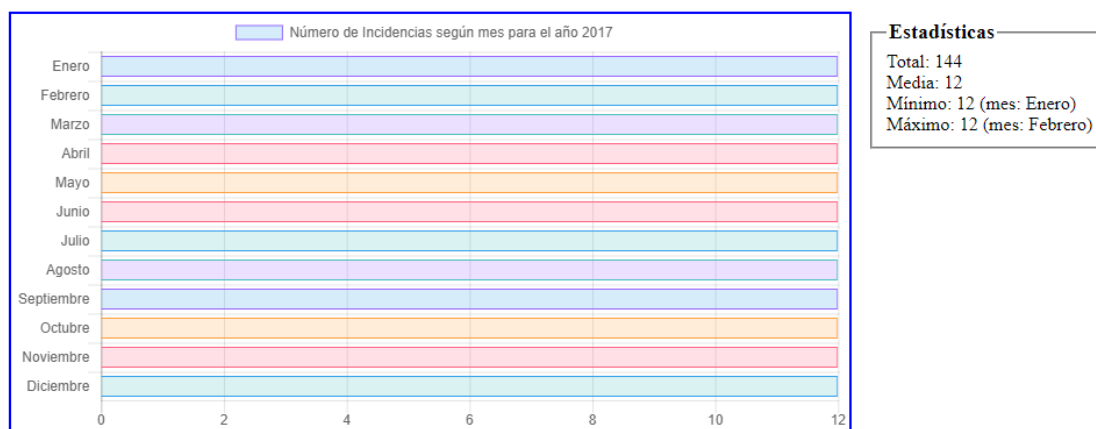


Figura 4-66. Número de incidencias mensual para el año 2017.

Se ha seleccionado para probar en esta ocasión la gráfica de barra horizontales.

En este caso la comprobación es directa, pues a la hora de generar los datasets para las pruebas, el número aleatorio de incidencias generado para cada año se reparte por igual para cada uno de los meses: $144 / 12 = 12$. **Los datos en sí son irrelevantes, lo importante es que se generen las gráficas y estadísticas correctamente.**

Si se selecciona un intervalo de tiempo definido, 20/06/2018 a 20/10/2018, por ejemplo:

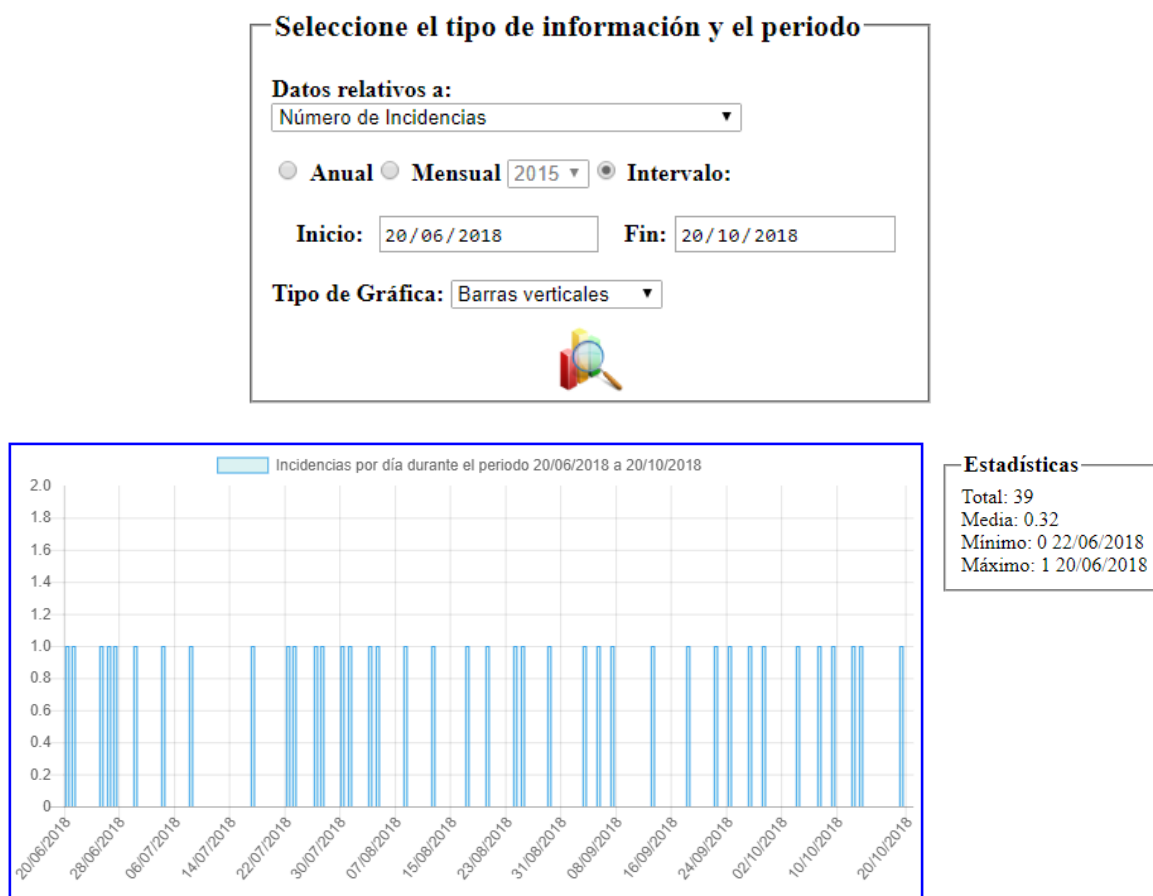


Figura 4-67. Número de incidencias para el periodo 20/06/2018 a 20/10/2018.

Las estadísticas indican el número total de incidencias, la media diaria y los valores mínimo y máximo para cada día. En el caso de que haya varias coincidencias para los valores mínimo y máximo, por defecto muestra el primer día.

Se puede comprobar que el recuento es correcto mediante conexión directa a la BBDD:

```
MariaDB [soteria]> select count(id) from INCIDENTS where detect_date>=201806200000 and detect_date<=201810200000;
+-----+
| count(id) |
+-----+
|          39 |
+-----+
1 row in set (0.001 sec)
```

Figura 4-68. Recuento de incidencias para el periodo 20/06/2018 a 20/10/2018.

Seguidamente se generan las estadísticas y la gráfica relativa al intervalo que transcurre entre la detección y la notificación:

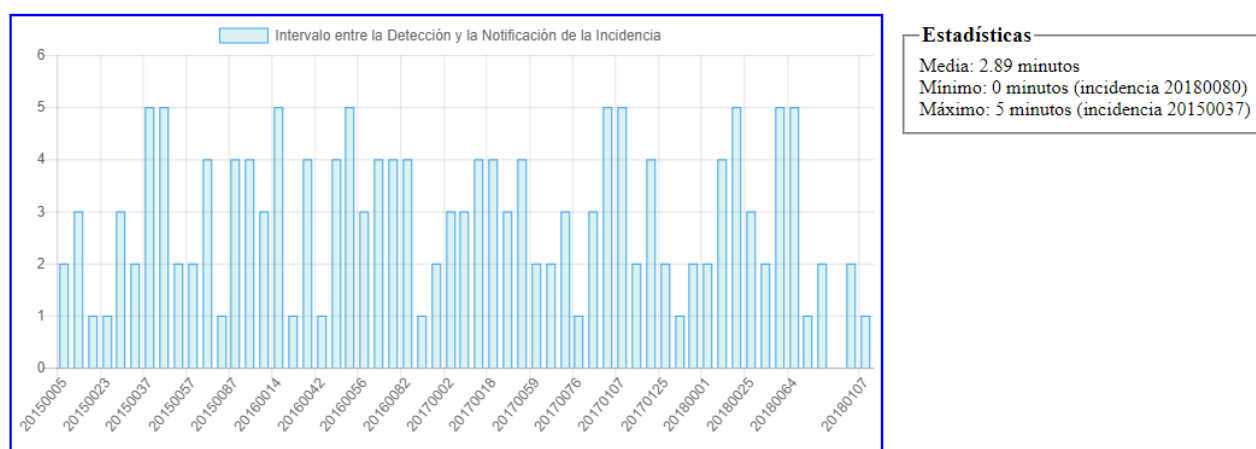


Figura 4-69. Intervalo entre la Detección y la Notificación de las incidencias.

Como se observa en la figura anterior, se muestran la media, el valor mínimo y el valor máximo, en minutos, de dicho intervalo. Debido al tipo de estadísticas de que se trata, para que se pueda considerar un valor medio fiable se requiere un gran número de valores representativos, por lo que se realiza para el conjunto de incidencias. Debido a que se recogen numerosos valores, la gráfica solamente muestra algunos valores de manera discreta, si bien las estadísticas se calculan sobre el total de valores. Para comprobarlo, se seleccionan algunas incidencias y se comprueba que la diferencia mostrada es la correcta. Si se pasa el ratón sobre el gráfico, se observará que de las incidencias que se muestran de manera discreta, indica el número de identificación. Haciendo la prueba se obtiene, por ejemplo, que en la incidencia 20180064 fue de 5 minutos, mientras que en la incidencia 20180088 el intervalo fue de 2 minutos. Comprobándolo mediante conexión directa a la BBDD:

```
MariaDB [soteria]> select id,detect_date,notify_date from INCIDENTS where id=20180088 or id=20180064;
+-----+-----+-----+
| id      | detect_date | notify_date |
+-----+-----+-----+
| 20180064 | 201808031846 | 03/08/2018 18:51 |
| 20180088 | 201810220743 | 22/10/2018 07:45 |
+-----+-----+-----+
2 rows in set (0.000 sec)
```

Figura 4-70. Comprobación intervalo entre Detección y Notificación de las incidencias.

Se pasa ahora a ofrecer las estadísticas y gráficas relativas al intervalo entre la Detección y el Cierre de las incidencias, en esta ocasión midiéndose en días:

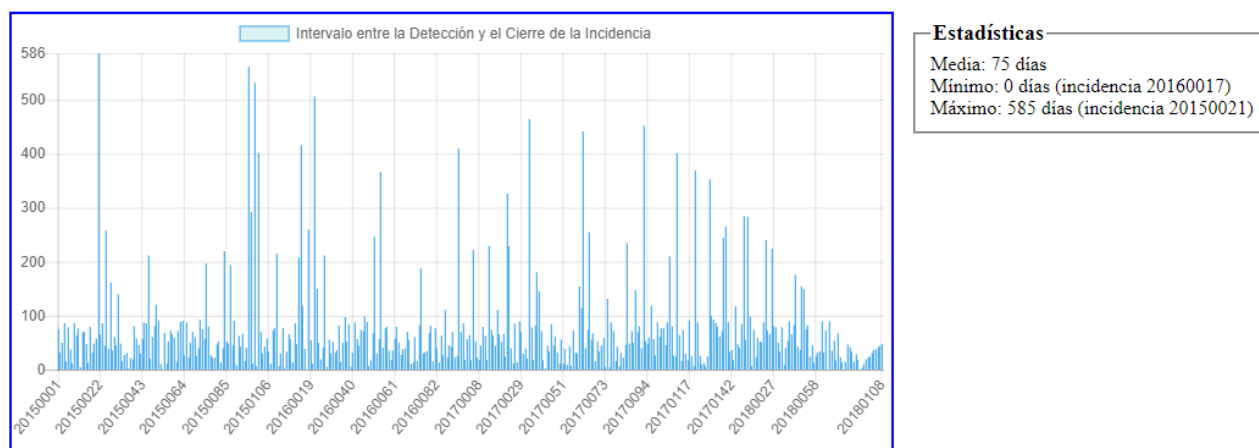


Figura 4-71. Intervalo entre la Detección y el Cierre de las incidencias.

Como en los casos anteriores, se selecciona sobre la gráfica dos incidencias concretas y se comprueba que los valores coinciden. En este caso, la incidencia 20170061 indica 441 días, mientras que la incidencia 20180055 indica 45 días. Comprobándolo mediante conexión directa a la BBDD:

```
MariaDB [soteria]> select id,detect_date,closing_date from INCIDENTS where id=20170061 or id=20180055;
```

id	detect_date	closing_date
20170061	201706020220	20180817
20180055	201807041326	20180818

2 rows in set (0.000 sec)

Figura 4-72. Comprobación intervalo entre la Detección y el Cierre de las incidencias.

En el caso de los falsos positivos y los falsos negativos, lo importante en este caso son las estadísticas, aunque en la interfaz también se hace una representación gráfica:

Estadísticas

Total: 43
Relación FP/incidencias: 9.43 %
Tiempo medio entre FP (días): 33

Figura 4-73. Estadísticas relativas a los falsos positivos detectados en la plataforma.

Estadísticas

Total: 17
Relación FN/incidencias: 3.73 %
Tiempo medio entre FN (días): 83

Figura 4-74. Estadísticas relativas a los falsos negativos detectados en la plataforma.

Comprobándolo mediante conexión directa a la BBDD:

```

MariaDB [soteria]> select count(id) from INCIDENTS where false_p='S';
+-----+
| count(id) |
+-----+
|         43 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where false_n='S';
+-----+
| count(id) |
+-----+
|         17 |
+-----+
1 row in set (0.000 sec)

```

Figura 4-75. Comprobación estadísticas de falsos positivos y falsos negativos detectados.

Para el cálculo del tiempo medio entre falsos positivos/negativos se ha contabilizado el total de días desde el inicio del registro: desde enero de 2015 hasta noviembre de 2018.

El siguiente paso es el estudio de la distribución de incidencias por severidad. En este caso se separa según el año y según las cuatro categorías de severidad establecidas:

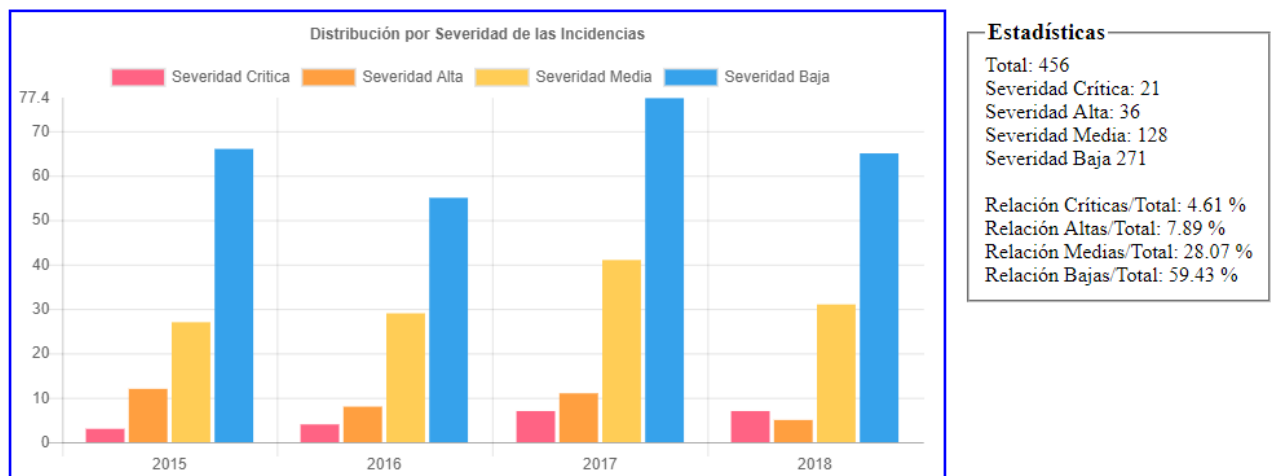


Figura 4-76. Distribución por Severidad de las Incidencias.

Para la comprobación basta seleccionar un año y realizar el conteo para cada categoría de severidad. Para el año 2017, por ejemplo, la gráfica indica: 7, 11, 41 y 85 incidencias para las categorías de Crítica, Alta, Media y Baja, respectivamente. Comprobándolo mediante conexión directa a la BBDD:

```

MariaDB [soteria]> select count(id) from INCIDENTS where severity='C' and id>20170000 and id<20180000;
+-----+
| count(id) |
+-----+
|          7 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where severity='A' and id>20170000 and id<20180000;
+-----+
| count(id) |
+-----+
|         11 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where severity='M' and id>20170000 and id<20180000;
+-----+
| count(id) |
+-----+
|         41 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where severity='B' and id>20170000 and id<20180000;
+-----+
| count(id) |
+-----+
|         85 |
+-----+
1 row in set (0.000 sec)

```

Figura 4-77. Comprobación de la distribución por Severidad de las Incidencias.

Respecto a la distribución por categorías de las incidencias (tipo):

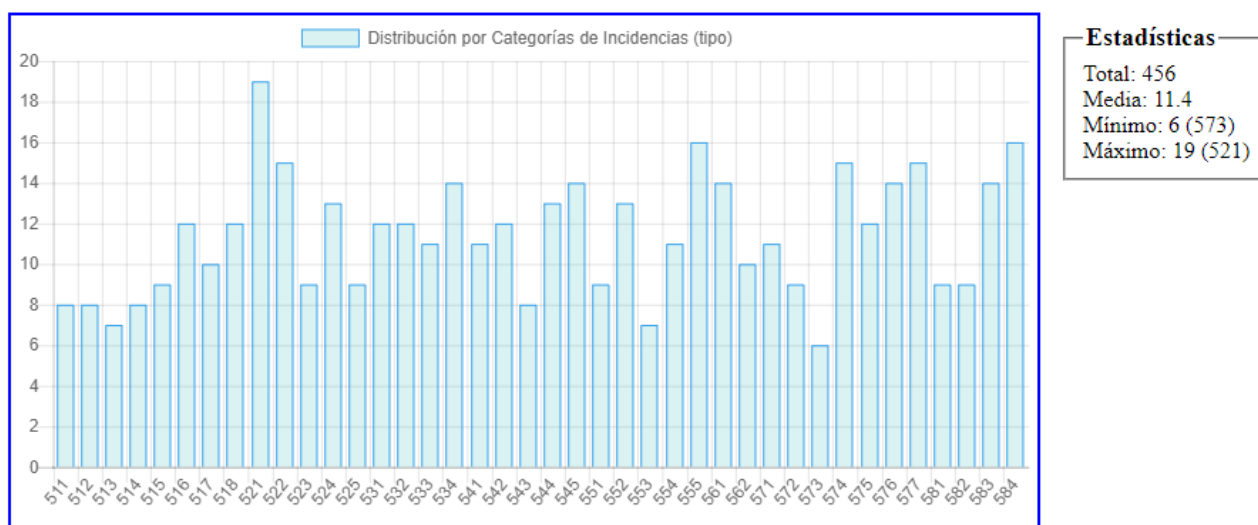


Figura 4-78. Distribución por Categorías de las Incidencias (tipo).

Para la comprobación, se obtiene el conteo, por ejemplo, de los tipos que se han repetido con menos y con más asiduidad (573 y 521, respectivamente):

```

MariaDB [soteria]> select count(id) from INCIDENTS where type=573;
+-----+
| count(id) |
+-----+
|         6 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where type=521;
+-----+
| count(id) |
+-----+
|        19 |
+-----+
1 row in set (0.000 sec)

```

Figura 4-79. Comprobación de la distribución por Categorías de las Incidencias (tipo).

El siguiente paso es la comprobación respecto a la generación de estadísticas relativas a los Equipos de Respuesta. Aunque en la interfaz también se muestra la gráfica correspondiente, este aspecto no es relevante. Lo relevante en este caso son las estadísticas:

Estadísticas	
Número de Equipos de Respuesta:	21
Número de Incidencias totales:	456
Relación CSIRT's/Nº de Incidencias:	4.61 %

Figura 4-80. Estadísticas relativas a los Equipos de Respuesta conformados.

Comprobándolo mediante conexión directa a la BBDD:

```

MariaDB [soteria]> select count(id) from INCIDENTS where CSIRT='S';
+-----+
| count(id) |
+-----+
|        21 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS;
+-----+
| count(id) |
+-----+
|       456 |
+-----+
1 row in set (0.000 sec)

```

Figura 4-81. Comprobación de estadísticas sobre Equipos de Respuesta conformados.

El siguiente estudio consiste en comprobar el escalado de las incidencias:

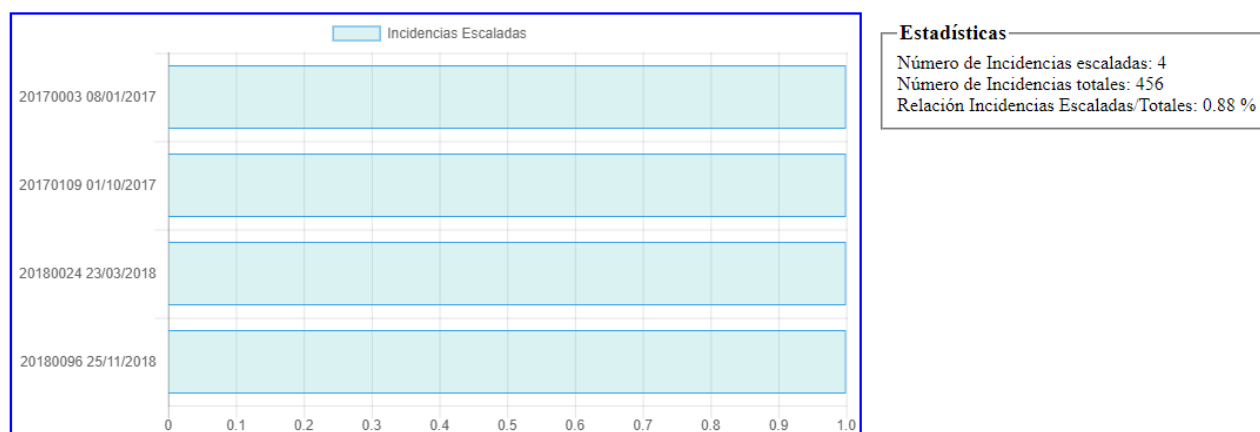


Figura 4-82. Escalado de incidencias.

En este caso hay que buscar aquellas incidencias que contengan la cadena “se escala la incidencia”, insertada en el campo de detalles. Comprobándolo mediante conexión directa a la BBDD:

```
MariaDB [soteria]> select id from INCIDENTS where details LIKE "%se escala la incidencia%";
+-----+
| id      |
+-----+
| 20170003 |
| 20170109 |
| 20180024 |
| 20180096 |
+-----+
4 rows in set (0.001 sec)
```

Figura 4-83. Comprobación del escalado de incidencias.

Por último, respecto a la distribución de incidencias según si el origen está en el sistema SIEM, o bien ha sido alta manual por parte del personal responsable de Seguridad de la Información:

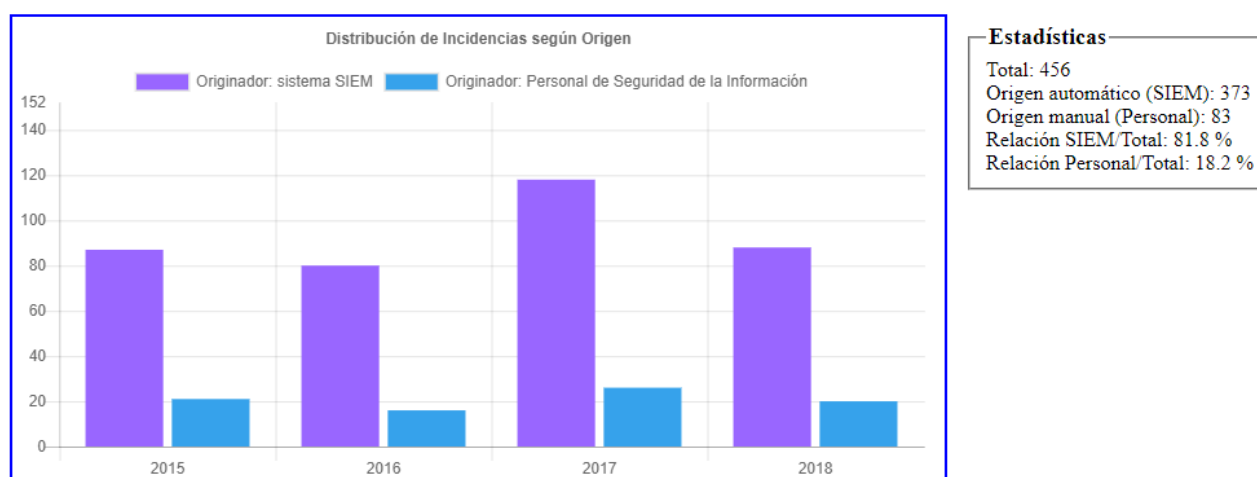


Figura 4-84. Distribución de Incidencias según Origen (SIEM / Personal).

Las cifras que se indica sobre la misma gráfica son:

- SIEM: 87, 80, 118 y 88, para los años 2015 a 2018, respectivamente.
- Personal: 21, 16, 26, 20, para los años 2015 a 2018, respectivamente.

Para comprobarlo, se realiza el conteo para cada año mediante conexión directa a la BBDD:

```
MariaDB [soteria]> select count(id) from INCIDENTS where originator='SIEM' and id>20150000 and id<20160000;
+-----+
| count(id) |
+-----+
|         87 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where originator<>'SIEM' and id>20150000 and id<20160000;
+-----+
| count(id) |
+-----+
|         21 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where originator='SIEM' and id>20160000 and id<20170000;
+-----+
| count(id) |
+-----+
|         80 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where originator<>'SIEM' and id>20160000 and id<20170000;
+-----+
| count(id) |
+-----+
|         16 |
+-----+
1 row in set (0.000 sec)
```

Figura 4-85. Comprobación distribución de Incidencias según Origen, años 2015 y 2016.

```
MariaDB [soteria]> select count(id) from INCIDENTS where originator='SIEM' and id>20170000 and id<20180000;
+-----+
| count(id) |
+-----+
|        118 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where originator<>'SIEM' and id>20170000 and id<20180000;
+-----+
| count(id) |
+-----+
|         26 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where originator='SIEM' and id>20180000;
+-----+
| count(id) |
+-----+
|         88 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select count(id) from INCIDENTS where originator<>'SIEM' and id>20180000;
+-----+
| count(id) |
+-----+
|         20 |
+-----+
1 row in set (0.000 sec)
```

Figura 4-86. Comprobación distribución de Incidencias según Origen, años 2017 y 2018.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de Análisis.**

4.7 Servicio de gestión de Conocimiento

El servicio de gestión de Conocimiento se encuentra dividido en dos secciones:

Seleccione el histórico que desee consultar

Incidentes por categoría:
 5.1.1 [MP.IF.1] ÁREAS SEPARADAS Y CON CONTROL DE ACCESO ▼



Incidentes notificados: 20170003 ▼ 

Figura 4-87. Servicio de gestión de Conocimiento.

- Incidentes por categoría: ofrece un compendio clasificado por categorías (tipo) de incidentes según la clasificación que ofrece la Guía CCN-STIC 804, de Implantación del ENS. Su objetivo es aglutinar el histórico de las medidas de protección aplicadas a lo largo de la vida de las incidencias que se encuentren ya cerradas y, por tanto, solucionado el problema que atendían. Si se accede a cualquiera de las entradas del listado, por ejemplo, la relativa a 5.1.1, el aspecto que muestra la interfaz es el siguiente:

5.1.1 [MP.IF.1] ÁREAS SEPARADAS Y CON CONTROL DE ACCESO

MEDIDAS DE PROTECCIÓN

DETALLES

INFORMES

Código Aplicado

Observaciones

328

No ▼

329

No ▼

Se puede aplicar en su lugar la siguiente medida substitutiva: bla bla ▲ ▼

330

Sí ▼

Precisa actualización del software: bla bla bla. Aplicada correctamente.

331

Sí ▼

Aplicada correctamente.

332

No ▼

Precisa actualización del software: bla bla bla.

Se inician las acciones para la resolución de la incidencia. Se aplica la medida de protección tal y se observa el comportamiento del sistema. Verificada su estabilidad, se aplica la medida de protección pascual. Se comprueba que la incidencia queda resuelta.

Código Aplicado

Observaciones

328

No ▼

Se inician las acciones para la resolución de la incidencia. Se aplica la medida de protección tal y se observa el comportamiento del sistema. Verificada su estabilidad, se aplica la medida de protección pascual. Se comprueba

518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador:
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-

Figura 4-88. Incidentes por categoría.

Para cada categoría que se elija, se muestra la información relativa a los campos *pm_info*, *details* y *reports* de todas aquellas incidencias cuyo campo *type* coincida con la categoría elegida. De esta manera se puede analizar caso a caso cómo se han ido

aplicando las medidas de protección, cómo se han ido solucionando los inconvenientes encontrados, etcétera.

Constituye, por tanto, una **referencia imprescindible para el personal de seguridad, de cara a atender incidencias del mismo tipo en el futuro.**

Para demarcar la información relativa a cada incidencia cerrada, se utiliza el separador:

Figura 4-89. Separador para la información de cada incidencia.

Se puede comprobar que, para cada tipo, el listado de medidas de protección se corresponde con los que figuran en la pestaña ENS. Por ejemplo, para el caso del tipo 5.1.1, las medidas de protección que contiene son la 328 a la 332, tal como aparece en la Figura 4-87, y tal como aparece en la pestaña ENS. La comprobación en este caso se realiza de manera visual para cada tipo de incidencia.

Respecto al contenido, se hará una pequeña prueba para comprobar que se ha clasificado correctamente y se ha extraído correctamente la información de la incidencia que correspondía. Si se vuelve a observar la Figura 4-87, aparece en segundo lugar la información de una incidencia con determinada información en sus campos *details* y *reports*. Como se muestran en orden creciente de la ID de cada incidencia, con la siguiente consulta se puede determinar a qué incidencia corresponde:

```
MariaDB [soteria]> select id from INCIDENTS where type=511;
+-----+
| id    |
+-----+
| 20150017 |
| 20150030 |
| 20150056 |
| 20150092 |
| 20160070 |
| 20160083 |
| 20180043 |
| 20180085 |
+-----+
8 rows in set (0.000 sec)
```

Figura 4-90. Localización incidencia según tipo y orden en la lista de Conocimiento.

Se puede inferir que se trata de la incidencia con ID 20150030. Efectivamente, si abrimos la consulta detallada de la información de dicha incidencia, aparte de comprobar de que, efectivamente, está cerrada, se ofrece la siguiente información:

Detalles

Se inician las acciones para la resolución de la incidencia. Se aplica la medida de protección tal y se observa el comportamiento del sistema. Verificada su estabilidad, se aplica la medida de protección pascual. Se comprueba que la incidencia queda resuelta.

Informes

518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador:
<https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador>

Figura 4-91. Información de la incidencia localizada.

Que coincide con la información que se mostraba en la base de Conocimiento.

Siguiendo este procedimiento se puede verificar que, efectivamente, se realiza la extracción correcta de la información de las incidencias cerradas que se encuentran relacionadas por el mismo tipo de incidencia.

- **Incidencias notificadas:** ofrece el listado de incidencias contenido en la tabla NOTIFIED, es decir, la recopilación de incidencias de mayor severidad (Crítica y Alta) actualmente en activo (Abiertas o en Cuarentena). El objetivo es ofrecer un lugar donde consultar las incidencias de mayor severidad que se encuentran pendientes de resolver. Son, por tanto, las incidencias donde más se tienen que centrar el personal responsable de Seguridad de la Información en cada momento.

Desde la interfaz de Conocimiento, si se necesita, se puede seleccionar cualquier incidencia del listado y se redirigirá hacia la interfaz de gestión de incidencias donde se mostrará su información de manera detallada:

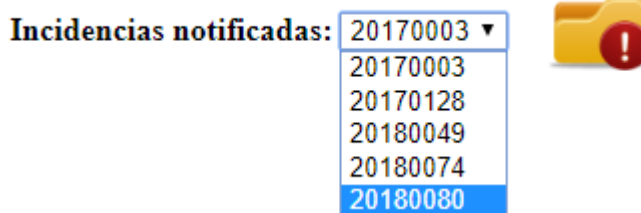


Figura 4-92. Selección de una incidencia notificada.

Figura 4-93. Selección de una incidencia notificada. Gestión de la incidencia.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de gestión de Conocimiento.**

4.8 Servicio de Información

El servicio de información ofrece información de consulta, referencia e interés relacionada con el ámbito de este trabajo en particular, y con el ámbito general de la Seguridad de la Información y la Protección de Datos.

Se encuentra dividido en 4 secciones:

- Información sobre Soteria, porqué dicha denominación.
- Enlaces a normativa de interés.
- Revistas y libros del sector de la Seguridad de la Información.
- Servicios de noticias e información de interés.

El aspecto gráfico es el siguiente:



Figura 4-94. Servicio de Información.

La verificación en este caso pasa por comprobar que cada uno de los enlaces a la información proporcionados conducen efectivamente a la dirección deseada.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de gestión de Información.**

4.9 Servicio de simulación del sistema SIEM

La simulación del sistema SIEM permite generar incidencias de manera automática, haciendo las veces de un sistema real.

Para comprobar su funcionamiento, se programa el gestor de planificación de tareas de Linux, CRON, de tal manera que se ejecute periódicamente el archivo Python que simula el funcionamiento del sistema SIEM (siem.py). Por ejemplo, para acelerar la ejecución y la comprobación, se puede programar para ejecutarse cada hora:

```
# Se prueba a ejecutar la simulacion del sistema SIEM cada hora:
@hourly python /var/www/Soteria/src/siem.py
```

Figura 4-95. Ejecución del script siem.py cada hora.

En efecto, para comprobar que realiza su función e inserta una nueva incidencia a la siguiente hora en punto, se puede extraer el valor máximo del campo *ID* de la tabla *INCIDENTS* antes y después de la siguiente hora en punto:

```
MariaDB [soteria]> select max(id) from INCIDENTS;
+-----+
| max(id) |
+-----+
| 20180108 |
+-----+
1 row in set (0.000 sec)

MariaDB [soteria]> select max(id) from INCIDENTS;
+-----+
| max(id) |
+-----+
| 20180109 |
+-----+
1 row in set (0.000 sec)
```

Figura 4-96. Comprobación de la ejecución del script siem.py cada hora.

Se puede extraer los datos de la fecha de detección para comprobar que, efectivamente, se acaba de generar:

```
MariaDB [soteria]> select id,detect_date,severity,notify_date,status from INCIDENTS where id=20180109;
+-----+-----+-----+-----+-----+
| id      | detect_date | severity | notify_date | status |
+-----+-----+-----+-----+-----+
| 20180109 | 201811092300 | A       | 09/11/2018 23:01 | U      |
+-----+-----+-----+-----+-----+
1 row in set (0.000 sec)
```

Figura 4-97. Información de la incidencia generada desde el simulador del sistema SIEM.

En la figura anterior se puede observar que se ha generado la incidencia con ID 20180109 de manera automática a las 23:00 del día 09/11/2018, y que, al ser de categoría Alta, se ha notificado 1 minuto después, a las 23:01 del día 09/11/2018. El servicio de notificaciones se verá en el siguiente subapartado. Destacar, por otro lado, que la incidencia se ha creado con el estado de Cuarentena (U), como está previsto para las incidencias con origen en el sistema SIEM.

El resto de la funcionalidad a comprobar consiste en dejar pasar varias horas para que se generen diferentes incidencias con diversa severidad.

La programación horaria de 1 hora establecida se debe a que son pruebas de verificación. Normalmente no habría un ritmo tan alto. Lo usual es que haya varias horas o incluso una media de días para generación real de incidencias. Para las pruebas se ha acelerado su ejecución, pero lo normal es establecer un ritmo diario, o incluso de varios días entre incidencia e incidencia.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de simulación del sistema SIEM.**

4.10 Servicio de Notificaciones

Este servicio se considera esencial para asegurar la operatividad de la plataforma, mantener informado al personal responsable de Seguridad de la Información y para el cumplimiento de la normativa legal vigente.

Según se ha expuesto en el apartado 2.5 *Normativa y legislación*, en el ámbito de las AA.PP., se notificarán al CCN aquellos incidentes que tengan un impacto significativo en la Seguridad de la Información manejada y en los servicios prestados. Normalmente esta notificación debería hacerse por parte del responsable de la organización, ya que se trata de una comunicación de organismo a organismo.

Por otro lado, como se ha expuesto igualmente en apartados anteriores, la detección de una posible filtración de datos personales conlleva, como mínimo, que el responsable del tratamiento de los datos personales, es decir, el responsable de la organización, notifique el incidente a la AEPD.

Por tanto, se precisa implementar un mecanismo para que la incidencia sea notificada al personal responsable de Seguridad de la Información (notificación técnica).

Cabe aclarar que la funcionalidad que se desarrolla en la plataforma Soteria se refiere a la notificación técnica de la incidencia, la cual servirá de base para las notificaciones finales que procedan por parte del responsable de la organización al CCN y/o a la AEPD.

Lo primero que se hace necesario es listar y describir de manera breve todas aquellas circunstancias que se consideren de suficiente importancia como para ser notificadas:

- Notificación de posible violación de la seguridad de los datos personales: Por tanto, cuando la incidencia sea del tipo 571 (código ENS: 571, descripción: DATOS DE CARÁCTER PERSONAL), además de ser categorizada como severidad Crítica, se notificará con un mensaje personalizado. Dicho mensaje, en este caso, tiene la siguiente apariencia:

ATENCION: posible violacion de la seguridad de los datos personales!



B C M <bchimar@outlook.es>

08/11/2018 2:40

Para: B C M

Se ha detectado una incidencia de severidad C en la que participa usted, que puede suponer una violacion de la seguridad de los datos personales. ID: 20180211.Codigo ENS: 571. Descripcion: 5.7.1 [MP.INFO.1] DATOS DE CARACTER PERSONAL.

Figura 4-98. Notificación ante posible violación de la seguridad de los datos personales.

- Notificación de incidencias de severidad Crítica o Alta: otro caso de uso habitual sería la notificación ante la detección de una incidencia de severidad Crítica o Alta. El procedimiento sería muy similar al del caso anterior, pero el asunto y el texto del mensaje que se remite serían distintos, en este caso:

ATENCION: detectada nueva incidencia!



B C M <bchimar@outlook.es>

09/11/2018 23:01

Para: B C M

Se ha detectado una incidencia de severidad A, en la que participa usted. ID: 20180109. Codigo ENS: 517. Descripcion: 5.1.7 [MP.IF.7] REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO.

Figura 4-99. Notificación ante la detección de una incidencia de severidad Crítica o Alta.

- Escalado de una incidencia: el escalado es un factor importante porque indica que no se tiene capacidad para atender una incidencia, por lo que se eleva a un órgano superior. La notificación en este caso iría dirigida hacia ese órgano superior para avisar sobre la circunstancia. La apariencia del mensaje en este caso sería la siguiente:

ATENCION: se ha escalado una incidencia!



B C M <bchimar@outlook.es>

09/11/2018 19:51

Para: B C M

Se ruega atiendan la incidencia 20180096.

Gracias y un cordial saludo.

Figura 4-100. Notificación ante el escalado de una incidencia a un órgano superior.

- Notificación de alta de nuevo usuario: el proceso de alta de nuevo usuario en la plataforma Soteria culmina con la notificación de incorporación a dicho usuario. El aspecto es el que se muestra a continuación:

ATENCION: ha sido dado de alta correctamente!



B C M <bchimar@outlook.es>

09/11/2018 16:34

Para: B C M

Bienvenido!

Ha sido incorporado a la Base de Datos de la plataforma Soteria correctamente.

Figura 4-101. Notificación de alta en la plataforma Soteria.

- Sustitución de un componente de un Equipo de Respuesta: por motivos logísticos u organizacionales, es posible que se necesite que un componente de un Equipo deba ser sustituido por otro compañero. En este caso el mensaje tiene la siguiente apariencia:

ATENCION: se ha modificado un Equipo de Respuesta!



B C M <bchimar@outlook.es>

0:27

Para: B C M

Se ha modificado el Equipo de Respuesta con ID: 201805, en el que participa usted.

Figura 4-102. Notificación de cambio de un componente de un Equipo de Respuesta.

- Sustitución de un componente de un Equipo de Respuesta por baja: en este caso se cubre la circunstancia sobrevenida de que un componente de un Equipo de Respuesta en activo cause baja por cualquier motivo: baja médica, baja definitiva, etcétera. En este caso el mensaje que se remite tiene la siguiente apariencia:

ATENCION: ha sido seleccionado como componente de un Equipo de Respuesta!



B C M <bchimar@outlook.es>

09/11/2018 13:10

Para: B C M

Ha sido seleccionado para formar parte del Equipo de Respuesta con ID 201815, por baja de personal.

Figura 4-103. Notificación cambio de un componente de un Equipo por baja.

- Notificación debido a la conformación de un Equipo de Respuesta: no requiere desarrollar funcionalidad propia, pues la conformación de un Equipo de Respuesta viene condicionada por una severidad Crítica de la incidencia, lo cual supone notificación, estando por tanto ya incluida la notificación a los tres componentes del Equipo.

Las notificaciones se envían por defecto al responsable de la incidencia afectada y, en el caso de que cuente con un Equipo de Respuesta, se envía a los tres componentes del mismo.

En todos los casos se comprueba que, efectivamente, bajo cualquiera de las circunstancias listadas, se recibe el correspondiente correo de notificación.

Llegados a ese punto, se puede concluir, por tanto, que **queda verificado el conjunto de la funcionalidad que ofrece el servicio de Notificaciones.**

4.11 Servicio de validación de la entrada

Este servicio se ha desarrollado y comprobado a lo largo del servicio de gestión de incidencias de Seguridad de la Información, donde se ponía de manifiesto que la validación de la entrada de datos funcionaba correctamente y no era posible introducir caracteres no permitidos.

Por tanto, **queda verificado el conjunto de la funcionalidad que ofrece el servicio de validación de la entrada de datos desde la interfaz web.**

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones de interés

Como colofón a la documentación, una vez concluido el trabajo, se recogen las conclusiones finales de interés a las que se ha podido llegar. En los siguientes subapartados se verificará el logro de los objetivos planteados inicialmente. También se propondrán una serie de líneas de trabajo futuras de cara a continuar, ampliar y mejorar la plataforma Soteria resultado del presente Trabajo de Fin de Máster.

En primer lugar, se exponen las conclusiones de mayor interés.

El presente trabajo ha sido todo un reto. Antes de tomar la decisión de elegir esta línea de trabajo, el autor tenía claro la dificultad que entrañaba y el trabajo que suponía, sin que ello supusiera algún tipo de óbice para encararlo. El trabajo aún:

- Diferentes tecnologías y técnicas para el desarrollo de servicios web.
- Diferentes ámbitos de gestión de incidentes de Seguridad de la Información.
- Diferentes áreas de la Seguridad de la Información.

Tal como se expuso en los capítulos introductorios, en la actualidad las AA.PP. en general, ni el MINISDEF en particular, cuenta con una herramienta que sintetice la funcionalidad que ofrece la plataforma Soteria. Lo más similar sería la herramienta del CCN LUCIA, con los inconvenientes que ya se plantearon en el apartado *1.2 Motivación*.

Por tanto y como primera conclusión, **destacar la satisfacción de poder hacer realidad esa idea primigenia de integrar el conjunto de servicios planteado bajo una misma plataforma de gestión.**

Uno de los mayores retos y ajustes a lo largo del trabajo ha sido poder determinar con claridad aquellos parámetros de las incidencias que deben ser categorizados como **fundamentales** y que debe impedirse su modificación o borrado, al objeto de **mantener la trazabilidad**. No resulta en absoluto sencillo intentar adoptar un criterio, pues se plantea el **compromiso Flexibilidad↔Trazabilidad**:

- Flexibilidad: se permite editar los campos, incrementando la funcionalidad.
- Trazabilidad: se limita la edición de algunos campos para asegurar la trazabilidad.

Tal como se propone en el apartado *5.3 Líneas futuras de trabajo*, se requiere un estudio previo al despliegue de la plataforma para determinar qué parámetros pueden ser modificados a lo largo de la vida de una incidencia, y, en cualquier caso, los criterios adoptados vendrán determinados en gran parte por la política de seguridad que establezca la organización.

No se puede cerrar este apartado sin recordar las bondades de contar con una plataforma de estas características:

- Reducción de los tiempos de indisponibilidad.
- Reducción de los tiempos de recuperación.
- Aminoración considerable del lucro cesante (no aplicable en el Sector Público, en este caso).
- Reducción de amenazas: mejorada notablemente en el caso de contar con un sistema SIEM real.
- Facilitar la labor del personal responsable de Seguridad de la Información, haciéndola más ágil y eficaz.
- Contar con un punto común donde la información relacionada con el ciclo completo de la vida de un incidente se encuentre integrada y accesible cada vez que se requiera.
- Poder responder fácilmente a los entes de control y de auditoría acerca de la debida diligencia en la atención de incidentes (Auditabilidad y servicio de Notificaciones). Especialmente importante de cara al cumplimiento de la normativa legal vigente y, en concreto, a los artículos 33 y 34 del nuevo RGPD actualmente en vigor, relativo a Notificaciones por violación de la seguridad de los datos personales; así como el cumplimiento del artículo 36 del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS, en lo que respecta a notificar al CCN aquellos incidentes que tengan un impacto significativo en la Seguridad de la Información manejada y en los servicios prestados.
- Convertir los datos en información valiosa descubriendo cómo los incidentes afectan a la organización y cuál es la tendencia de los mismos (Gestión del Conocimiento).
- Poder identificar cual es la eficacia en la gestión de los incidentes y poder así establecer las capacidades que se deben fortalecer (Gestión del Conocimiento).
- Incrementar la seguridad activa y pasiva del sistema, reduciendo el nivel de ocurrencia de incidentes y su impacto, respectivamente.

Como se argumentaba en el apartado *1 Introducción y objetivos*, el trabajo desarrollado constituye una de las dos líneas de trabajo en el marco de un Centro de Operaciones de Seguridad. La segunda línea se fundamentaba en el desarrollo de un sistema SIEM real que fuese capaz de establecer comunicación con la plataforma Soteria y ofrecer la generación automática de incidencias. Es, sin duda, una línea de trabajo muy interesante también y que incrementaría notablemente la calidad en la gestión de la Seguridad de la Información de la organización.

Ello permitiría disponer de una herramienta completa del estilo de OSSIM, tal como se veía en el apartado *1.2 Motivación*, pero de desarrollo propio y cubriendo todas las áreas de la Seguridad de la Información, no solo la seguridad informática.

Puede accederse a todo el código y maquetación HTML desarrollados a través del repositorio:

<https://github.com/bchimar/soteria>

5.2 Logro de objetivos

Mediante este apartado y una vez completado el trabajo, se realiza un repaso recapitulando los objetivos planteados inicialmente, y verificando si se ha logrado alcanzarlos. La siguiente tabla cubre el éxito alcanzado en cada objetivo propuesto:

Objetivo	Éxito
Recogida de incidentes de seguridad de la información, catalogación y registro	✓
Gestión de Equipos de Respuesta ante Incidentes de seguridad de la información	✓
Gestión de medidas de protección recogidas en la guía CCN-STIC 804	✓
Gestión de personal responsable de seguridad	✓
Cuadro de mandos con estadísticas y gráficas para el apoyo a la toma de decisiones	✓
Consolidación de una base de datos de Errores Conocidos (Conocimiento)	✓
Información específica de apoyo a la gestión de la seguridad de la información	✓
Acceso web seguro multiusuario	✓
Cumplimiento de la normativa legal vigente (incluido servicio de notificaciones)	✓
Validación de las entradas	✓
Comprobación de la coherencia de los datos introducidos por los usuarios	✓
Depuración de efectos colaterales	✓

Tabla 5-1. Verificación del logro de objetivos.

5.3 Líneas futuras de trabajo

Una vez completada la obra, se proponen una serie de líneas mediante las cuales continuar y mejorar el presente trabajo. Debido a la extensión de este proyecto, las posibilidades se muestran inescrutables, por lo que se enunciarán e introducirán solo algunas de ellas.

- Sería muy interesante el poder adaptar un sistema SIEM real, a ser posible de desarrollo propio, a la plataforma Soteria. Ello contribuiría a incrementar notablemente la eficiencia del sistema y liberar al personal responsable de seguridad de las tareas de análisis para la detección más tediosas.
- Permitir la selección de la valoración del sistema (Alto, Medio, Bajo) según guía CCN-STIC 803, de Valoración de los Sistemas. Ello supone la variación en las medidas de protección aplicables, según el caso.
En el contexto de este trabajo, debido a que la plataforma web desarrollada es susceptible de ser aplicada en el ámbito del Ministerio de Defensa, incluyendo sobre redes clasificadas, no se ha hecho necesario implementar esta funcionalidad, ya que por defecto se considera el sistema categorizado como nivel Alto.
- Permitir algún nivel de personalización de la interfaz web. Debido a las limitaciones para el desarrollo de este trabajo, no se ha podido dedicar más tiempo al aspecto estético de la

interfaz web. Se deja, por tanto, como línea de trabajo futura el que se permite al usuario que esté operando la plataforma web poder personalizar la interfaz y acomodarla a sus preferencias, mediante algún menú contextual y una paleta de herramientas.

- Desarrollar las capacidades del sistema SIEM de tal manera que se intente gestionar los incidentes de manera más inteligente. Por ejemplo, detectar si el momento de detección se ha producido dentro de horario laboral y en día laborable. En ese caso, se podría reservar la conformación de Equipos de Respuesta de manera discrecional y manual al personal responsable de seguridad que se encuentra en las instalaciones. Si la incidencia tiene severidad Crítica, tras notificar el incidente, el sistema podría quedar a la espera de ser atendida por el personal responsable de seguridad presente, en lugar de conformar y activar directamente un CSIRT de manera automática desde el sistema SIEM.
- Continuando con la propuesta anterior, se podría introducir control de horario de tal manera que se ajuste la gestión de incidencias según se trate de un día y hora laborable, en el que el personal responsable de seguridad se encuentra presente, o bien la detección de una incidencia crítica se ha detectado fuera de horario laboral. Si el alta de la incidencia es manual, quiere decir que se realiza en horario laboral y, aunque sea crítica, se atiende de inmediato con el personal presente. En el caso de que la detección por el SIEM se produzca en horario laboral y en día laborable, como se proponía en el punto anterior, se podría dejar a criterio del personal de seguridad el modificar el equipo conformado, o incluso anularlo.
- El objetivo principal del trabajo es disponer de un sistema de gestión capaz de categorizar la incidencia desde el punto de vista del ámbito de la seguridad de la información que se vea afectado, así como disponer de las medidas de protección aplicables. Para ello, se ha seguido el ENS, si bien se podría ampliar el alcance del trabajo en el sentido de incluir otras clasificaciones y guías de medidas de protección recomendadas, incluso se podría plantear, en base al Conocimiento adquirido con la experiencia, incorporar medidas de protección personalizadas para la organización, generadas por el personal responsable de seguridad. Ello potenciaría sin duda la plataforma, haciendo más ágil la gestión de cada nueva incidencia, reduciría el nivel de amenazas y mejoraría la Base de Conocimiento. De cara a poder realizar esta extensión del trabajo, hay que tener en cuenta el tipo de organización y la normativa aplicable. En el ejemplo de implementación que ocupa este trabajo, la pretensión es que sea aplicado en el ámbito global de las AA.PP., y en el ámbito concreto del Ministerio de Defensa, por lo que en este caso se ha regido por el ENS y las guías y recomendaciones originadas en el CCN. Otro aspecto a considerar, de gran importancia, es el mantener la consistencia de los datos de las incidencias y evitar los cambios de datos fundamentales. En el apartado 3.3 *Diseño e implementación de la base de datos* se expone dicha consideración.
- Continuando con la propuesta anterior, el mantenimiento actualizado de la tabla ENS significa aplicar en todo momento la guía CCN-STIC 804, de Implantación del ENS, que haya en vigor y utilizada como referencia. Con ello se debe asumir el riesgo que una gran actualización de dicha guía genere una codificación de las medidas de protección distinta a la contemplada. Esto significa que el personal de mantenimiento encargado del desarrollo y mantenimiento de la plataforma web de gestión de incidentes de seguridad de la información deberá realizar las acciones oportunas para, dado el caso, actualizar la plataforma en su conjunto adecuándola a la nueva versión de la guía de referencia. Quizá, más que una línea futura, se deba contemplar como una acción necesaria de mantenimiento de la plataforma web.
- En este trabajo no se considerarán los falsos negativos que pueden achacarse también al personal (detección tardía, contando ya con evidencias), ya que resulta muy complejo establecer un límite a partir del cual deja de ser sólo un falso negativo del sistema SIEM y

constituye también un falso negativo del personal. Es decir, cuando el personal de seguridad detecta una amenaza, en ese momento se sabe con seguridad que el sistema SIEM ha fallado, ya que no ha sido éste el que la ha descubierto, pero, ¿cómo saber si también el personal de seguridad ha fallado y se podría haber detectado antes...? Se deja, por tanto, como posible línea futura de trabajo el poder afinar este aspecto.

- Con fecha 04/10/2018, el CCN mediante un comunicado a través de su sistema de avisos, informa de la disponibilidad de una nueva Guía CCN-STIC 819, de Medidas compensatorias. Según expresa el comunicado: *“el objetivo de esta guía es servir de ayuda a las entidades del ámbito de aplicación del ENS en la determinación e implantación de las medidas compensatorias cuando no sea posible la adecuada implantación de las medidas de seguridad contempladas en el Esquema”*.

La línea de trabajo futura, por tanto, sería: contemplar dichas medidas, incorporándolas a la BBDD de Soteria, y permitir que sean seleccionadas e incorporadas a la gestión de las incidencias, en caso de ser necesario.

- Podrían darse casos excepcionales en que se detecte una incidencia de severidad crítica o alta en horario de trabajo, pero que no ha requerido la conformación de un Equipo de Respuesta. Si la incidencia reviste gran importancia y se acerca de la hora del alto en el trabajo, quizá sería interesante poder crear y asociar un Equipo de Respuesta a la incidencia. Tal como está diseñada la plataforma actualmente se podría hacer manualmente insertando los datos conectándose directamente a la BBDD desde la línea de comandos, si bien no se permite realizarlo desde la interfaz web de Soteria. Se deja como línea de trabajo el permitir la generación de un nuevo Equipo de Respuesta de manera automática, y asociarlo a la incidencia que se está gestionando.
- Como se exponía en el apartado 5.1 *Conclusiones de interés*, determinar los parámetros modificables y los no modificables a lo largo de la vida de una incidencia no es sencillo, siempre aparecerá el **compromiso Flexibilidad↔Trazabilidad**. Por tanto, se deja como línea de trabajo futura el poder establecer criterios para ello.

No obstante, más que una línea de trabajo futura, en realidad supone un estudio previo y necesario de cara a intentar aplicar la plataforma de gestión de incidencias a un escenario concreto, es decir, a una organización concreta. Antes del despliegue de la plataforma, se hará necesario realizar dicho estudio y establecer las adaptaciones necesarias en función de los criterios elegidos.

- Se podría incluir algún apartado relativo a Análisis Forense que permita automatizar la recogida de evidencias y la generación de la documentación necesaria.
- En el caso de la aplicación en redes abiertas, se podrían integrar sistemas recolectores de datos relacionados con incidencias de Seguridad de la Información: principalmente informes sobre incidencias e informes sobre su resolución. Ello se podría incorporar a la Base de Conocimiento, incrementando notablemente la eficacia y eficiencia del sistema, así como reduciendo el nivel de amenaza. Para estas tareas relativas a la automatización de las búsquedas se podría aplicar Inteligencia Artificial [26].
- Como compendio y línea de trabajo futura general aplicable a este trabajo, hay que volver a incidir en que se trata de un campo muy amplio, por lo que se pueden plantear numerosas nuevas necesidades y materializarlas en forma de servicios, junto con la definición de los datos necesarios para su gestión.

5.4 Clausura del documento.

Retomando el primer concepto que se trataba en este documento, es de desear que la tendencia llegue en algún momento a revertir, siendo habitual y estando integrada de pleno en todos los sectores y en todas las facetas de la vida, la Ciberseguridad.

6 BIBLIOGRAFÍA

En esta sección se indican las referencias a la bibliografía utilizada para la confección del presente trabajo.

- [1] ISO/IEC 27035, ISO/IEC 27001, ISO/IEC 18044, NIST800-61 y Hanbook de CERT/CC.
- [2] <https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html>
- [3] <https://siriusitpro.com>
- [4] <https://en.wikipedia.org/wiki/OSSIM>
- [5] <https://www.manageengine.com.mx/servicedesk-plus/vision-general>
- [6] <https://www.youtube.com/watch?v=Fp6ukwv0FKw>
- [7] http://www.kmkey.com/software_help_desk/
- [8] http://www.cybsec.com/ES/servicios/gestion_incidentes.php
- [9] <https://www.microsoft.com/es-es/store/b/windows>
- [10] <https://es.wikipedia.org/wiki/Unix>
- [11] <https://todopostgresql.com/ventajas-y-desventajas-de-postgresql/>
<http://postgresql-dbms.blogspot.com/p/limitaciones-puntos-de-recuperacion.html>
<http://empresayeconomia.republica.com/aplicaciones-para-empresas/ventajas-y-desventajas-de-postgresql.html>
<https://es.wikipedia.org/wiki/SQLite>
<http://sqlitedatabasegrupo.blogspot.com/p/caracteristicas-de-sqlite.html>
<https://basesdedatosactividad2.wordpress.com/2014/08/20/desventajas-de-4-bases-de-datos/>
<http://www.tuprogramacion.com/bases-de-datos/mariadb-vs-mysql/>
<https://es.wikipedia.org/wiki/MariaDB>
<http://mariadbhistoria.blogspot.com/>
- [12] <https://spectrum.ieee.org/>

- [13] <https://www.slant.co/options/1398/alternatives/~flask-alternatives>
- [14] <https://oauth.net/>
- [15] https://github.com/itemir/apache_2fa
- [16] <https://www.solvetic.com/tutoriales/article/4285-instalar-configurar-google-authenticator-ubuntu-linux/>
- [17] <http://bibing.us.es/proyectos/abreproy/11908/fichero/Memoria%252F5TeoriadeBasedeDatos.pdf>
- [18] <https://programandoointentandolo.com/2012/11/como-crear-pestanas-con-html.html>
- [19] https://www.w3schools.com/js/tryit.asp?filename=tryjs_timing_clock
- [20] <https://sweetalert.js.org/>
- [21] <http://www.chartjs.org/>
- [22] Trabajo de Fin de Máster Universitario en Ingeniería de Telecomunicación, Universidad de Alcalá, curso 2015/2016. Autor: Blas Chica Martos.
- [23] https://httpd.apache.org/docs/current/es/mod/mod_authn_core.html#authtype
- [24] <https://httpd.apache.org/docs/trunk/howto/htaccess.html>
- [25] <https://stackoverflow.com/questions/4154187/how-to-logout-user-for-basic-http-authentication>
- [26] A partir de los conceptos sobre algoritmos de búsqueda basados en IA vistos a lo largo de la asignatura: Guiado de Vehículos No Tripulados, del Máster Universitario en Ingeniería de Telecomunicación, Universidad de Alcalá, curso 2015/2016.

ANEXO I: GLOSARIO

A

Activos de una organización: conjunto de recursos e información que alberga la organización. Fuente: documentación de la asignatura Ciberseguridad, del Máster Universitario en Ingeniería de Telecomunicación, Universidad de Alcalá, curso 2015/2016.

AWS (Amazon Web Services): servicios ofrecidos por Amazon con acceso vía web (tanto para contratación como para la gestión de los propios servicios contratados). Fuente: desarrollo propio.

C

CCN: Centro Criptológico Nacional. Organismo responsable de garantizar la seguridad las Tecnologías de la Información y la Comunicación (TIC) en las diferentes entidades del Sector Público, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada. Fuente: <https://www.ccn.cni.es/index.php/es/menu-ccn-es>.

CCN-CERT: Centro Criptológico Nacional-Computer Emergency Response Team. Se trata de la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español. Su misión es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes. Fuente: <https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html>.

CEO (Chief Executive Officer): término de origen anglosajón para el cargo equivalente de Director Ejecutivo. Fuente: desarrollo propio.

Ciberseguridad: conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Fuente: Recomendación UIT-T X.1205 (04/2008): <https://www.itu.int/net4/ITU-T/search/api/redirection?dest=http://handle.itu.int/11.1002/1000/9136-en?locatt=id:2&auth>.

Según la definición de la norma ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity: se trata del “entorno complejo resultante de la interacción de personas, software y servicios en internet por medio de dispositivos tecnológicos y redes interconectadas que no existe en una forma física”.

CISO (Chief Information Security Officer): término de origen anglosajón para el cargo equivalente de Director de Seguridad de la Información. Fuente: desarrollo propio.

Código abierto (Open Source): estándar de desarrollo mediante el cual se ofrecen los ficheros fuente del mismo. En su mayoría se distribuyen mediante licencias de uso gratuito, con algunas limitaciones en el caso de hacer un uso comercial del desarrollo. Fuente: material y bibliografía del Máster.

CRON: administrador regular de procesos en segundo plano (demonio) que ejecuta procesos o guiones a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el fichero crontab. El nombre cron viene del griego chronos, que significa "tiempo". Fuente: [https://es.wikipedia.org/wiki/Cron_\(Unix\)](https://es.wikipedia.org/wiki/Cron_(Unix)).

CSO (Chief Security Officer): término de origen anglosajón para el cargo equivalente de Director de Seguridad. Fuente: desarrollo propio.

E

EC2 (Elastic Cloud Computing): servicio de aprovisionamiento de máquinas virtuales de Amazon Web Services. Fuente: desarrollo propio.

ENS: Esquema Nacional de Seguridad. Tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Ámbito de aplicación: Administraciones Públicas, entidades de derecho público vinculadas o dependientes de las mismas; ciudadanos en sus relaciones con las Administraciones Públicas; y relaciones entre las distintas Administraciones Públicas. Normativa: Ley 11/2007, de 22 de junio; Real Decreto 3/2010, de 8 de enero; Ley 40/2015, de 1 de octubre; y Real Decreto 951/2015, de 23 de octubre. Fuente: <https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens>.

F

Flag (bandera): término informático relativo al desarrollo de software utilizado como sistema de control. Según su valor supondrá desencadenar una serie de eventos u otra, permitiendo controlar el flujo de la ejecución, contenido de variables, etcétera. Fuente: desarrollo propio.

FTP (File Transfer Protocol): protocolo de transferencia de archivos que trabaja sobre la torre de protocolos TCP/IP. Fuente: material y bibliografía del Máster.

Framework: marco de trabajo o plataforma

H

HTTPS (Hypertext Transfer Protocol Secure): protocolo seguro de transferencia de hipertexto. Protocolo del nivel de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto. Fuente: https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto.

I

IIS (Internet Information Services): se trata de un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows. Fuente: https://es.wikipedia.org/wiki/Internet_Information_Services.

Ingeniería social: técnicas de engaño empleadas por un atacante contra personas, con el objetivo de provocar acciones que de otra manera no realizarían y obtener información sensible a las que el atacante no tiene autorización para acceder. Fuente: material y bibliografía del Máster.

Inyección de código: vector de ataque mediante el cual el atacante intenta insertar una cadena maliciosa que, de no ser validada correctamente, podría provocar que la BBDD devuelva datos que no debería, o bien un malfuncionamiento en la misma. Fuente: material y bibliografía del Máster.

ISDEFE: empresa pública de consultoría e ingeniería, medio propio y servicio técnico de la Administración, al servicio de organismos públicos nacionales e internacionales. Fuente: <https://www.isdefe.es/>.

ITIL (Information Technology Infrastructure Library): Biblioteca de Infraestructura de Tecnologías de Información. Se trata de un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma. descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Fuente: https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library.

M

Machine Learning: sistema de aprendizaje automático para máquinas. Constituye una de las ramas más importantes de la Inteligencia Artificial. El objetivo es que los sistemas sean capaces de aprender por sí mismos, no de que se les enseñe. Basado en la búsqueda de patrones a partir de la información previa de que se dispone. Fuente: material proporcionado por el profesorado de la asignatura COM6 - Transformación digital e innovación.

Malware: programa informático malicioso que tiene como objetivo infiltrarse o dañar una computadora o sistema de información. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. Fuente: <https://es.wikipedia.org/wiki/Malware>.

Middleware: se trata de SOFTWARE que hace de intermediario entre dos (o más) aplicaciones (o capas). También se denomina plumbing, porque hace de tubería (pipe) por donde pasan los datos de una capa (o aplicación) a otra. Se suele emplear, o bien debido a que las aplicaciones de ambos extremos se encuentran en distintos lenguajes de programación, o bien por motivos de seguridad. Fuente: material y bibliografía del Máster.

O

Ordenador Aduana: se emplea para la transferencia segura entre la red interna de la organización y el exterior, como punto de aduana, de ahí su denominación. Normalmente lleva asociado un segundo

ordenador empleado para descontaminación de los archivos a transferir (si se realiza en el sentido de incorporar a la red corporativa). La inserción/extracción hacia/desde la red corporativa suele realizarse empleando medios controlados, como pueden ser memorias USB o discos duros externos USB reservados y controlados mediante el número de serie. Sólo a estos dispositivos se les permite conectarse a la red corporativa desde un punto controlado (gestionado por el personal bajo cuya responsabilidad se encuentra la administración del ordenador Aduana). Fuente: desarrollo propio.

OSSIM (Open Source Security Information Management): se trata de un sistema para la gestión automatizada de información de seguridad y de eventos. Está dotado de un sistema SIEM y cuenta con distintas herramientas para los administradores de seguridad informática, incluida la generación de gráficas. Fuente: <https://en.wikipedia.org/wiki/OSSIM>.

P

Phishing: conocido como suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. Fuente: <https://es.wikipedia.org/wiki/Phishing>.

PYME's: Pequeñas y Medianas Empresas.

R

Ransomware: tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. Fuente: <https://es.wikipedia.org/wiki/Ransomware>.

Red Team: grupo independiente que desafía a una organización a mejorar su efectividad asumiendo un rol o punto de vista adverso. En el ámbito de la ciberseguridad, se trata de un equipo organizado cuyo objetivo es encontrar vulnerabilidades y formas de atacar, de manera controlada y pactada, los activos de una organización. Fuente: https://en.wikipedia.org/wiki/Red_team y elaboración propia.

S

SARA: Sistemas de Aplicaciones y Redes para las Administraciones. Conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones Públicas Españolas e Instituciones Europeas facilitando el intercambio de información y el acceso a los servicios. Fuente: <https://administracionelectronica.gob.es/ctt/redsara>.

Script de sistema: archivo de órdenes basadas en líneas de comandos para desarrollar diversa funcionalidad. Suele emplearse en la automatización de tareas y ejecución programada de las mismas. Fuente: material y bibliografía del Máster.

SIEM (Security Information and Event Management, Sistema de Gestión Eventos e Información de Seguridad): sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad. De esta forma permite un análisis de la situación en múltiples ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales. La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación que recopilan eventos relacionados con la seguridad. Combina funciones de un Sistema de gestión de información de seguridad (SIM del inglés Security information management), encargado del almacenamiento a largo plazo, el análisis y la comunicación de los datos de seguridad; y un Sistema de gestión de eventos de seguridad, encargado del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola de la información de seguridad. Fuente: https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_eventos_e_informaci%C3%B3n_de_seguridad.

SQL (Structured Query Language): lenguaje de consulta estructurado para el acceso a sistemas de BBDD relacionales. Una de sus principales características es el manejo del álgebra y el cálculo relacional para efectuar consultas con el fin de recuperar, de forma sencilla, información de bases de datos, así como realizar cambios en ellas. Fuente: <https://es.wikipedia.org/wiki/SQL>

T

Ticketing: sistema de gestión de peticiones e incidencias basado en el uso de ticket's o identificadores uniformes. Utilizado normalmente en los sistemas de soporte y atención al cliente. Fuente: material y bibliografía del Máster.

Token (testigo): en el ámbito de la autenticación para el acceso controlado a los sistemas, un token es la información que se comparte con el servidor de autenticación y que demuestra la autenticidad del usuario que pretender acceder. Normalmente consta de una cadena cifrada de datos. Fuente: material y bibliografía del Máster.

Troyano: software aparentemente inofensivo que simula realizar una actividad lícita, cuando en realidad está ejecutando código malicioso en el sistema de la víctima. Fuente: material y bibliografía del Máster.

V

Vector de ataque: método empleado por un atacante para vulnerar la seguridad y lograr su objetivo. Fuente: material y bibliografía del Máster.

VPN: Virtual Private Network. Servicio de interconexión que permite establecer una conexión cifrada entre distintos puntos, ofreciendo un canal seguro. Suele emplearse para establecer conexiones seguras entre distintas sedes de una misma organización. Fuente: material y bibliografía del Máster.

W

Wannacry: malware de tipo Ransomware cuyos efectos comenzaron a descubrirse en mayo de 2017. Alcanzó una gran expansión global, afectando a más de 230.000 equipos en 179 países según los datos de Europol. Se considera uno de los malware más graves de la historia reciente. Se puede seguir su cronología en numerosas páginas de Internet, como: <https://www.genbeta.com/a-fondo/cronologia-de-wannacry-asi-se-expandio-el-virus-que-paralizo-a-medio-mundo>.

Webinar: conferencia web o conferencia en línea. Similar a una reunión mediante videoconferencia, pero permite a los asistentes, normalmente alumnos, interactuar entre sí.

WSGI (Web Server Gateway Interface): término empleado para las funciones de redireccionamientos de los servidores web de las peticiones que reciben, a las aplicaciones o plataformas web correspondientes que las atienden. Se encuentran escritas en lenguaje Python. Fuente: https://en.wikipedia.org/wiki/Web_Server_Gateway_Interface

ANEXO II: SCRIPTS

En este apartado se incluyen los ficheros scripts de configuración y funcionalidad de apoyo. Debido a su reducido tamaño, se insertan en forma de imagen para poder apreciar los distintos campos y tipos de datos que lo integran, según colores del editor de texto:

```
# -*- coding: utf8 -*-

#####
#                               CUD - MARÍN                               #
#                               MGSTICS                                #
#                               2017/2018                             #
#                               TRABAJO DE FIN DE MÁSTER              #
#    DISEÑO E IMPLEMENTACIÓN DE UNA PLATAFORMA WEB PARA              #
#    LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN        #
#                               ALUMNO: BLAS CHICA MARTOS.           #
#####

#####
#                               config.py:                             #
#    módulo de configuración de la aplicación Flask                 #
#####

import os
DEBUG = True

_basedir = os.path.abspath(os.path.dirname(__file__))

DEFAULT_TPL = 'default'

SECRET_KEY = 'secret devel key'

URL = 'http://0.0.0.0:80/'
TITLE = 'Soteria'
AUTOR = 'Blas Chica Martos'
VERSION = '1.0'
LANG = 'es'
LANG_DIRECTION = 'ltr' # Left To Right
YEAR = 'Noviembre 2018'

del os

#####
# FIN config.py #
#####
```

Figura A2-1. Configuración de la aplicación Flask en caso de utilizar el servidor interno.

```
# -*- coding: utf8 -*-

#####
#                               CUD - MARÍN                               #
#                               MGSTICS                                #
#                               2017/2018                               #
#                               TRABAJO DE FIN DE MÁSTER                #
#    DISEÑO E IMPLEMENTACIÓN DE UNA PLATAFORMA WEB PARA                #
#    LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN          #
#                               ALUMNO: BLAS CHICA MARTOS.              #
#####

#####
#                               Soteria.wsgi:                          #
#    módulo de configuración de la aplicación Flask                    #
#    en el caso de utilizar un servidor web externo                    #
#####

#!/usr/bin/python
import sys
import logging
logging.basicConfig(stream=sys.stderr)
sys.path.insert(0, "/var/www/Soteria/src")

activate_this = '/var/www/Soteria/env/bin/activate_this.py'
execfile(activate_this, dict(__file__=activate_this))

from Soteria import app as application
application.secret_key = 'ESCRIBA_LA_CLAVE_SECRETA_AQUÍ'

#####
# FIN config.py #
#####
```

Figura A2-2. Configuración de la aplicación Flask en caso de utilizar un servidor externo.

```
# -*- coding: utf8 -*-

#####
#                               CUD - MARÍN                               #
#                               MGSTICS                                #
#                               2017/2018                               #
#                               TRABAJO DE FIN DE MÁSTER                #
#                               DISEÑO E IMPLEMENTACIÓN DE UNA PLATAFORMA WEB PARA #
#                               LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN #
#                               ALUMNO: BLAS CHICA MARTOS.                #
#####

#####
#                               get_user.sh:                            #
#                               script para obtener el usuario recién autenticado #
#####

#!/bin/bash
cd /apache_2fa/state/
user_file=$(ls -rt | tail -n 1)
cat "$user_file" | tail -n 1

# Al autenticarse el usuario se crea un fichero cookie bajo el directorio /apache_2fa/state/
# de Google Authenticator. Los últimos 9 caracteres del fichero contienen el nombre del usuario logueado!
```

Figura A2-3. Extracción del nombre del usuario recién autenticado.

```
#!/bin/bash

#####
#                               CUD - MARÍN                               #
#                               MGSTICS                                #
#                               2017/2018                               #
#                               TRABAJO DE FIN DE MÁSTER                #
#                               DISEÑO E IMPLEMENTACIÓN DE UNA PLATAFORMA WEB PARA #
#                               LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN #
#                               ALUMNO: BLAS CHICA MARTOS.                #
#####

#####
#                               set_new_user.sh:                        #
#                               Shell Script para gestionar el alta de nuevos usuarios. #
#####

clear
server="127.0.0.1"

cp /home/common-password_hardening /etc/pam.d/common-password # Se asegura que se establece una contraseña de suficiente robustez.

echo 'Introduzca el nombre de usuario a dar de alta:'
read new_user # Lectura desde la consola.
adduser $new_user # Creación del nuevo usuario

mkdir /home/users/$new_user # Se crea la carpeta que albergará las credenciales del usuario para Google Authenticator.

echo -en '\n'
echo 'A continuación se generarán la clave secreta y el código QR para Google Authenticator.'
echo 'El nuevo usuario debe capturar el código QR, añadiéndolo a la aplicación cliente:'
sudo -u $new_user -H sh -c "cd /home/$new_user; google-authenticator" # Se cambia a la cuenta del nuevo usuario.
# Se ejecuta la herramienta para generar la nueva clave/código QR para autenticación mediante PIN.

# Antes de nada, se realiza una copia de seguridad del archivo de configuración de Google Authenticator del usuario:
cp /home/$new_user/.google_authenticator /home/users/$new_user
# Ello permitirá restituir el permiso de acceso en caso necesario.

# En este punto también se recomienda, por parte del personal de seguridad, capturar la pantalla que contiene el código QR:
echo -en '\n'
echo 'Personal de gestión de cuentas: por favor, capture el código QR y regístrelo en la carpeta /home/users/'$new_user
echo 'Pulse una tecla para continuar...'
read -n 1 -s

echo -en '\n'
echo 'Inserte la clave secreta (aparece justo debajo del código QR):'
read token

echo -en '\n'
echo 'Se añaden las credenciales a los archivos de Google Authenticator:'
htdigest /home/osboxes/apache_2fa/apache_credentials $server $new_user

echo -en '\n'
echo 'Por último, se añade el nuevo usuario al fichero de tokens 2FA de Google Authenticator (tokens.json).'
sed 's@"$@"",\n \'"$new_user"': \"$token"@g' /home/osboxes/apache_2fa/tokens_backup.json > /home/osboxes/apache_2fa/tokens.json

echo -en '\n'
echo 'Alta de nuevo usuario completada!'
echo -en '\n'
```

Figura A2-4. Proceso de alta de nuevo usuario.

ANEXO III: INSTALACIÓN DEL SOFTWARE ESENCIAL.

A continuación, se describen los pasos y se expone el software esencial de la plataforma Soteria. Se trata de notas recogidas por el autor a lo largo del desarrollo que facilitan el despliegue y puesta en marcha de la plataforma.

1º Como siempre: `sudo apt-get update // sudo apt-get upgrade`.

2º Instalar apache: `sudo apt install apache2`.

3º Copiar los archivos de la plataforma a `/var/www/html/Soteria`.

4º Se comprueba que se visualiza Soteria correctamente.

5º Se comprueba que se puede utilizar el comando `adduser` y se crea correctamente una cuenta nueva.

6º Se instala Google Authenticator: <https://www.solvetic.com/tutoriales/article/4285-instalar-configurar-google-authenticator-ubuntu-linux/>:

```
sudo apt install libpam-google-authenticator
```

```
sudo nano /etc/pam.d/common-auth (también puede hacerse con gedit)
```

→ se añade la línea `auth required pam_google_authenticator.so` encima de la línea:

```
auth [success=1 default=ignore] pam_unix.so nullok_secure
```

→ guardar los cambios!

Esta línea realmente sólo sirve para autenticarse en Linux. Se puede dejar comentada, ya que realmente la autenticación de doble factor se va a utilizar para el acceso web, no para autenticarse en el sistema Linux. ¡De hecho, es mejor dejarlo deshabilitado ya que impide que se ejecuten otras tareas como `adduser`!

7º Para cada nueva cuenta que se quiera dar de alta en el sistema de Google Authenticator:

Se crea la cuenta con `sudo adduser "nuevo usuario"`.

`sudo su "nuevo usuario"` → se cambia al nuevo usuario

`cd /home/"nuevo usuario"` → se entra en la carpeta personal del nuevo usuario

`google-authenticator` (y seguir los pasos de configuración descritos en la memoria: y, y, y, n, y)

(NO OLVIDAR ESCANEAR EL CÓDIGO QR!!)

8º El siguiente paso es habilitar autenticación de doble factor en el acceso web, en este caso, a través del servidor Apache y la herramienta `apache_2fa`:

Para ello se sigue el manual: https://github.com/itemir/apache_2fa:

Se accede a la cuenta Linux y carpeta personal del responsable del alta de usuarios:

```
sudo apt-get install git
sudo git clone https://github.com/itemir/apache_2fa
cd apache_2fa
sudo apt-get install python-pip
sudo pip install onetimepass
sudo mkdir state
sudo chmod 777 state
ps aux | egrep '(apache|httpd)' → para obtener el id de usuario del proceso de apache (www-data)
Una vez que se conoce el usuario que ejecuta el proceso de apache:
sudo chown www-data:www-data state
sudo chown www-data:www-data tokens.json
sudo chmod 750 state // sudo chmod 640 tokens.json → se otorgan permisos
```

```
sudo a2enmod rewrite
sudo a2enmod auth_digest (tal vez requiera: sudo a2enmod authn_core)
sudo a2enmod cgid
sudo service apache2 restart
```

Generar el fichero .conf para Apache (apache_2fa.conf).

Cargar el fichero .conf generado: sudo a2ensite apache_2fa.conf.

Deshabilitar configuración anterior: sudo a2dissite 000-default.conf (según el archivo que hubiera!)

Reiniciar Apache: sudo service apache2 restart

Comprobar que la configuración es correcta en Apache: sudo apachectl configtest.

Si se quiere probar la configuración con HTTP: editar el archivo auth y comentar las siguientes líneas:

```
cookie['2FA_Auth']['secure'] = True
cookie['2FA_Auth']['httponly'] = True
```

Para añadir nuevos usuarios:

```
sudo apt-get install apache2-utils (contiene la herramienta htdigest)
sudo htdigest apache_credentials "yourdomain.com" <new_user>
Ejemplo: sudo htdigest apache_credentials 127.0.0.1 blachimar
```

Añadir el token (clave secreta de Google Authenticator) al fichero tokens.json

9º Instalación de Flask:

```
sudo pip install Flask==1.0.2 (por defecto: pip install -U Flask)
sudo pip install Flask-Script
sudo pip install Flask-Login
sudo pip install Flask-SQLAlchemy
sudo pip install rauth
sudo apt-get install apache2 python-setuptools libapache2-mod-wsgi
```

10º Instalación del gestor de BBDD MariaDB:

https://downloads.mariadb.org/mariadb/repositories/#mirror=tedeco&distro=Ubuntu&distro_release=trusty--ubuntu_trusty&version=10.3

[Configuración del repositorio oficial, descarga e instalación de la última versión!]

```
sudo apt-get install software-properties-common
```

```
sudo apt-key adv --recv-keys --keyserver hkps://keyserver.ubuntu.com:80 0xc9cb082a1bb943db
```

```
sudo add-apt-repository 'deb [arch=amd64,i386,ppc64el]
http://tedeco.fi.upm.es/mirror/mariadb/repo/10.3/ubuntu trusty main'
```

```
sudo apt-get update
```

```
sudo apt-get install mariadb-server
```

[Llegados aquí, MariaDB está instalado en su última versión!]

Para entrar y comprobar que está en ejecución:

```
mysql -u root -p"PASSWORD"
```

mysql -u root -p"PASSWORD" < MGSTICS_TFM_create_FULL.sql → Para cargar TODO en un solo paso.

11º Para acceder desde Python (programáticamente):

```
sudo pip install mysql-connector-python
```

Y en el script Python:

```
import mysql.connector as mariadb
```

En variables globales (al inicio de ejecución del script, tras la sección import):

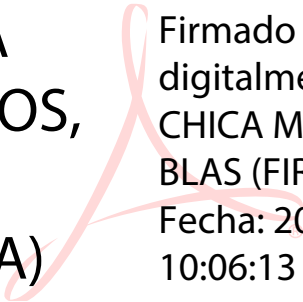
```
mariadb_connection = mariadb.connect(user='root', password='XXXXXXXXX', database='soteria')
```

```
cursor = mariadb_connection.cursor()
```

`mariadb_connection.commit()` → para hacer efectivos los cambios en la BBDD programáticamente.

A partir de ahí ya se pueden realizar consultas.

CHICA
MARTOS,
BLAS
(FIRMA)



Firmado
digitalmente por
CHICA MARTOS,
BLAS (FIRMA)
Fecha: 2018.11.12
10:06:13 +01'00'