



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Autoprotección Digital para autoridades Analógicas.

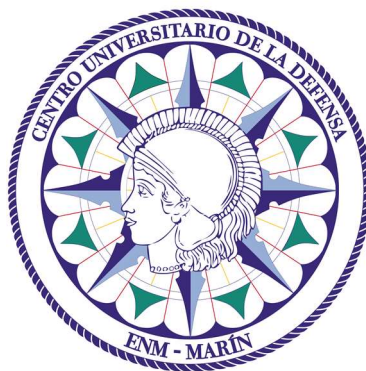
Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Carlos Vicente Contreras

DIRECTORES: Miguel Rodelgo Lacruz

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Autoprotección Digital para autoridades Analógicas.

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

Universida_ddeVigo

RESUMEN

La transformación digital del Ministerio de Defensa y otras entidades gubernamentales ha mejorado la eficiencia táctica y operativa, pero también, ha puesto de manifiesto la debilidad contra las amenazas cibernéticas avanzadas, tales como el phishing avanzado, o el "whaling". Este tipo de ataques, que aprovecha una sofisticada ingeniería social, puede comprometer la seguridad de todo el Ministerio de Defensa al dirigirse a oficiales o autoridades de alto rango con acceso a información crítica. El estudio se centra en la necesidad de concienciar a las autoridades sobre estos riesgos a través de la educación en ciberseguridad, resaltando casos emblemáticos como Stuxnet o los ataques a Estonia, que subrayan la urgente necesidad de una cultura que parta desde lo más profundo de la organización con protocolos eficaces. También se subraya la relevancia de realizar talleres de ciberseguridad y programas de simulación con el objetivo de cultivar habilidades técnicas y potenciar la resiliencia y autoprotección de las autoridades con acceso a redes clasificadas y datos críticos. El análisis incorpora iniciativas habituales en entornos similares como las implementadas por la OTAN y el INCIBE, que fusionan formación avanzada y colaboración a nivel internacional. Este Trabajo Fin de Master propone la elaboración también de un test para medir la capacitación en ciberseguridad, destinado a autoridades militares, con la finalidad de potenciar su habilidad para autoevaluar, y mejorar la reacción ante amenazas cibernéticas emergentes, en consonancia con normativas internacionales. La investigación concluye que una estrategia holística de sensibilización digital tiene el potencial de proteger la seguridad de todo el ministerio, no solo en las herramientas de mando y control, también la de su propio entorno personal, manteniendo a las autoridades seguras también en el uso de las redes sociales o de las herramientas colaborativas.

PALABRAS CLAVE

Ciberseguridad, concienciación, resiliencia digital, phishing, whaling.

AGRADECIMIENTOS

Agradezco sinceramente a mi tutor del Trabajo Fin de Máster, Miguel Rodelgo Lacruz, por su orientación, paciencia y dedicación durante todo el desarrollo de este proyecto. Han sido esenciales sus aportaciones para superar los retos de este trabajo.

Como no puede ser de otra forma, agradezco a mi familia por su apoyo incondicional. Afrontaba múltiples responsabilidades y poder finalizar este trabajo ha sido posible gracias a su confianza y comprensión.

Agradezco a mis compañeros de la UME por su camaradería, que me han permitido compaginar la realización de este trabajo con mi responsabilidad en plena emergencia de Valencia.

CONTENIDO

Contenido	5
Índice de Figuras	6
1 Introducción y objetivos	7
1.1 Introducción.	7
1.2 Objetivos.	9
1.3 Estructura de la Memoria	10
2 Estado del arte	11
2.1 Concienciación en España.....	11
2.2 Concienciación en la OTAN.	13
2.3 Concienciación para empresas del INCIBE.....	14
2.4 La concienciación como herramienta de autoprotección.	15
3 Desarrollo y resultados	19
3.1 Análisis sobre la concienciación de OTAN e INCIBE actual en ataques pasados.	19
3.2 Test Sobre conocimientos en ciberseguridad y análisis de resultados.....	25
3.2.1 Objetivo del test.	25
3.2.2 Preguntas y justificación de las preguntas.	26
3.2.3 Análisis de la muestra.....	45
3.2.4 Análisis y Grafico de los resultados anónimos de los componentes del Master.....	46
3.3 Taller de Sensibilización sobre Ciberseguridad para Autoridades Militares	61
3.3.1 Objetivo del Taller	61
3.3.2 Elementos de la Prueba de Laboratorio	62
3.3.3 Simulaciones de Ataques Expuestos en Situaciones Reales	62
3.3.4 Búsqueda de exposición digital.....	62
3.3.5 Capacitación en la Detección de Amenazas.....	64
3.3.6 4. Manejo de Credenciales y Accesos Importantes	66
3.3.7 Acceso a redes y destinos inseguros.	68
4 Conclusiones y líneas futuras	71
4.1 Conclusiones.	71
4.2 Líneas futuras dirigidas	72
5 Bibliografía.....	73

ÍNDICE DE FIGURAS

3-1 Grafico 1ª Pregunta	46
3-2 2ª Pregunta	47
3-3 3ª Pregunta	47
3-4 4ª Pregunta	48
3-5 5ª Pregunta	48
3-6 6ª Pregunta	49
3-7 7ª Pregunta	50
3-8 8ª Pregunta	51
3-9 9ª Pregunta	51
3-10 10ª Pregunta	52
3-11 11ª Pregunta	52
3-12 12ª Pregunta	53
3-13 13ª Pregunta	54
3-14 14ª Pregunta	54
3-15 15ª Pregunta	55
3-16 16ª Pregunta	55
3-17 17ª Pregunta	56
3-18 18ª Pregunta	57
3-19 19ª Pregunta	58
3-20 20ª Pregunta	59
3-21 21ª Pregunta	60

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción.

La rápida adopción de tecnologías digitales en las entidades gubernamentales y las fuerzas armadas ha transformado radicalmente la administración de los datos, la formulación de decisiones estratégicas y los procedimientos en los tres niveles: táctico, operacional y estratégico. Estas innovaciones han incrementado de manera significativa la eficiencia de todas las instituciones, incluido el Ministerio de Defensa. Sin embargo, también han aumentado su exposición a amenazas cibernéticas, cada vez más sofisticadas, poniendo en riesgo tanto la seguridad nacional como la estabilidad de las entidades. Entre estas amenazas se destaca el whaling, una modalidad de ataque cibernético altamente dirigida que se dirige hacia los niveles superiores de una estructura organizativa, que por la edad muchas veces relacionada con los conocimientos técnicos, también coincide que son los menos preparados para enfrentarse a estas amenazas.

El Whaling, es un tipo de phishing que constituye un tipo particular de ingeniería social avanzada cuyo propósito es manipular a altos ejecutivos, funcionarios o líderes estratégicos con acceso privilegiado a información crítica o recursos financieros. Este tipo de ataque se distingue del phishing tradicional por su sofisticación y personalización características. Los agresores dedican tiempo a investigar a sus objetivos, utilizando datos recopilados de redes sociales, sitios web corporativos, entrevistas públicas y otras fuentes accesibles. Esta pericia exhaustiva les facilita la elaboración de mensajes que reproducen con exactitud la comunicación cotidiana del entorno profesional de la víctima o buscan vectores que pasen desapercibidos para las autoridades objetivo.

Un rasgo distintivo del método Whaling es la elaboración de mensajes fraudulentos que apelan a la urgencia o la autoridad, con el objeto de que las víctimas actúen con prontitud sin cuestionar la legitimidad de las peticiones, es esencial que las autoridades sean capaces de identificar cuáles son sus posibles vulnerabilidades [1]. Por ejemplo, los agresores podrían suplantar la identidad de un Teniente General o un Almirante, con el fin de solicitar cambios de posición de las unidades, autorizar accesos a sistemas delicados o incluso tomar decisiones estratégicas que comprometan la integridad de la organización, que las autoridades puedan identificar los intentos de ingeniería social es algo necesario [2].

En el ámbito de las empresas privadas, los ataques de Whaling han originado casos destacados. En el año 2016, FACC, la compañía aeroespacial austriaca, fue el blanco de uno de estos ataques, lo que pone de manifiesto la importancia de contar con protocolos de verificación sólidos para evitar este tipo de incidentes. Mediante la suplantación de la identidad del Director Ejecutivo, los agresores emitieron un correo electrónico fraudulento solicitando una transferencia de 50 millones de euros. La transacción se llevó a cabo, lo que resultó en una devastadora pérdida financiera y el despido de los ejecutivos principales [3]. En el mismo año, la red social Snapchat experimentó un ataque de Whaling cuando un empleado de Recursos Humanos, creyendo que estaba en contacto con el Director Ejecutivo, divulgó información de la nómina de los empleados, comprometiendo así información personal de carácter privado. Ambos sucesos enfatizan la relevancia de la formación en ciberseguridad para todos los estratos de una entidad [4].

El sector gubernamental y en concreto el militar, como no podía ser de otra manera, no se encuentra exento de estos ataques, y los efectos pueden ser aún más devastadores. En el año 2019, el grupo de piratas informáticos Phineas Fisher, muy activo en América del Sur, realizó el conocido caso MilicoLeaks en Chile, filtrando más de dos gigabytes de correos electrónicos y documentos internos pertenecientes al personal militar. Este incidente reveló falencias en las comunicaciones estratégicas y comprometió la seguridad nacional al divulgar información delicada relacionada con la inteligencia y

las relaciones internacionales [5]. De forma análoga, en el año 2022, el grupo de piratería informática Guacamaya perpetró el ataque denominado SEDENA Leaks en México, accediendo a seis terabytes de datos pertenecientes al Ministerio de la Defensa Nacional. La información divulgada comprendía comunicaciones de carácter confidencial, actividades de vigilancia dirigidas a opositores políticos y conexiones de todos estos actores con entidades delictivas [6].

El Whaling no emplea únicamente correos electrónicos falsificados. En determinadas circunstancias, los agresores han utilizado técnicas de deepfakes para efectuar llamadas telefónicas o videoconferencias simuladas, presentándose como superiores jerárquicos. Por ejemplo, en 2020, una empresa del Reino Unido reportó que los atacantes usaron una imitación sintética de la voz del director ejecutivo para autorizar una transferencia bancaria, causando pérdidas significativas [7]. Estas técnicas sofisticadas de manipulación tecnológica incrementan la amplitud y la eficacia de los ataques de Whaling. Es muy evidente que todos estos ataques son mucho más sofisticados si los atacantes conocen las actuales herramientas de inteligencia artificial.

La efectividad de estos ataques se basa en la habilidad de los ciberdelincuentes para explotar la psicología humana y la rigidez de las estructuras jerárquicas militares. Es obligado reforzar la idea anterior expuesta de que los mensajes suelen tener en cuenta aspectos como la urgencia, la confianza y explotar el respeto hacia la autoridad. En numerosas organizaciones, las instrucciones de altos cargos suelen ser cumplidas sin realizar verificaciones exhaustivas, situación que los atacantes aprovechan para maximizar el impacto de sus estrategias [8].

Los ataques de Whaling evidencian que, pese a los progresos en tecnología de detección de intrusiones, cortafuegos y sistemas de seguridad, el factor humano continúa siendo el elemento más vulnerable. La insuficiencia de formación apropiada para detectar intentos de suplantación de identidad o solicitudes fraudulentas convierte a los individuos en el principal agente de ataque. Esta observación resulta particularmente pertinente en sectores donde la comunicación se basa en gran medida en el correo electrónico o los sistemas digitales como el Ministerio de Defensa.

En respuesta a estos desafíos, numerosas organizaciones han iniciado la implementación de políticas de verificación más rigurosas. Estos incluyen la implementación de mecanismos de autenticación doble, la restricción del acceso a información delicada y la aplicación de tecnologías que detecten patrones inusuales en las comunicaciones. No obstante, es imperativo que dichas medidas sean complementadas con una cultura organizacional de ciberseguridad. Esto no solo conlleva la educación de los empleados en la identificación de amenazas, sino también el empoderamiento de los mismos para cuestionar solicitudes, incluso si estas provienen de niveles jerárquicos más elevados, la rígida estructura militar hace este punto más complicado aún que en otras organizaciones.

Otros ejemplos contemporáneos comprenden ataques dirigidos hacia entidades internacionales y corporaciones de alcance global. En el año 2021, un alto cargo de una compañía tecnológica fue engañado a través de un correo electrónico fraudulento que aparentaba ser de un socio comercial. La agresión se produjo mediante la entrega de credenciales que permitieron a los agresores acceder a información confidencial de productos en desarrollo. Estas campañas buscaban no solo información financiera, sino también inteligencia estratégica que pudiera ser empleada con propósitos geopolíticos [9].

Los incidentes de Whaling también han tenido un impacto significativo en el desarrollo de normativas relacionadas con la ciberseguridad. Por ejemplo, en España, la Ley de Protección de Infraestructuras Críticas ha reforzado la obligatoriedad de implementar medidas preventivas y de reporte de incidentes en sectores estratégicos. Asimismo, a nivel internacional, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea ha servido como modelo para garantizar la transparencia y la rápida

notificación de brechas de seguridad en entidades públicas y privadas. En diversas jurisdicciones, se requiere que las entidades reporten incidentes de seguridad en un plazo establecido, lo cual promueve la transparencia y estimula la inversión en medidas preventivas. Adicionalmente, las entidades internacionales están promoviendo la cooperación entre los sectores público y privado con el fin de establecer un frente común contra estas amenazas, que pueden ser lanzadas simultáneamente en ambos entornos.

La formación en ciberseguridad y la concienciación constituyen unos elementos fundamentales para la prevención del whaling. Es imperativo que las organizaciones implementen programas de sensibilización que comprendan simulaciones de ataques, seminarios prácticos y formación continua para todos los estratos jerárquicos de la organización. Estas iniciativas tienen como objetivo no solo salvaguardar a las instituciones contra pérdidas financieras o fugas de información, sino también fortalecer la confianza en un entorno digital que se torna cada vez más complejo y desafiante, esto es lo que se tratará en este TFM

1.2 Objetivos.

Revisión de iniciativas de concienciación en ciberseguridad:

Se realizará un análisis de las estrategias y programas instaurados por entidades como la OTAN e INCIBE, con el objetivo de identificar las prácticas óptimas que fomenten una cultura robusta de sensibilización y autoprotección en ciberseguridad, aplicables a las autoridades militares. Este análisis facilitará la contextualización de las necesidades en todo lo relacionado con la concienciación de las autoridades de las fuerzas armadas en un marco de referencia tanto a nivel nacional como internacional.

Estudio de casos de ciberataques y su impacto en la seguridad militar:

Se llevará a cabo la revisión de incidentes documentados que hayan impactado en infraestructuras esenciales, plataformas de gestión y control, o sistemas estratégicos, evaluando cómo la insuficiente sensibilización contribuyó al éxito de estos ataques. El análisis se enfocará en discernir cómo la sensibilización y el conocimiento apropiado podrían haber atenuado sus efectos, subrayando la relevancia de la autoprotección digital como una obligación tanto individual como colectiva.

Diseño de un test para evaluar el grado de concienciación:

Elaborar un instrumento de evaluación para cuantificar el grado de conocimiento actual e identificar deficiencias en la autoprotección cibernética entre los funcionarios.

Creación de un diseño para el taller de concienciación en ciberseguridad:

El objetivo es diseñar un taller tipo laboratorio enfocado en la formación práctica y la simulación, con un enfoque particular en:

- Instruir a las autoridades militares acerca de las amenazas cibernéticas concretas y los peligros vinculados a una ausencia de protección personal.
- Proveer un ambiente propicio para la práctica de la detección de indicadores de ataques y el desarrollo de estrategias de respuesta eficaces.
- Impartir a las autoridades las habilidades requeridas para detectar amenazas de manera precoz y actuar de manera conjunta con los expertos en ciberseguridad de su entorno.

1.3 Estructura de la Memoria

La memoria se estructura en diversos capítulos, cada uno con una orientación precisa y articulada, que orienta al lector desde los principios fundamentales del estudio hasta sus resultados y conclusiones. A continuación, se proporciona una descripción concisa del contenido de cada sección:

1.3.1 Introducción y objetivos:

Este capítulo expone el marco general del estudio, la importancia del tema abordado y los objetivos concretos que se buscan alcanzar. Incorpora una introducción al concepto de ciberseguridad en el contexto militar y la relevancia de la sensibilización en esta disciplina.

1.3.2. Estado del arte:

Se lleva a cabo un análisis meticuloso de las actuales iniciativas de sensibilización en ciberseguridad, tanto en España como en la OTAN. Adicionalmente, se analizan las iniciativas del INCIBE para fomentar la concienciación entre las organizaciones, estableciendo un marco teórico que respalda el desarrollo laboral.

1.3.3. Desarrollo del TFM:

Este capítulo representa el eje central del trabajo y se segmenta en diversas secciones:

1.3.3.1 Análisis sobre la concienciación de OTAN e INCIBE actual en ataques pasados:

Se lleva a cabo un análisis de casos representativos de ciberataques, evaluando cómo una preparación más exhaustiva en ciberseguridad podría haber mitigado su repercusión.

1.3.3.2 Test sobre conocimientos en ciberseguridad y análisis de resultados:

Incorpora el diseño y fundamentación de un cuestionario, el examen de las respuestas de una muestra, y un análisis gráfico de los resultados obtenidos. Esta sección facilita la identificación de deficiencias y áreas susceptibles de mejora en la capacitación en ciberseguridad.

1.3.3.3 Taller de sensibilización sobre ciberseguridad para autoridades militares:

El diseño de un taller práctico que comprende simulaciones, ejercicios de formación en la identificación de amenazas, gestión de credenciales y exposición a redes de inseguridad. Este taller tiene como objetivo suministrar instrumentos prácticos y estrategias de autoprotección para las autoridades militares.

1.3.4. Conclusiones y líneas futuras:

Este capítulo condensa los principales descubrimientos del estudio, subrayando los avances logrados en lo que respecta a la sensibilización y formación. Adicionalmente, se sugieren posibles líneas de investigación futuras con el objetivo de continuar con el desarrollo de iniciativas en el campo de la concienciación de autoridades militares.

2 ESTADO DEL ARTE

2.1 Concienciación en España

La relevancia de la sensibilización en ciberseguridad ha experimentado una evolución significativa durante las últimas dos décadas, impulsada por el incremento en la digitalización de nuestras existencias y la creciente dependencia de tecnologías conectadas. Desde el contexto personal hasta el institucional, la expansión de dispositivos conectados y la dependencia de servicios en línea han hecho que las amenazas cibernéticas sean una realidad persistente y en todos los ámbitos de nuestras vidas, en el trabajo y en casa. En el marco actual, la educación en ciberseguridad tiene como objetivo no solo prevenir incidentes, sino también construir una cultura de resiliencia ante un panorama de amenazas en constante evolución. Tanto entidades gubernamentales como corporaciones privadas han implementado estrategias integrales para la formación de una variedad de público, que abarca desde estudiantes y ciudadanos hasta altos ejecutivos y personal militar. Estos proyectos han experimentado una evolución desde meras campañas de sensibilización hasta programas interactivos que integran tecnologías de vanguardia como la inteligencia artificial y la realidad aumentada.

El Instituto Nacional de Ciberseguridad (INCIBE) en España ha desempeñado un papel fundamental en la promoción de la conciencia en este ámbito. Con una perspectiva centrada en la inclusión y accesibilidad, sus programas comprenden desde recursos educativos fundamentales hasta simulaciones sofisticadas diseñadas para sectores específicos. Por ejemplo, el Kit de Concienciación del INCIBE es una herramienta extensamente empleada por empresas con el fin de optimizar la formación de sus trabajadores. Este kit destaca por su enfoque práctico, integrando simulaciones de escenarios reales y recursos interactivos adaptados a distintos niveles de experiencia, lo que lo diferencia de otras iniciativas similares. Este conjunto comprende instrucciones detalladas, vídeos informativos y ejercicios interactivos que abordan amenazas habituales como el phishing, el ransomware y la suplantación de identidad. Un caso notable de implementación se llevó a cabo en una compañía de logística, donde el kit fue empleado para capacitar a los conductores y operadores en la identificación de correos electrónicos parciales. Después de un período de seis meses de utilización, la compañía reportó una disminución del 40% en incidentes asociados con errores humanos [10].

Otra iniciativa esencial del INCIBE es el programa Cibercooperantes, el cual tiene como objetivo la participación de voluntarios en la divulgación de buenas prácticas en ciberseguridad. Estos voluntarios se someten a formación para impartir talleres y conferencias en instituciones educativas, comunidades y pequeñas organizaciones. Un caso destacado es el trabajo llevado a cabo en una escuela secundaria de Andalucía, en la cual los alumnos participaron en actividades prácticas que les instruyeron en la identificación de intentos de ciberacoso y en la protección de sus dispositivos frente a malware. Este programa no solo promueve el aprendizaje práctico, sino que además establece una red de colaboración comunitaria que potencia el impacto de la conciencia.

En el contexto corporativo, hay empresas Microsoft o IBM que han implementado una extensa variedad de recursos con el fin de optimizar la ciberseguridad de sus clientes. Sus Kits de Conciencia de Seguridad comprende herramientas de simulación, guías personalizadas y cursos en línea diseñados para diversos niveles de experiencia. Las simulaciones de suplantación de identidad son particularmente notables, dado que posibilitan a las organizaciones evaluar la preparación de sus trabajadores frente a correos electrónicos fraudulentos [11] [12]. En un caso documentado por la revista Tecbound Technology, una empresa multinacional empleó estas simulaciones con el fin de identificar las áreas de mejora en su estructura interna de comunicación. Previo a la implementación del programa, más del 20% de los empleados interactuaba con correos electrónicos de suplantación de identidad. Tras la conclusión de un curso intensivo de capacitación, este porcentaje se redujo al 5%, lo que evidencia la eficacia de las iniciativas de sensibilización meticulosamente diseñadas [13].

Los cursos destinados a autoridades gubernamentales y personal de alto nivel constituyen otro enfoque crucial en la batalla contra las amenazas cibernéticas. Este tipo de capacitación aborda los riesgos singulares vinculados al acceso a información delicada, como datos de inteligencia o credenciales de alto nivel, y sistemas de vital importancia, como infraestructuras críticas de energía o redes de comunicación. Por ejemplo, en España, el Centro Criptológico Nacional ha implementado un curso especializado en Gestión de Ciber crisis, que emplea técnicas de gamificación para capacitar a los participantes en la respuesta a incidentes de alta complejidad. A lo largo de estas sesiones, los participantes se ven confrontados con escenarios simulados que reproducen ataques dirigidos contra infraestructuras esenciales, tales como sistemas de energía o transporte. Este método no solo optimiza las competencias técnicas, sino que también fortalece la habilidad de los equipos para laborar bajo presión y tomar decisiones estratégicas en tiempo real [14].

La tecnología desempeña igualmente un papel crucial en la actualización de los programas de sensibilización. La inteligencia artificial ha emergido como un instrumento esencial para la personalización de los contenidos educativos y el análisis de patrones de comportamiento que podrían señalar riesgos de seguridad. Por ejemplo, algunas plataformas educativas emplean algoritmos de aprendizaje automático para personalizar los cursos de acuerdo con las necesidades particulares de cada usuario. Esto posibilita que los participantes obtengan información pertinente y sugerencias personalizadas, optimizando así la eficiencia del proceso de aprendizaje.

En lo que respecta al impacto, la evaluación es fundamental para asegurar que las iniciativas de sensibilización alcancen sus metas establecidas. Las entidades están implementando metodologías fundamentadas en datos para evaluar el éxito de sus iniciativas. Por ejemplo, las encuestas realizadas previas y posteriores a los cursos, en conjunto con el análisis de la disminución de incidentes reportados, ofrecen una perspectiva nítida de las áreas que requieren mejoras. Está demostrado que tras la formación en ciberseguridad los clics en correos de suplantación de identidad disminuyen, el porcentaje de la disminución dependerá de la eficacia del programa y de la capacidad de los alumnos para asumir estos nuevos conocimientos.

Las iniciativas de sensibilización no se circunscriben exclusivamente a los sectores organizativos. La formación en seguridad cibernética para la población general ha adquirido importancia, particularmente ante el incremento de fraudes dirigidos a usuarios individuales. Iniciativas tales como las campañas de concientización pública, que comprenden publicidad en medios de comunicación y seminarios comunitarios, han demostrado ser eficaces para alcanzar a un público amplio. La campaña denominada "Protege tu Negocio" está orientada hacia pequeñas empresas y emprendedores. Esta campaña integra recursos en línea, vídeos didácticos y sesiones presenciales con el fin de instruir a los propietarios de empresas sobre la protección de su información financiera y la prevención de fraudes en línea.

La conciencia en ciberseguridad en la actualidad es el producto de años de evolución y colaboración entre sectores público y privado. Desde herramientas fundamentales hasta tecnologías de vanguardia, el objetivo ha permanecido invariable: dotar a los individuos de las competencias y el conocimiento necesarios para afrontar un entorno digital en constante evolución. Con la sofisticación de las amenazas, las estrategias de formación deben continuar innovando, incorporando nuevas tecnologías y adaptándose a las necesidades de una población cada vez más digitalizada, pero que sigue dirigida por personas que no tienen por qué estar tan digitalizadas.

2.2 Concienciación en la OTAN.

La concienciación en ciberseguridad dentro del marco de la OTAN es uno de los cimientos esenciales de la seguridad contemporánea en un mundo donde las amenazas digitales se han transformado en un reto estratégico y táctico para las operaciones militares, la estabilidad de las naciones y la resiliencia de las sociedades modernas. Este aspecto de la formación, particularmente dirigido a autoridades y responsables militares, abarca los elementos técnicos necesarios para comprender las amenazas cibernéticas. Además, analiza las implicaciones estratégicas, legales y operativas que surgen en un entorno digital cada vez más complejo.

El ciberespacio, reconocido oficialmente como un “dominio” operativo por la OTAN, ha revolucionado la forma en que las fuerzas armadas planifican y llevan a cabo sus operaciones. Los enfoques tradicionales ya no son suficientes; el líder militar debe adaptarse a una realidad en la que las capacidades cibernéticas juegan un papel fundamental en la disuasión y la defensa. Las herramientas digitales han ampliado el espectro de la guerra moderna, introduciendo conceptos como el "cibercampo de batalla", en el cual las infraestructuras críticas y las comunicaciones se convierten en objetivos primordiales. Un ejemplo reciente de esto es el ataque coordinado a sistemas de energía en Europa Oriental, donde ciberdelincuentes interrumpieron las comunicaciones militares y civiles, gracias a un malware denominado Blackenergy, demostrando la vulnerabilidad de las infraestructuras críticas en conflictos contemporáneos [15].

El Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN (CCDCOE), ubicado en Tallin, Estonia, se ha consolidado como una entidad muy destacada en la concepción y ejecución de programas de capacitación en ciberseguridad. Los cursos, seminarios y actividades prácticas están diseñados para abarcar una audiencia heterogénea que incluye desde técnicos operativos hasta altos mandos y responsables políticos. Estas iniciativas ofrecen un enfoque holístico que combina teoría, práctica y colaboración internacional, fortaleciendo las capacidades colectivas de ciberdefensa. Un ejemplo destacado de esta combinación es el desarrollo de protocolos conjuntos para la protección de infraestructuras críticas en ejercicios multinacionales, lo que ha permitido mejorar significativamente la coordinación entre países aliados en situaciones de crisis [16].

Una de las estrategias clave de la OTAN es la integración del aprendizaje virtual, implementada mediante la plataforma Joint Advanced Distributed Learning (JADL). Esta herramienta permite a los participantes acceder a módulos que cubren desde fundamentos del ciberespacio hasta temas especializados como el análisis forense digital y las normativas legales de operaciones cibernéticas. Estos módulos no solo facilitan la accesibilidad, sino que también ofrecen la flexibilidad necesaria para adaptarse a las demandas y niveles de conocimiento de los participantes.

El enfoque modular de los programas refleja la diversidad de necesidades entre los Estados Miembros. Por ejemplo, el curso "ADL 076: Conciencia en Ciberdefensa" introduce conceptos básicos para oficiales sin experiencia previa, mientras que módulos avanzados como "Malware and Exploit Essentials" se centran en aspectos técnicos específicos. Esto asegura que tanto los principiantes como los expertos encuentren formación adecuada para sus necesidades.

Además de los cursos técnicos, la OTAN subraya la importancia de la planificación estratégica en el ciberespacio. Un ejemplo destacado es el curso "Integrating Cyberspace Considerations into Operational Planning", diseñado para proporcionar a los responsables militares herramientas para evaluar vulnerabilidades y diseñar estrategias resilientes. Estas competencias son críticas en un entorno donde las amenazas cibernéticas impactan tanto en redes militares como en infraestructuras esenciales que sostienen las operaciones [17].

Un elemento distintivo en la estrategia de la OTAN es el énfasis en la experiencia práctica. Ejercicios como "Locked Shields", el mayor simulacro de ciberdefensa a nivel internacional, permiten a los participantes enfrentar situaciones reales en un entorno controlado. Durante estas actividades, los oficiales colaboran en equipos multidisciplinarios para responder a ataques simulados y salvaguardar infraestructuras críticas. Este enfoque no solo mejora las habilidades técnicas, sino que también permite instruir y fortalecer la toma de decisiones en condiciones de alta presión.

Conforme el ciberespacio continúa evolucionando, la OTAN adapta sus programas para abordar áreas emergentes como la inteligencia artificial, la automatización y el análisis de grandes volúmenes de información. Por ejemplo, en ejercicios recientes, ya se ha utilizado inteligencia artificial para identificar patrones anómalos en grandes redes simuladas, optimizando así la detección de posibles ciberamenazas. Estas tecnologías prometen transformar la gestión de amenazas cibernéticas, posicionando a las fuerzas armadas en la vanguardia de la innovación y asegurando su capacidad para enfrentar desafíos futuros. La colaboración entre los Estados Miembros y las alianzas con el sector privado se perfilan como pilares fundamentales para garantizar la sostenibilidad y eficacia de las estrategias de ciberseguridad.

2.3 Concienciación para empresas del INCIBE

El Instituto Nacional de Ciberseguridad (INCIBE) ha sido establecido un plan de concienciación, con el propósito de brindar asistencia, recursos y orientación en el campo de la ciberseguridad a empresas y ciudadanos. En un entorno global cada vez más interconectado y dependiente de las tecnologías digitales, las amenazas cibernéticas representan uno de los riesgos más significativos para la seguridad de la información, los activos digitales y las infraestructuras críticas. El propósito primordial de INCIBE es establecer un ambiente digital seguro que promueva la confianza de los usuarios en las tecnologías, proteja los datos sensibles y contribuya al fortalecimiento de la infraestructura crítica del país ante los ataques cibernéticos.

INCIBE colabora estrechamente con entidades del sector público y privado, tanto a nivel nacional como internacional, para alcanzar sus objetivos. Estas iniciativas incluyen la elaboración de materiales educativos, la provisión de servicios de consultoría especializada, la implementación de programas de formación en ciberseguridad y la promoción de la colaboración entre diversos actores del ecosistema digital. Adicionalmente, INCIBE participa de manera activa en la investigación de amenazas emergentes, el análisis de riesgos y la gestión de crisis cibernéticas, proporcionando soluciones técnicas y operativas que permiten a las organizaciones enfrentar de manera más eficiente los ciberataques. Un ejemplo reciente de colaboración internacional por parte de INCIBE es la cooperación con la Unión Europea para fortalecer las capacidades colectivas de ciberdefensa, subrayando su liderazgo en el ámbito digital, y de la concienciación. [18].

La visión futura de INCIBE se centra en posicionar a España como uno de los principales referentes en ciberseguridad a escala europea y también global. Para ello, se dedica a fomentar el desarrollo de la industria nacional de la ciberseguridad, respaldando la creación y fortalecimiento de empresas y emprendedores en este ámbito. Asimismo, colabora con instituciones académicas y centros de investigación para promover la innovación en tecnologías de protección digital. Un aspecto destacado de su estrategia es la capacitación y el perfeccionamiento de habilidades para enfrentar las amenazas cibernéticas que afectan a empresas, instituciones y ciudadanos.

Una de las líneas de acción prioritarias de INCIBE es fomentar una cultura de seguridad cibernética que se extienda a todos los estratos de la sociedad, desde la educación primaria hasta los sectores más especializados de la industria. INCIBE reconoce que la concienciación es clave para enfrentar la creciente amenaza digital, y por ello ha diseñado programas que abarcan desde la concienciación de ciudadanos hasta la formación avanzada para directivos. Por ejemplo, su ya citado "Kit de

Concienciación en Ciberseguridad" ha demostrado ser una herramienta eficaz para capacitar tanto a empleados como a ejecutivos, logrando reducir significativamente los incidentes asociados con errores humanos en empresas participantes [19].

En este contexto, la capacitación y concienciación de los encargados de la toma de decisiones dentro de las empresas es fundamental. Los ejecutivos desempeñan un papel crucial en la definición de políticas y prácticas de seguridad. La sofisticación de los ataques cibernéticos exige que los líderes empresariales posean un conocimiento profundo de las amenazas y las estrategias necesarias para mitigar los riesgos, ya que como en las fuerzas armadas no solo tienen acceso a información crítica para la empresa, también tienen la responsabilidad de mantenerlos sistemas y los datos protegidos. INCIBE organiza seminarios, talleres y eventos educativos donde se abordan temas como la gestión de riesgos cibernéticos, la planificación de respuestas ante incidentes y la continuidad del negocio en caso de un ataque. Estos esfuerzos han fortalecido la resiliencia de numerosas organizaciones frente a amenazas cibernéticas.

Adicionalmente, INCIBE impulsa la cooperación internacional como un pilar estratégico para afrontar los desafíos globales en ciberseguridad. Colabora con entidades como la Unión Europea y organizaciones internacionales para compartir información sobre amenazas emergentes, mejores prácticas y tecnologías de defensa digital. Estas alianzas no solo refuerzan la capacidad de España para enfrentar ciberataques, sino que también contribuyen al desarrollo de un marco global más robusto en materia de ciberseguridad.

INCIBE también trabaja con asociaciones empresariales y académicas para fomentar una industria de ciberseguridad competitiva y avanzada en España. Este esfuerzo brinda a las empresas y profesionales acceso a tecnologías de última generación y formación especializada que mejora sus capacidades para proteger sus activos digitales.

La creación de una cultura de seguridad cibernética es un objetivo esencial de INCIBE. Para lograrlo, promueve la ciberseguridad en todos los niveles educativos, desde la enseñanza primaria hasta la formación universitaria, y fomenta la sensibilización en la sociedad sobre la importancia de la protección digital.

Por todo lo anterior INCIBE desempeña un papel fundamental en garantizar que empresas y ciudadanos españoles puedan operar con más confianza en el ámbito digital. Su visión de consolidar a España como líder en ciberseguridad europea es respaldada por diferentes iniciativas innovadoras que abarcan desde la formación de líderes hasta la colaboración internacional. La capacitación de los directivos y la sensibilización corporativa son esenciales para fortalecer la resiliencia de las organizaciones frente a amenazas cibernéticas cada vez más elaboradas, y INCIBE continúa siendo un referente en este campo por su constante actualización en este entorno.

2.4 La concienciación como herramienta de autoprotección.

La concienciación en ciberdefensa constituye un componente esencial para la salvaguarda efectiva de cualquier ambiente digital y, finalmente, para la prevención de ataques cibernéticos que puedan poner en riesgo la integridad de sistemas, información y usuarios. En un mundo progresivamente interconectado la dependencia de la tecnología ha experimentado un incremento exponencial, la seguridad ya no puede ser conceptualizada meramente como un conjunto de instrumentos tecnológicos o medidas técnicas. La dimensión humana desempeña el papel fundamental, dado que los individuos frecuentemente constituyen tanto la línea de defensa inicial como el eslabón más débil en las estrategias de seguridad, las autoridades militares deben ser conscientes de esta realidad.

El motivo primordial para dar relevancia a la concienciación en ciberdefensa reside en la esencia intrínseca de los ciberataques. Estos no se limitan únicamente a las deficiencias tecnológicas, sino que también abordan crecientemente los errores humanos. Los atacantes aprovechan la insuficiencia de conocimientos, la negligencia o las conductas imprudentes de los usuarios para infiltrarse en sistemas que, de otro modo, estarían adecuadamente resguardados a través de soluciones tecnológicas. En este contexto, la capacitación y educación de los usuarios representan instrumentos eficaces para la mitigación de riesgos y el fortalecimiento de la resiliencia ante amenazas cibernéticas.

La concienciación se inicia con el entendimiento de los riesgos asociados a un descuido. Es imperativo que los individuos estén debidamente informados acerca de los riesgos de sus descuidos en un entorno digital y cómo estos pueden manifestarse también en su vida cotidiana u ocupacional. Por ejemplo, comprender que las contraseñas vulnerables pueden ser fácilmente descifradas por ciberdelincuentes o que la divulgación de información delicada en las plataformas de redes sociales podría propiciar ataques dirigidos constituye una etapa esencial. En ausencia de este entendimiento básico pero fundamental, resulta improbable que los usuarios modifiquen sus comportamientos para adoptar prácticas de mayor seguridad.

Tras la comprensión de los riesgos por parte de los individuos, se requiere su formación para identificar las señales de alerta de potenciales amenazas. Esta habilidad de identificación precoz es crucial, dado que numerosos ataques se inician con interacciones menores que podrían permanecer inadvertidas si no se posee la información pertinente. Un escenario habitual es el del phishing, en el que los perpetradores transmiten correos electrónicos que simulan ser procedentes de fuentes fiables con el objetivo de manipular a los usuarios y adquirir información de carácter confidencial. Mediante una formación apropiada, los usuarios podrían detectar elementos sospechosos, tales como errores ortográficos, direcciones URL inusuales o peticiones de información personal, evitando así la susceptibilidad a la trampa, sin hablar del whaling donde también tienen que ser conscientes de sus propias vulnerabilidades como oficiales de alto rango y hacer una autocrítica a cuales podrían ser los vectores de ataque que podría usar un supuesto enemigo para forzar ese clic que le dé acceso a la información o al sistema que desea, todas estas detecciones con la utilización de la inteligencia artificial por parte de los atacantes, cada vez hacen más difícil la detección ante los ojos poco entrenados.

La sensibilización promueve asimismo la adopción de comportamientos seguros en el contexto digital. Esto abarca medidas como mantener el software actualizado y al día para resguardarse de vulnerabilidades identificadas, emplear instrumentos de autenticación multifactor para incrementar un nivel adicional de seguridad y garantizar el cifrado de datos delicados, tanto en estado de reposo como en tránsito. Cada uno de estos comportamientos disminuye considerablemente el área de ataque accesible para los ciberdelincuentes. Por ejemplo, un software desactualizado puede albergar vulnerabilidades susceptibles de ser explotadas; sin embargo, un usuario que implementa actualizaciones de manera periódica puede neutralizar dicha brecha de vulnerabilidad.

Adicionalmente, un elemento crucial de la sensibilización en ciberdefensa radica en la habilidad para minimizar los errores humanos, que constituyen una de las causas primordiales de los incidentes de seguridad. Las acciones que parecen inocuas, tales como el clic en un enlace no identificado, la descarga de un archivo sospechoso o el intercambio de contraseñas con “supuestos” compañeros, pueden acarrear repercusiones devastadoras para la seguridad de una entidad o individuo. Mediante la capacitación, los usuarios incrementan su conciencia respecto a las consecuencias de sus decisiones y fomentan una mayor prudencia al interactuar con sistemas y dispositivos.

La instauración de una cultura de seguridad constituye otra ventaja significativa derivada de la sensibilización. Cuando los individuos comprenden la relevancia de la ciberseguridad y asumen la responsabilidad de salvaguardar la información, no solo optimizan sus propias prácticas, sino que

también ejercen una influencia positiva en su entorno, y esto es más efectivo si se trata de autoridades con capacidad de liderazgo y de generar cambios profundos en las organizaciones. En un contexto laboral, esto podría materializarse en una comunicación transparente acerca de potenciales riesgos o en la implementación colectiva de estrategias de prevención. Una cultura de seguridad firmemente instaurada asegura que la ciberseguridad se perciba como una obligación colectiva, en lugar de ser percibida como una responsabilidad exclusiva de los departamentos técnicos, como sucede en la actualidad.

La implementación efectiva de programas de concienciación requiere la adopción de un enfoque holístico que integre diversos métodos de aprendizaje y sensibilización. Las herramientas más frecuentemente empleadas incluyen talleres presenciales, cursos en línea, simulaciones de ciberataques y campañas de información. Cada una posee una utilidad particular y tiene la capacidad de ajustarse a las necesidades particulares de una organización o comunidad. Por ejemplo, las simulaciones posibilitan a los usuarios la experiencia de escenarios reales de amenazas en un entorno controlado, lo que potencia su habilidad para responder eficientemente en circunstancias concretas.

Es de vital importancia que los programas de sensibilización sean persistentes y actualizados, dado que el escenario de amenazas experimenta una evolución constante. Lo que es pertinente en la actualidad podría no serlo en el futuro, y las estrategias empleadas por los atacantes adquieren una creciente sofisticación. En consecuencia, la capacitación debería ser un proceso dinámico que integre las tendencias más recientes y los riesgos emergentes.

En el siguiente apartado se analizará como la sensibilización en ciberseguridad en los ataques conocidos hubiera sido una inversión indispensable para disminuir la probabilidad de ciberataques y atenuar su repercusión. Mediante la instrucción de los individuos sobre los riesgos, la instrucción en el reconocimiento de amenazas, la promoción de comportamientos seguros, la minimización de errores humanos y la construcción de una cultura de seguridad, se hubiera conseguido robustecer de manera significativa la posición defensiva de cualquier entidad o sujeto. La seguridad en el ciberespacio no es meramente una cuestión técnica; constituye una obligación colectiva que se inicia con la sensibilización y el compromiso de todos los actores involucrados, en los supuestos siguientes solo desde el punto de vista de la concienciación se pretende exponer como los ataques podrían haberse evitado o al menos hubieran sido menos efectivos.

3 DESARROLLO Y RESULTADOS

3.1 Análisis sobre la concienciación de OTAN e INCIBE actual en ataques pasados.

El examen de incidentes cibernéticos pasados proporciona lecciones significativas acerca de las vulnerabilidades presentes y cómo la concienciación podría haber modificado la trayectoria de dichos sucesos. En esta sección, se analizan las estrategias de sensibilización impulsadas por la OTAN e INCIBE en respuesta a ataques significativos, con el objetivo de evaluar su posible repercusión en la prevención y mitigación de dichas amenazas. Estos incidentes, que comprenden desde la divulgación masiva de datos en entidades gubernamentales hasta ataques dirigidos contra infraestructuras esenciales, evidencian deficiencias notables en la preparación y reacción de las autoridades involucradas.

La división de los ataques en subapartados responde a la necesidad de abordar cada caso desde tres perspectivas: el desarrollo del ataque, su impacto estratégico, y cómo las medidas de concienciación adecuadas podrían haber alterado el resultado. Esta metodología estructurada no sólo optimiza el análisis, sino que también enfatiza la diversidad de amenazas cibernéticas y las oportunidades de mejora en el campo de la ciberseguridad.

La elección de los casos se rige por un criterio representativo: desde incidentes masivos como Buckshot Yankee y Stuxnet, que establecieron un punto de inflexión en la estrategia de ciberdefensa, hasta eventos más recientes como SEDENA Leaks y el ataque al Ministerio de Trabajo y Economía Social de España, que ponen de manifiesto las deficiencias contemporáneas en la capacitación. Además, se incorporan casos de espionaje global como Pegasus, que evidencian las vulnerabilidades inherentes a los dispositivos móviles incluso en el contexto gubernamental del más alto nivel.

Con esta estructura se pretende facilitar no solo la asimilación de lecciones aprendidas, sino también la enfatización de la importancia de programas como los simulacros de la OTAN y las iniciativas de INCIBE, que insisten en la sensibilización y la capacitación práctica como instrumentos esenciales para fortalecer la autoprotección y la resiliencia en el ámbito de la ciberseguridad.

3.1.1 Buckshot Yankee (2008)

3.1.1.1 Desarrollo de la Operación

En 2008, el Departamento de Defensa de los Estados Unidos enfrentó una de sus primeras amenazas cibernéticas significativas con la operación conocida como Buckshot Yankee. Este ataque comenzó cuando un USB infectado con malware, dejado intencionadamente en un aparcamiento militar, fue insertado en una computadora conectada a la red clasificada del Pentágono. El malware, identificado como Agent.btz, se propagó rápidamente por las redes internas, recopilando y transfiriendo datos sensibles.

3.1.1.2 Impacto Estratégico

El daño causado por Buckshot Yankee obligó al Pentágono a desconectar temporalmente sistemas críticos y a establecer una nueva división de ciberseguridad, USCYBERCOM. La operación expuso una desconexión importante entre las estrategias de ciberseguridad y las decisiones de alto nivel [20].

3.1.1.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Directrices claras sobre el uso de dispositivos externos: Si las autoridades hubieran implementado políticas estrictas sobre el manejo de dispositivos USB en instalaciones militares, la introducción inicial del malware podría haberse prevenido.
2. Liderazgo en la promoción de prácticas seguras: Programas como Locked Shields y la concienciación del INCIBE subrayan la importancia de que los líderes sean un ejemplo en la adherencia a protocolos.
3. Supervisión estratégica: Las autoridades, debidamente capacitadas, podrían haber priorizado la instalación de sistemas avanzados de detección de anomalías en redes críticas.

3.1.2 SEDENA Leaks (2022)

3.1.2.1 Desarrollo del Ataque

En 2022, la Secretaría de la Defensa Nacional de México (SEDENA) sufrió una de las mayores filtraciones de datos clasificados en su historia. El ataque, atribuido a un colectivo hacktivista conocido como Guacamaya, comprometió información sensible sobre operaciones militares, estrategias de seguridad nacional y datos personales de altos mandos.

La operación se llevó a cabo mediante la explotación de vulnerabilidades en servidores expuestos, lo que permitió a los atacantes acceder y exfiltrar grandes volúmenes de datos sin ser detectados.

3.1.2.2 Impacto Estratégico

El ataque de **SEDENA Leaks** expuso las debilidades en la seguridad cibernética de una institución crítica, destacando la necesidad urgente de medidas que combinen tecnología, concienciación y simulación práctica. Además, este evento subrayó el rol de las fuerzas armadas como un objetivo prioritario para actores malintencionados, especialmente en un contexto de inestabilidad geopolítica [21].

3.1.2.3 Cómo las Medidas de Concienciación Podrían Haber Cambiado el Escenario

1. Participación en ejercicios como Lock Shields de la OTAN: Lock Shields, un ejercicio internacional de ciberdefensa, ofrece escenarios prácticos en los que las instituciones pueden ensayar respuestas a ataques cibernéticos reales. Si SEDENA hubiera participado en este tipo de simulacros, sus equipos habrían estado mejor preparados para identificar patrones de ataque como los utilizados en SEDENA Leaks, especialmente en lo que respecta a la detección temprana de movimientos laterales dentro de las redes. Por ejemplo, Lock Shields permite practicar cómo responder a la exfiltración masiva de datos, algo que en el caso de SEDENA no se detectó a tiempo. Este ejercicio también enfatiza la coordinación entre equipos técnicos y líderes estratégicos, una carencia evidente en la respuesta al ataque.
2. Fortalecimiento de la gestión de accesos privilegiados: Una medida clave para prevenir el tipo de acceso no autorizado observado en el ataque sería la implementación de políticas estrictas de gestión de accesos. Estas políticas incluyen el uso de autenticación multifactor (MFA) y la limitación de privilegios según las funciones de los usuarios. En el caso de SEDENA, el ataque pudo haber sido facilitado por accesos insuficientemente protegidos, permitiendo a los atacantes extraer datos masivos sin restricciones.
3. Concienciación sobre la importancia de la seguridad digital en los altos mandos: En el caso de SEDENA Leaks, la falta de formación y sensibilización en ciberseguridad de los altos mandos pudo haber facilitado el éxito del ataque. El uso inapropiado de dispositivos personales o la

negligencia en la protección de credenciales son prácticas que a menudo se convierten en el eslabón más débil de la cadena. Programas de formación diseñados específicamente para líderes estratégicos habrían ayudado a evitar estos errores y a priorizar la seguridad digital en las decisiones operativas.

3.1.2 Operación SolarWinds (2020)

3.1.2.1 Desarrollo de la Operación

En 2020, uno de los ciberataques más sofisticados y estratégicos afectó a la cadena de suministro de SolarWinds. Los atacantes, vinculados a un actor estatal, introdujeron malware en una actualización del software Orion, utilizado por gobiernos y empresas clave. Esto permitió acceso sigiloso a datos sensibles durante meses.

3.1.2.2 Impacto Estratégico

El ataque afectó la credibilidad de las herramientas de gestión tecnológica y reveló una grave falta de supervisión por parte de las autoridades responsables. Organizaciones críticas, incluidas agencias gubernamentales como el Departamento del Tesoro de EE.UU., quedaron expuestas [22].

3.1.2.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Evaluación estratégica de proveedores: La capacitación habría reforzado la necesidad de auditar regularmente a los proveedores de software.
2. Responsabilidad en decisiones técnicas: Líderes estratégicos entrenados podrían haber implementado revisiones adicionales antes de adoptar actualizaciones críticas.
3. Priorización de la detección temprana: Programas como Lock Shields destacan la importancia de un monitoreo proactivo en redes críticas, algo que podría haber alertado sobre el comportamiento anómalo antes de que el daño fuera significativo.

3.1.4 Stuxnet (2010)

3.1.4.1 Desarrollo de la Operación

Stuxnet, diseñado para atacar las centrifugadoras nucleares de Irán en Natanz, fue un malware pionero en afectar infraestructuras físicas. Se introdujo a través de dispositivos USB infectados en redes aisladas, manipulando las velocidades de las centrifugadoras hasta dañarlas.

3.1.4.2 Impacto Estratégico

Stuxnet retrasó significativamente el programa nuclear de Irán y sentó precedentes sobre el uso de ciberarmas en conflictos geopolíticos. Además, expuso la falta de preparación global para proteger infraestructuras críticas contra ataques avanzados [23].

3.1.4.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Gestión estratégica de dispositivos externos: Las autoridades podrían haber implementado controles estrictos sobre el uso de dispositivos USB en entornos aislados.
2. Monitorización de sistemas, en este caso industriales: Programas como Lock Shields enfatizan la importancia de identificar comportamientos anómalos en sistemas SCADA.

3.1.5 Ataques de Estonia (2007)

3.1.5.1 Desarrollo de la Operación

En 2007, Estonia fue blanco de ataques masivos de denegación de servicio distribuido (DDoS) que paralizaron instituciones gubernamentales, bancos y medios de comunicación. Este ciberataque, vinculado con Rusia, marcó un antes y un después en la defensa digital de naciones pequeñas.

3.1.5.2 Impacto Estratégico

La interrupción temporal de servicios esenciales subrayó la vulnerabilidad de las infraestructuras críticas en un entorno globalizado. Además, destacó la necesidad de fortalecer la cooperación internacional en materia de ciberseguridad [24].

3.1.5.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Resiliencia ante ataques DDoS: Locked Shields entrena en la implementación de soluciones de mitigación, como la segmentación de redes y sistemas de respaldo.
2. Cooperación internacional: La sensibilización de líderes habría promovido respuestas coordinadas entre naciones aliadas.
3. Concienciación de las autoridades: La formación habría permitido a los responsables anticipar los riesgos asociados a tensiones geopolíticas.

3.1.6 Ataque al Ministerio de Trabajo y Economía Social de España (2021)

3.1.6.1 Desarrollo de la Operación

En 2021, el Ministerio de Trabajo y Economía Social de España fue objeto de un ataque cibernético que comprometió sistemas clave y afectó la operatividad del organismo durante varios días. Aunque no se confirmó oficialmente el origen del ataque, se sospecha que fue un ataque de ransomware que buscaba cifrar información sensible y exigir un rescate.

3.1.6.2 Impacto Estratégico

El ataque afectó la prestación de servicios esenciales y la confianza de los ciudadanos en la capacidad del gobierno para proteger datos sensibles. Además, puso en evidencia la necesidad de mejorar la seguridad en los sistemas de administración pública [25].

3.1.6.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Resiliencia Operativa: Locked Shields entrena a los líderes estratégicos para comprender la importancia de políticas de recuperación tras ataques, reduciendo significativamente el tiempo de inactividad.
2. Sensibilización ante Ransomware: La concienciación del INCIBE habría capacitado a las autoridades para implementar controles estrictos y estrategias de prevención efectivas.

3.1.7 Red October (2007 - en curso)

3.1.7.1 Desarrollo de la Operación

La operación Red October, descubierta en 2012 pero activa desde 2007, fue una campaña de ciberespionaje avanzada que afectó a gobiernos, instituciones militares y organizaciones científicas en más de una docena de países. Utilizando correos de phishing dirigidos y malware modular, los atacantes lograron acceder a comunicaciones diplomáticas y datos clasificados.

3.1.7.2 Impacto Estratégico

El robo sistemático de información estratégica durante años destacó fallas críticas en la supervisión de sistemas gubernamentales. Además, expuso la falta de protocolos de detección temprana [26].

3.1.7.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Concienciación en ciberseguridad: Una capacitación adecuada podría haber prevenido la apertura de archivos adjuntos sospechosos.
2. Políticas de doble autenticación: Locked Shields promueve controles de acceso más estrictos, como la implementación de autenticación multifactorial para cuentas críticas.
3. Sensibilización sobre phishing avanzado: La concienciación del INCIBE podría haber ayudado a identificar patrones de correos maliciosos, reduciendo significativamente el éxito de los ataques.

3.1.8 Ciberataque a Colonial Pipeline (2021)

3.1.8.1 Desarrollo de la Operación

En mayo de 2021, Colonial Pipeline, la red de oleoductos más grande de Estados Unidos, sufrió un ciberataque masivo que comprometió sus sistemas de tecnología operativa (OT). El ataque fue llevado a cabo por un grupo de ransomware conocido como DarkSide, quienes lograron interrumpir el suministro de combustible a gran parte de la costa este del país. Los atacantes accedieron inicialmente a la red utilizando credenciales comprometidas adquiridas en el mercado negro.

3.1.8.2 Impacto Estratégico

El ataque resultó en la paralización temporal de los oleoductos, causando escasez de combustible y una crisis económica y logística significativa. Además, evidenció la vulnerabilidad de las infraestructuras críticas ante amenazas cibernéticas avanzadas [27].

3.1.8.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Gestión estratégica de accesos: La implementación de autenticación multifactorial, destacada en Locked Shields, podría haber prevenido el acceso inicial de los atacantes.
2. Simulaciones de crisis: La participación en ejercicios como Locked Shields habría ayudado a las autoridades a planificar y coordinar respuestas rápidas ante interrupciones de infraestructuras críticas.
3. Supervisión y auditoría periódica: La concienciación del INCIBE podría haber sensibilizado a los líderes sobre la importancia de supervisar los sistemas OT para evitar accesos no autorizados.

3.1.9 Hackeo al Parlamento Noruego (2020)

3.1.9.1 Desarrollo de la Operación

En 2020, el Parlamento de Noruega fue víctima de un ataque cibernético dirigido, en el que los atacantes accedieron a cuentas de correo electrónico de varios legisladores y robaron información confidencial. Las investigaciones apuntaron a un grupo de actores estatales, quienes utilizaron tácticas de phishing avanzado para obtener credenciales y acceder a las redes del Parlamento.

3.1.9.2 Impacto Estratégico

El ataque puso en evidencia la falta de medidas adecuadas de protección de las comunicaciones gubernamentales, además de generar tensiones diplomáticas entre Noruega y los países sospechosos de apoyar el ataque [28].

3.1.9.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Protección avanzada de correos electrónicos: Locked Shields entrena en la configuración de sistemas de seguridad en las plataformas de correo, lo que podría haber bloqueado intentos de phishing.
2. Concienciación de autoridades: La concienciación del INCIBE podría haber enfatizado la importancia de usar contraseñas seguras y autenticar accesos con medidas adicionales.
3. Planes de contingencia: La simulación de incidentes como este en ejercicios estratégicos habría mejorado la capacidad de respuesta y mitigación de los líderes políticos.

3.1.10 Pegasus y el espionaje global (2016 - en curso)

3.1.10.1 Desarrollo de la Operación

Pegasus, un software espía desarrollado por NSO Group, ha sido utilizado desde 2016 para infiltrarse en dispositivos móviles de políticos, periodistas y activistas en todo el mundo. Los ataques se realizaron mediante enlaces maliciosos enviados por SMS o mensajes de aplicaciones como WhatsApp, que, al ser abiertos, otorgaban acceso completo al dispositivo.

3.1.10.2 Impacto Estratégico

El uso de Pegasus expuso la capacidad de los gobiernos para realizar ciberespionaje masivo, lo que provocó importantes controversias éticas y legales. También resaltó la vulnerabilidad de los dispositivos móviles, incluso cuando se trataba de líderes de alto nivel [29].

3.1.10.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Sensibilización sobre seguridad móvil: La concienciación del INCIBE podría haber capacitado a los líderes para evitar abrir enlaces sospechosos en dispositivos sensibles.
2. Actualización y revisión constante de dispositivos: Locked Shields enfatiza la importancia de mantener los dispositivos actualizados y protegidos contra vulnerabilidades conocidas.
3. Políticas de comunicación segura: El uso de sistemas cifrados y restringidos, promovido en entrenamientos estratégicos, habría minimizado el impacto del espionaje.

3.1.11 Phising Farmacéutica Zendal O Porriño

3.1.11.1 Desarrollo de la Operación

En noviembre de 2020, el conglomerado farmacéutico Zendal, ubicado en O Porriño, Galicia, fue objeto de un fraude cibernético a través de "phishing". Los hackers suplantarón la identidad de un ejecutivo de alto nivel en la corporación, mediante el envío de correos electrónicos fraudulentos al director del departamento financiero. Estos comunicados proporcionaban directrices para efectuar transacciones bancarias a una presunta entidad multinacional asiática, argumentando que estaban vinculadas con la generación de vacunas contra la COVID-19. Durante un lapso de cuatro días, se llevaron a cabo veinte transacciones, acumulando un valor total superior a los nueve millones de euros [30].

3.1.11.2 Impacto Estratégico

La estafa ejerció un impacto financiero en Zendal, originando dificultades de liquidez que culminaron en la detección del fraude. La organización interpuso una denuncia ante la Guardia Civil, que emprendió una indagación con el objetivo de rastrear el destino de los fondos e identificar a los responsables. Este incidente evidenció la susceptibilidad de las organizaciones frente a ataques de ingeniería social y la urgente necesidad de robustecer las estrategias de ciberseguridad para resguardarse de tales amenazas.

3.1.1.3 Cómo la Concienciación para Autoridades Podría Haber Cambiado el Escenario

1. Normativas explícitas en relación con la verificación de órdenes financieras aconsejadas también por INCIBE: Si las autoridades corporativas hubieran implementado políticas rigurosas para la confirmación de órdenes de transferencia, particularmente aquellas que involucran grandes sumas de dinero, a través de canales de comunicación alternativos o autenticación multifactor, el fraude podría haber sido identificado previamente a su implementación.
2. Concienciación contra el phishing de INCIBE: La promoción activa de una cultura de ciberseguridad por parte de la alta dirección, que abarca la instrucción regular en la detección de correos electrónicos fraudulentos y la sensibilización sobre técnicas de ingeniería social, podría haber potenciado la habilidad del personal para detectar y prevenir intentos de fraude.

3.2 Test Sobre conocimientos en ciberseguridad y análisis de resultados

3.2.1 Objetivo del test.

La evaluación del grado de concienciación en ciberdefensa del personal se ha erigido como un instrumento esencial para la prevención de riesgos y la garantía de la seguridad en las organizaciones. Para alcanzar este propósito, se ha elaborado un test que facilita la identificación precisa de las fortalezas y debilidades en este campo, ofreciendo una perspectiva más nítida del nivel de concienciación y preparación de las autoridades militares.

El diseño del test surge de la necesidad de disponer de un instrumento eficiente y ágil que aborde las áreas más críticas de la ciberseguridad, tales como la administración de contraseñas, la identificación de phishing, la gestión segura de dispositivos y la seguridad en las redes sociales. Estas áreas han sido identificadas a partir de un análisis meticuloso del entorno actual en el contexto digital real y están concebidas para evaluar competencias particulares que podrían ser situaciones reales.

El valor primordial del test reside en su habilidad para proporcionar una valoración exhaustiva y fundamentada, tanto para las propias autoridades como para los equipos de capacitación. La evaluación

del grado de conocimiento del personal permite la formulación de estrategias educativas personalizadas que se ajusten a las necesidades específicas de cada individuo o colectivo. Así, se optimizan los recursos asignados a la capacitación y se potencia la eficacia de las estrategias de seguridad implementadas.

La estructura del test ha sido concebida con un enfoque en la sencillez y la claridad, eludiendo interrogantes superfluos y asegurando su ejecución rápida y eficaz. Cada interrogante se acompaña de un fundamento general que explica la razón de su inclusión, evidenciando de esta manera la relevancia de cada tópico tratado, centrado en la identificación de áreas susceptibles de mejora. Su implementación posibilita a las organizaciones enfocar sus estrategias de seguridad y adaptarse de forma proactiva a los retos del actual contexto digital.

3.2.2 Preguntas y justificación de las preguntas.

3.2.2.1 Pregunta: ¿Pertenece usted a las FAS?

Opciones:

1. Sí.
2. No.
3. No, pero sí al MDEF.
4. No sé qué es FAS.

3.2.2.1.1 Justificación de la pregunta:

Esta pregunta tiene como objetivo contextualizar el perfil del encuestado dentro del ámbito de las Fuerzas Armadas (FAS) o el Ministerio de Defensa (MDEF). La pertenencia a las FAS implica que el participante está sujeto a normas estrictas de seguridad informática debido al manejo potencial de información sensible o clasificada. Esta información ayuda a diferenciar los niveles de responsabilidad y exposición a riesgos cibernéticos, lo que es crucial para identificar patrones en la conciencia de ciberseguridad dentro de diferentes roles.

La opción de “No sé qué es FAS” también aporta valor al test al identificar lagunas de conocimiento en los términos y estructuras organizativas básicas, lo que puede ser indicativo de una falta de formación inicial o exposición limitada a temas de seguridad en este ámbito.

3.2.2.1.2 Respuesta correcta y justificación:

No hay una respuesta correcta o incorrecta en esta pregunta, ya que su objetivo es obtener información de contexto sobre los participantes. Sin embargo, para aquellos que pertenecen a las FAS o el MDEF, esta identificación permite orientar mejor las acciones de formación específica según sus necesidades. Por ejemplo, un miembro de las FAS puede necesitar formación sobre amenazas específicas, como el phishing dirigido, mientras que alguien externo puede beneficiarse más de una introducción general a buenas prácticas de seguridad.

3.2.2.1.3 Análisis de las respuestas incorrectas:

1. **“No”:** Esta opción no es incorrecta, pero indica que el encuestado no está vinculado directamente a las FAS. Esto podría significar que su exposición a protocolos estrictos de ciberseguridad es menor, lo que podría influir en sus respuestas posteriores.
2. **“No, pero sí al MDEF”:** Esta respuesta es válida, ya que refleja una vinculación con el Ministerio de Defensa sin formar parte directa de las FAS. Este perfil podría estar expuesto a normativas y formaciones similares a las de las FAS, pero con un enfoque más administrativo o menos operativo.

3. **“No sé qué es FAS”:** Esta opción revela una carencia de conocimiento básico sobre el entorno de defensa y seguridad, lo que podría ser preocupante si el encuestado está involucrado en actividades relacionadas con la seguridad informática. Este dato podría usarse para enfocar la formación en términos básicos antes de avanzar hacia conceptos más complejos.

3.2.2.1.4 Desarrollo ampliado:

La inclusión de esta pregunta inicial establece un marco para analizar la diversidad de participantes y ajustar las expectativas sobre su conocimiento previo en ciberseguridad. Los miembros de las FAS suelen estar sujetos a amenazas cibernéticas avanzadas debido a la naturaleza de su trabajo, que incluye la protección de datos clasificados y sistemas críticos. Por ejemplo, las operaciones militares modernas dependen en gran medida de sistemas conectados, desde comunicación por satélite hasta el uso de drones y redes de mando y control.

Un civil que no pertenece a las FAS o al MDEF puede no estar familiarizado con estas amenazas específicas, pero también es vulnerable a ataques comunes, como el phishing o el ransomware, que podrían tener consecuencias indirectas para las FAS si el atacante logra infiltrarse en la red mediante accesos comprometidos.

Por otro lado, la respuesta “No sé qué es FAS” resalta una brecha de conocimiento que podría ser útil para identificar la necesidad de educar a los participantes sobre los conceptos básicos relacionados con la defensa y la ciberseguridad. Por ejemplo, un participante que desconoce el significado de FAS podría no ser consciente de los riesgos asociados al manejo de información sensible, como el hecho de compartir contraseñas o acceder a sistemas sin autorización.

3.2.2.2 Pregunta: ¿Cuál es su rango de edad?

Opciones:

1. 20 - 29
2. 30 - 39
3. 40 - 49
4. 50 - 59
5. Más de 60.

3.2.2.2.1 Justificación de la pregunta:

Esta pregunta tiene como objetivo identificar posibles correlaciones entre el rango de edad de los participantes y su nivel de conciencia sobre ciberseguridad. Las diferentes generaciones tienen niveles variados de exposición y experiencia con tecnología digital y amenazas cibernéticas. Por ejemplo, personas más jóvenes podrían tener más experiencia en el uso de herramientas digitales, mientras que las generaciones mayores podrían estar menos familiarizadas con las amenazas emergentes, como el phishing o el malware avanzado.

Esta información puede ayudar a diseñar estrategias de formación en ciberseguridad adaptadas a las necesidades específicas de cada grupo etario. Además, permite evaluar si ciertos rangos de edad son más propensos a cometer errores relacionados con la ciberseguridad o a adoptar buenas prácticas.

3.2.2.2.2 Respuesta correcta y justificación:

Al igual que en la pregunta anterior, no hay una respuesta correcta o incorrecta, ya que esta pregunta está diseñada para recopilar datos demográficos. Sin embargo, el análisis de las respuestas permitirá

establecer patrones o tendencias que podrían influir en la eficacia de las campañas de concienciación en ciberseguridad.

3.2.2.2.3 Análisis de las respuestas incorrectas:

No aplica en esta pregunta, ya que todas las opciones son válidas y no implican valoraciones incorrectas.

3.2.2.2.4 Desarrollo ampliado:

La relación entre el rango de edad y la ciberseguridad es un área de investigación importante. Los estudios demuestran que las generaciones más jóvenes, como los millennials y la generación Z, tienden a tener una mayor alfabetización digital debido a su exposición temprana a la tecnología. Sin embargo, también pueden ser más propensos a asumir riesgos, como el uso de contraseñas simples o compartir información personal en redes sociales.

Por otro lado, las generaciones mayores, como los baby boomers, podrían ser más cautelosas, pero su menor familiaridad con términos técnicos o amenazas cibernéticas avanzadas podría hacerlos más vulnerables a tácticas como el phishing. Por ejemplo, un correo electrónico que simula ser de una institución bancaria podría ser más efectivo contra alguien que no está acostumbrado a identificar indicadores de fraude digital, como errores gramaticales o URLs sospechosas.

Entender las diferencias generacionales también ayuda a diseñar materiales educativos más efectivos. Para los jóvenes, podría ser más útil utilizar aplicaciones interactivas o simulaciones de ataques, mientras que, para los mayores, un enfoque basado en talleres presenciales podría ser más adecuado, este es el motivo de los laboratorios diseñados. En cualquier caso, reconocer estas diferencias es esencial para aumentar el nivel general de concienciación en ciberseguridad.

3.2.2.3 Pregunta: ¿Tiene asignado ordenador, teléfono o tablet del MDEF?

Opciones:

1. Sí.
2. No.
3. No, pero tengo acceso usuario y acceso a servicios CIS de MDEF.
4. No sé qué es MDEF.

3.2.2.3.1 Justificación de la pregunta:

Esta pregunta está diseñada para identificar el nivel de acceso tecnológico de los encuestados a dispositivos y sistemas gestionados por el Ministerio de Defensa (MDEF). La asignación de dispositivos como ordenadores, teléfonos o tablets implica una responsabilidad directa en el manejo seguro de estos recursos. Además, permite evaluar si los usuarios cuentan con los medios necesarios para interactuar con sistemas protegidos y si están conscientes de los protocolos de seguridad asociados.

Los servicios CIS (Comunicaciones y Sistemas de Información) son críticos en la gestión de información clasificada y comunicaciones seguras. La opción de "No sé qué es MDEF" también es relevante, ya que puede reflejar una falta de conocimiento organizativo o técnico que debería abordarse mediante formación específica.

3.2.2.3.2 Respuesta correcta y justificación:

No hay una respuesta correcta universal, ya que esta pregunta busca categorizar a los participantes según su nivel de acceso y familiaridad con los recursos del MDEF. Sin embargo, responder "Sí" o "No, pero

tengo acceso usuario y acceso a servicios CIS de MDEF" implica un nivel de compromiso y potencial exposición a riesgos cibernéticos que deben ser considerados en evaluaciones posteriores.

3.2.2.3.3 *Análisis de las respuestas incorrectas:*

1. **“No”:** Aunque válida, esta opción sugiere que el encuestado podría no estar directamente involucrado en la gestión o uso de dispositivos del MDEF, reduciendo su exposición a amenazas dirigidas a estos sistemas.
2. **“No, pero tengo acceso usuario y acceso a servicios CIS de MDEF”:** Esta respuesta indica un nivel de acceso relevante que debe ser gestionado con cuidado, ya que los servicios CIS son puntos críticos para la seguridad del MDEF.
3. **“No sé qué es MDEF”:** Similar a otras opciones de "desconocimiento", esta respuesta resalta una posible brecha en formación o experiencia, que podría comprometer la seguridad general si el encuestado accede a sistemas sin la preparación adecuada.

3.2.2.3.4 *Desarrollo ampliado:*

El uso de dispositivos asignados por organizaciones gubernamentales o militares, como el MDEF, conlleva riesgos y responsabilidades únicos. Estos dispositivos suelen estar configurados con medidas de seguridad avanzadas, como autenticación multifactorial, encriptación de datos y restricciones en el acceso a redes no seguras. Sin embargo, estas medidas solo son efectivas si los usuarios entienden y siguen los protocolos establecidos.

Por ejemplo, un teléfono del MDEF podría estar conectado a redes seguras que permiten la transmisión de información sensible. Si el usuario no es consciente de los riesgos de conectarse a redes públicas, podría inadvertidamente comprometer la seguridad del dispositivo y, por extensión, de toda la red. Además, el acceso a servicios CIS implica una mayor necesidad de formación, ya que estos sistemas gestionan información estratégica que podría ser objetivo de ciberataques.

3.2.2.4 **Pregunta: ¿Qué entiende Ud. por "mínimo privilegio"?**

Opciones:

1. Conceder acceso a toda la información a todos los miembros de la unidad.
2. Dar a cada usuario el mínimo acceso necesario para realizar su trabajo.
3. Permitir solo el acceso ilimitado a los miembros VIP.
4. No sé qué es.

3.2.2.4.1 *Justificación de la pregunta:*

El principio de "mínimo privilegio" es fundamental en la ciberseguridad, especialmente en entornos donde se maneja información sensible o clasificada. Esta pregunta evalúa si los participantes comprenden este concepto clave, que se refiere a limitar los accesos y permisos de los usuarios al nivel estrictamente necesario para cumplir con sus funciones.

Implementar este principio ayuda a reducir el riesgo de accesos no autorizados y minimiza el impacto potencial de un ataque interno o externo. Si los participantes no entienden este concepto, podría ser indicativo de la necesidad de una formación específica para garantizar que las prácticas organizativas de seguridad sean efectivas.

3.2.2.4.2 *Respuesta correcta y justificación:*

La respuesta correcta es "Dar a cada usuario el mínimo acceso necesario para realizar su trabajo." Este enfoque asegura que cada usuario tenga acceso solo a los recursos esenciales para sus

responsabilidades, limitando el riesgo de que información sensible sea comprometida por error o por intención maliciosa.

3.2.2.4.3 Análisis de las respuestas incorrectas:

1. **"Conceder acceso a toda la información a todos los miembros de la unidad"**: Esta opción contradice completamente el principio de mínimo privilegio y representa un riesgo significativo para la seguridad de la información.
2. **"Permitir solo el acceso ilimitado a los miembros VIP"**: Aunque los miembros VIP podrían requerir acceso a ciertos recursos adicionales, otorgarles acceso ilimitado es innecesario y puede aumentar las vulnerabilidades.
3. **"No sé qué es"**: Esta respuesta refleja una falta de conocimiento que podría comprometer la aplicación efectiva de políticas de seguridad y subraya la necesidad de formación.

3.2.2.4.4 Desarrollo ampliado:

El principio de privilegio mínimo se implementa en una variedad de esferas, desde la configuración de permisos en sistemas operativos hasta el acceso a documentos clasificados. Por ejemplo, un analista de inteligencia podría tener acceso exclusivo a los informes pertinentes a su campo de especialización, mientras que el acceso a otros documentos permanece limitado. Esto restringe los peligros en el escenario de que las competencias del analista sean comprometidas.

Dentro del ámbito bélico o gubernamental, la implementación de este principio disminuye la probabilidad de que un atacante, ya sea interno o externo, utilice accesos superfluos para adquirir información de naturaleza clasificada. Adicionalmente, este enfoque es crucial en la administración de incidentes, dado que posibilita la detección del origen de una brecha de seguridad y la mitigación de su repercusión.

Por ejemplo, en un sistema de correo electrónico clasificado, únicamente los usuarios que requieren la transmisión de mensajes asociados a operaciones particulares deberían tener acceso a dichas funcionalidades. Los usuarios que desempeñan funciones administrativas no deberían acceder a información operativa, dado que esto podría incrementar las probabilidades de un error humano o un ataque cibernético.

La formación en el principio de privilegio mínimo debería constituir una prioridad para asegurar su implementación efectiva. Esto engloba la concienciación de los usuarios respecto a los peligros inherentes a la concesión o solicitud de accesos superfluos, así como la implementación de sistemas automatizados que restrinjan los privilegios de forma predeterminada. Adicionalmente, las auditorías periódicas de acceso contribuyen a la preservación de este principio y aseguran que los permisos correspondan a las necesidades contemporáneas de los utilizadores.

3.2.2.5 Pregunta: ¿Utiliza la misma contraseña para diferentes cuentas o servicios?

Opciones:

1. Sí, en todas.
2. Sí, pero solo en algunas.
3. No, utilizo contraseñas diferentes para todo.
4. No estoy seguro/a.

3.2.2.5.1 Justificación de la pregunta:

Esta pregunta busca evaluar las prácticas de los encuestados en cuanto al manejo de contraseñas, un aspecto crítico de la ciberseguridad. El uso de la misma contraseña para múltiples cuentas representa un riesgo significativo, ya que, si una de estas cuentas se ve comprometida, todas las demás también quedarían vulnerables.

Comprender los hábitos de los usuarios en este ámbito ayuda a identificar áreas donde se necesita educación adicional sobre buenas prácticas, como la implementación de gestores de contraseñas o la creación de claves robustas y únicas.

3.2.2.5.2 Respuesta correcta y justificación:

La mejor respuesta es "No, utilizo contraseñas diferentes para todo." Esta práctica minimiza el impacto de una posible brecha de seguridad, ya que comprometer una cuenta no implica el acceso automático a otras.

3.2.2.5.3 Análisis de las respuestas incorrectas:

1. **"Sí, en todas":** Esta es la peor práctica posible, ya que permite que un atacante que obtenga una contraseña acceda a todas las cuentas vinculadas.
2. **"Sí, pero solo en algunas":** Aunque es mejor que la anterior, sigue siendo arriesgada, especialmente si las contraseñas compartidas protegen cuentas importantes o sensibles.
3. **"No estoy seguro/a":** Indica una falta de conciencia o control sobre las propias prácticas de ciberseguridad, lo que también es preocupante.

3.2.2.5.4 Desarrollo ampliado:

La implementación de contraseñas singulares para cada cuenta o servicio constituye una de las recomendaciones más significativas en el campo de la ciberseguridad. Esta práctica disminuye considerablemente el riesgo de un "efecto dominó" en caso de un compromiso con una contraseña.

Por ejemplo, un ciberdelincuente podría acceder a las credenciales de un usuario mediante una plataforma en línea con una seguridad insuficiente. Si dicho usuario emplea la misma contraseña para su correo electrónico y cuentas bancarias, el perpetrador podría acceder a datos financieros delicados y ocasionar perjuicios de magnitud considerable.

Para promover esta práctica, las entidades pueden incentivar la utilización de administradores de contraseñas, instrumentos que permiten la generación y almacenamiento seguro de claves únicas y robustas. Adicionalmente, la implementación de políticas que demanden la actualización regular de contraseñas y la utilización de mecanismos de autenticación multifactorial contribuye a la mitigación de riesgos.

Una contraseña segura ejemplar puede ser una frase extensa que amalgama palabras aleatorias, números y caracteres especiales, tal como "CiberSeguridad2024!Aprender". Esto la convierte en un desafío para la predicción, pero facilita su retención.

En síntesis, la instrucción de los usuarios acerca de los peligros inherentes al reciclaje de contraseñas y la provisión de soluciones prácticas resulta fundamental para optimizar la estrategia de seguridad global.

3.2.2.6 Pregunta: ¿Tiene su contraseña fechas o nombres que son fáciles de recordar para Ud.?

Opciones:

1. Sí.
2. Sí, pero no son evidentes como mi cumpleaños.
3. No, todo aleatorio.

3.2.2.6.1 Justificación de la pregunta:

Esta pregunta busca evaluar si los participantes están utilizando contraseñas seguras o si basan sus claves en información personal que podría ser fácilmente deducida por atacantes. Las contraseñas basadas en datos personales, como fechas significativas o nombres, son más vulnerables a ataques de fuerza bruta o de ingeniería social.

Conocer estas prácticas permite diseñar estrategias educativas para sensibilizar sobre la importancia de crear contraseñas robustas que no estén vinculadas a información identificable.

3.2.2.6.2 Respuesta correcta y justificación:

La mejor respuesta es "No, todo aleatorio." Esto refleja una práctica óptima en seguridad al garantizar que las contraseñas no sean predecibles ni vinculadas a datos personales.

3.2.2.6.3 Análisis de las respuestas incorrectas:

1. **"Sí":** Utilizar datos personales como contraseñas es una práctica altamente insegura. Información como fechas o nombres puede ser obtenida a través de redes sociales o interacciones con el usuario.
2. **"Sí, pero no son evidentes como mi cumpleaños":** Aunque es ligeramente mejor, esta opción sigue siendo arriesgada. Atacantes con suficiente información podrían deducir estas contraseñas mediante métodos de ingeniería social o ataques dirigidos.

3.2.2.6.4 Desarrollo ampliado

La protección de una contraseña está intrínsecamente vinculada a su imprevisibilidad y complejidad. Las contraseñas aleatorias que combinan letras, números y símbolos presentan una mayor dificultad para ser descifradas a través de ataques de fuerza bruta.

Por ejemplo, una contraseña como "M@5t3R-D1r3t1C" se caracteriza por su mayor seguridad en comparación con "Juan1978", dado que no presenta patrones de asociación fácil con el usuario. Adicionalmente, la utilización de administradores de contraseñas puede simplificar la generación y administración de claves robustas, eliminando la necesidad de recordarlas de forma manual.

Es imperativo instruir a los usuarios acerca de los peligros inherentes al uso de información personal en contraseñas para optimizar su estrategia de seguridad. Es también aconsejable instaurar políticas organizativas que insten a la renovación periódica de contraseñas y al empleo de verificaciones de alta complejidad.

3.2.2.7 Pregunta: ¿Qué hace si recibe un correo electrónico sospechoso de una fuente desconocida?

Opciones:

1. Lo abro para verificar que no me suena.

2. Lo marco como spam y lo elimino.
3. Lo reenvío a los compañeros de CIS para preguntar.
4. Nada, lo ignoro.

3.2.2.7.1 Justificación de la pregunta:

Esta pregunta evalúa la capacidad de los participantes para manejar correos electrónicos sospechosos, una de las principales vías de ataque en ciberseguridad. Acciones como abrir el correo o ignorarlo sin tomar medidas pueden aumentar el riesgo de comprometer la seguridad del sistema.

El objetivo es identificar qué tan conscientes son los usuarios de las buenas prácticas para evitar ataques de phishing o malware.

3.2.2.7.2 Respuesta correcta y justificación:

La mejor respuesta es "Lo marco como spam y lo elimino." Esto asegura que el correo no pueda causar daño ni en el momento ni en el futuro, reduciendo el riesgo de hacer clic en enlaces maliciosos o descargar archivos infectados.

3.2.2.7.3 Análisis de las respuestas incorrectas:

1. **"Lo abro para verificar que no me suena":** Esta acción es peligrosa, ya que algunos correos maliciosos pueden ejecutar código al ser abiertos o recopilar datos como confirmación de que la dirección de correo está activa.
2. **"Lo reenvío a los compañeros de CIS para preguntar":** Aunque involucra a un equipo de soporte, reenviar correos sospechosos puede propagar el contenido malicioso y poner en riesgo a otros usuarios.
3. **"Nada, lo ignoro":** Ignorar el correo no resuelve el problema, ya que el correo seguirá presente en la bandeja de entrada y podría ser abierto accidentalmente en el futuro.

3.2.2.7.4 Desarrollo ampliado:

La correcta gestión de correos electrónicos sospechosos es esencial para prevenir ataques de suplantación de identidad, que constituyen una amenaza considerable tanto para usuarios individuales como para organizaciones. De acuerdo con estadísticas contemporáneas, más del 90% de los ciberataques se originan a partir de un correo electrónico malintencionado.

Procedimientos tales como la categorización del correo electrónico como spam y su eliminación inmediata no solo disminuyen la probabilidad de interacción, sino que también contribuyen al entrenamiento de los filtros automáticos de correo no deseado. Adicionalmente, la divulgación de estos correos electrónicos al departamento de seguridad o al equipo de tecnología de la información puede simplificar la detección de amenazas dirigidas y optimizar las medidas de seguridad organizacionales.

Por ejemplo, una comunicación vía correo electrónico con el asunto "Urgente: Confirmar su cuenta ahora" que se origina desde una dirección inusual o presenta errores gramaticales debe ser considerado sospechoso. Es imperativo capacitar a los usuarios para identificar y reaccionar de manera adecuada para robustecer la ciberseguridad.

3.2.2.8 Pregunta: ¿Ha recibido alguna formación específica sobre cómo identificar correos de phishing?

Opciones:

1. Sí, recientemente.

2. Sí, pero hace más de un año.
3. No.
4. No sé.

3.2.2.8.1 Justificación de la pregunta:

Esta pregunta busca evaluar el nivel de formación de los participantes en la identificación de correos de phishing, una técnica de ataque común y altamente efectiva en ciberseguridad. Conocer si los encuestados han recibido formación y la frecuencia de esta permite identificar brechas en su preparación para manejar amenazas cibernéticas.

3.2.2.8.2 Respuesta correcta y justificación:

La respuesta ideal depende de las circunstancias, pero "Sí, recientemente" es la más deseable. La formación reciente asegura que los participantes estén al tanto de las últimas tácticas de phishing y sepan cómo identificarlas y responder a ellas.

5. Análisis de las respuestas incorrectas:

1. **"Sí, pero hace más de un año":** Aunque indica que el usuario tiene algún nivel de formación, las tácticas de phishing evolucionan rápidamente, lo que hace necesario actualizarse periódicamente.
2. **"No":** Indica una falta total de preparación en este tema, lo que puede poner al usuario en alto riesgo frente a correos maliciosos.
3. **"No sé":** Refleja una falta de conciencia o interés en su propio nivel de formación, lo cual es preocupante desde el punto de vista de la ciberseguridad.

3.2.2.8.3 Desarrollo ampliado:

El phishing constituye la principal causa de los ciberataques exitosos en entidades organizativas. Por consiguiente, la formación continua es indispensable para mitigar dicho riesgo. Por ejemplo, una sesión reciente podría instruir a los usuarios en la detección de correos electrónicos sospechosos mediante el análisis de la dirección del emisor, inexactitudes gramaticales y enlaces de naturaleza dudosa.

Las organizaciones eficaces en el ámbito de la ciberseguridad frecuentemente llevan a cabo simulaciones de suplantación de identidad con el objetivo de evaluar y consolidar el conocimiento de su personal. Estos ejercicios facilitan la identificación de los individuos más susceptibles a ser víctimas y orientan los esfuerzos pedagógicos hacia ellos.

La instrucción continua y las actualizaciones acerca de estrategias de phishing no solo salvaguardan a los individuos, sino que también robustecen la seguridad organizacional al disminuir la probabilidad de intrusiones.

3.2.2.9 Pregunta: ¿Bloquea su ordenador o móvil cuando se aleja de su puesto de trabajo?

Opciones:

1. Siempre.
2. A veces.
3. Nunca.
4. No es necesario, en mi caso nadie entra en mi despacho.

3.2.2.9.1 Justificación de la pregunta:

Esta pregunta busca identificar los hábitos de los usuarios respecto a la seguridad física de sus dispositivos. Bloquear un ordenador o móvil al dejarlo desatendido es una práctica fundamental para evitar accesos no autorizados y proteger información sensible.

3.2.2.9.2 Respuesta correcta y justificación:

"Siempre" es la respuesta más adecuada, ya que garantiza que el dispositivo esté protegido en todo momento, independientemente del entorno.

3.2.2.9.3 Análisis de las respuestas incorrectas:

1. **"A veces"**: Esta respuesta indica una práctica inconsistente que puede exponer al usuario a riesgos innecesarios, especialmente en entornos compartidos.
2. **"Nunca"**: Representa una grave negligencia en términos de seguridad, dejando el dispositivo completamente vulnerable.
3. **"No es necesario, en mi caso nadie entra en mi despacho"**: Este razonamiento es erróneo, ya que la seguridad no debe depender de supuestos sobre el acceso físico al espacio.

3.2.2.9.4 Desarrollo ampliado.

El bloqueo de dispositivos constituye una práctica fundamental, aunque esencial, en el ámbito de la seguridad cibernética y física. Incluso en contextos catalogados como seguros, los aparatos pueden ser susceptibles a intrusiones no autorizadas. Por ejemplo, un atacante interno o un visitante esporádico podrían utilizar un dispositivo desbloqueado para sustraer datos.

Con el objetivo de promover esta práctica, numerosas entidades establecen políticas de bloqueo automático tras un período breve de inactividad. Adicionalmente, la instrucción de los usuarios acerca de la relevancia del bloqueo de sus dispositivos puede evitar incidentes de seguridad tanto intencionados como accidentales.

Un hábito eficaz consiste en bloquear manualmente el dispositivo al levantarse, complementado por acciones automáticas. Esta garantía garantiza que, incluso en situaciones de olvido, el dispositivo mantendrá su protección.

3.2.2.10 Pregunta: ¿Utiliza redes Wi-Fi para acceder a información con los dispositivos de MDEF?

Opciones:

1. Sí, frecuentemente.
2. Sí, solo cuando estoy fuera de la oficina y tengo que trabajar.
3. Sí, pero siempre uso VPN.
4. No, solo con el teléfono o la tablet.
5. No, nunca me conecto con dispositivos de MDEF a Wi-Fi "civiles".

3.2.2.10.1 Justificación de la pregunta:

Esta pregunta busca identificar el nivel de exposición de los dispositivos oficiales del Ministerio de Defensa (MDEF) a redes Wi-Fi no controladas. Conectarse a redes públicas o civiles con dispositivos

gubernamentales representa un riesgo significativo de seguridad, ya que estas redes pueden ser utilizadas para interceptar datos o llevar a cabo ataques dirigidos.

3.2.2.10.2 Respuesta correcta y justificación:

"No, nunca me conecto con dispositivos de MDEF a Wi-Fi 'civiles'" es la respuesta más segura, ya que elimina el riesgo de interacciones con redes potencialmente comprometidas. En caso de ser necesario el uso de redes externas, "Sí, pero siempre uso VPN" sería aceptable, ya que garantiza un nivel adicional de protección mediante cifrado.

3.2.2.10.3 Análisis de las respuestas incorrectas:

1. **"Sí, frecuentemente"**: Esta práctica es altamente riesgosa, ya que incrementa la exposición de los dispositivos a redes inseguras y posibles ataques.
2. **"Sí, solo cuando estoy fuera de la oficina y tengo que trabajar"**: Aunque refleja una necesidad práctica, esta opción sigue siendo peligrosa si no se utilizan medidas de seguridad adicionales.
3. **"No, solo con el teléfono o la tablet"**: Si bien puede parecer menos riesgoso, los teléfonos y tablets también contienen información sensible y deben ser protegidos de igual manera.
4. **"Sí, pero siempre uso VPN"**: Aunque es una práctica aceptable en situaciones inevitables, lo ideal sería evitar redes no controladas siempre que sea posible.

3.2.2.10.4 Desarrollo ampliado:

La utilización de redes Wi-Fi públicas o no verificadas con dispositivos pertenecientes al MDEF puede poner en riesgo datos delicados y sistemas de importancia crítica. Por ejemplo, un agresor en una red pública tiene la capacidad de interceptar comunicaciones, inyectar software malicioso o incluso acceder a sistemas internos mediante la utilización de vulnerabilidades.

La implementación de una Red Privada Virtual (VPN) constituye una estrategia de mitigación efectiva, dado que cifra las comunicaciones y disminuye la probabilidad de interceptación. No obstante, incluso utilizando una VPN, las redes públicas pueden continuar siendo susceptibles a ataques de tipo "man-in-the-middle".

Es imperativo que las entidades gubernamentales y militares privilegien la utilización de redes privadas seguras y proporcionen educación a los usuarios acerca de los riesgos inherentes a las redes externas. Adicionalmente, los aparatos oficiales deben estar configurados para eliminar de manera automática la conexión a redes no autorizadas y solicitar la autorización de los administradores para su utilización.

3.2.2.11 Pregunta: ¿Con qué frecuencia borra el historial de sus conexiones Wi-Fi?

Opciones:

1. Nunca.
2. Una vez al año.
3. Siempre después de conectarme.
4. No sé.

3.2.2.11.1 Justificación de la pregunta:

Esta pregunta pretende evaluar la conciencia de los participantes sobre la seguridad de las redes a las que se conectan. El historial de conexiones Wi-Fi puede ser utilizado por atacantes para identificar patrones de uso o explotar redes previamente utilizadas.

3.2.2.11.2 Respuesta correcta y justificación:

"Siempre después de conectarme" es la mejor práctica, ya que elimina el riesgo de que un atacante utilice información del historial para replicar redes confiables (ataques de suplantación o "evil twin").

3.2.2.11.3 Análisis de las respuestas incorrectas:

1. **"Nunca"**: Dejar un historial completo de conexiones aumenta el riesgo de ataques dirigidos y expone patrones de uso.
2. **"Una vez al año"**: Aunque mejor que nunca, no es suficiente para garantizar la seguridad en caso de dispositivos utilizados en redes externas.
3. **"No sé"**: Refleja una falta de conciencia sobre la importancia de esta práctica, lo que podría comprometer la seguridad del usuario.

3.2.2.11.4 Desarrollo ampliado:

La eliminación del historial de conexiones Wi-Fi tras su utilización constituye una estrategia preventiva esencial para disminuir la susceptibilidad a redes fraudulentas o malintencionadas. Por ejemplo, un atacante podría replicar el nombre de una red previamente implementada con el objetivo de manipular al dispositivo y lograr acceso.

La implementación automatizada de esta práctica puede realizarse mediante la configuración de dispositivos para evitar el almacenamiento automático de redes Wi-Fi. Adicionalmente, las entidades pueden instruir a los usuarios acerca de los peligros vinculados al historial de conexiones y las estrategias para su gestión segura.

En contextos gubernamentales, donde la seguridad es de vital importancia, esta práctica debe ser complementada con la política de eludir redes públicas y utilizar exclusivamente redes protegidas o conexiones seguras, como las Redes de Privación Virtual (VPN).

3.2.2.12 Pregunta: ¿Qué haces si tu dispositivo de trabajo te pide una actualización de software en medio de tu jornada laboral?

Opciones:

1. Actualizo inmediatamente.
2. Lo pospongo para otro momento.
3. Lo ignoro.
4. Consulto con un compañero de CIS antes de proceder.

3.2.2.12.1 Justificación de la pregunta:

Esta pregunta evalúa cómo los participantes manejan actualizaciones de software, una práctica esencial para mantener la seguridad del dispositivo. Las actualizaciones suelen incluir parches para vulnerabilidades conocidas, y no realizarlas a tiempo puede exponer al sistema a riesgos innecesarios.

3.2.2.12.2 Respuesta correcta y justificación:

"Actualizo inmediatamente" es la respuesta ideal, ya que asegura que el dispositivo esté protegido contra las últimas amenazas conocidas.

3.2.2.12.3 *Análisis de las respuestas incorrectas:*

1. **"Lo pospongo para otro momento":** Esta opción puede parecer conveniente, pero aumenta el tiempo en que el dispositivo está vulnerable a ataques que podrían haberse prevenido con la actualización.
2. **"Lo ignoro":** Ignorar las actualizaciones es una práctica extremadamente riesgosa, ya que deja el dispositivo expuesto indefinidamente.
3. **"Consulta con un compañero de CIS antes de proceder":** Aunque refleja prudencia, en la mayoría de los casos las actualizaciones deben realizarse sin demoras, salvo que haya instrucciones específicas en contra.

3.2.2.12.4 *Desarrollo ampliado:*

La actualización periódica del software representa una de las estrategias más eficaces para salvaguardar dispositivos y redes frente a ataques cibernéticos. Por ejemplo, numerosas brechas de seguridad, tal como el ataque "WannaCry", explotaron vulnerabilidades previamente corregidas mediante parches.

Es imperativo que las organizaciones establezcan una política explícita para la implementación de actualizaciones automáticas o manuales inmediatas cuando sea seguro hacerlo. En contextos críticos, donde las actualizaciones podrían tener repercusiones en las operaciones en curso, puede resultar razonable realizar una consulta previa al procedimiento. Sin embargo, esto debería ser una excepción y no una norma.

Es vital instruir a los usuarios acerca de la relevancia de las actualizaciones e instaurar mecanismos que reduzcan las interrupciones operativas durante su implementación.

3.2.2.13 **Pregunta: Si ves una actividad sospechosa en tu computadora (por ejemplo, ventanas emergentes o software no autorizado), ¿Qué haces?**

Opciones:

1. Lo ignoro.
2. Informo inmediatamente a los compañeros de CIS.
3. Reinicio la computadora.
4. Trato de solucionarlo por mi cuenta.

3.2.2.13.1 *Justificación de la pregunta:*

Esta pregunta busca medir la capacidad de los participantes para responder adecuadamente ante señales de posible compromiso de seguridad. Una reacción oportuna y adecuada puede prevenir daños mayores.

3.2.2.13.2 *Respuesta correcta y justificación:*

"Informo inmediatamente a los compañeros de CIS" es la mejor respuesta, ya que asegura que el incidente sea gestionado por expertos en ciberseguridad con las herramientas y procedimientos adecuados.

3.2.2.13.3 *Análisis de las respuestas incorrectas:*

1. **"Lo ignoro":** Ignorar actividad sospechosa permite que posibles amenazas sigan operando sin restricciones, aumentando el riesgo.
2. **"Reinicio la computadora":** Aunque puede solucionar problemas menores, reiniciar no aborda el problema raíz y podría eliminar temporalmente evidencia crucial para la investigación.

3. **"Trato de solucionarlo por mi cuenta":** A menos que el usuario tenga formación específica en ciberseguridad, esta acción puede empeorar la situación o eliminar información necesaria para el análisis.

3.2.2.13.4 Desarrollo ampliado:

La identificación precoz y la respuesta apropiada constituyen elementos fundamentales para atenuar los perjuicios derivados de un incidente de seguridad. La notificación de actividad sospechosa al equipo de ciberseguridad facilita un examen exhaustivo y la implementación de acciones correctivas y preventivas.

Por ejemplo, la aparición de ventanas emergentes atípicas podría sugerir la presencia de software malicioso o adware, mientras que la presencia de software no autorizado podría sugerir un acceso no autorizado al sistema. El equipo encargado de CIS tiene la capacidad de llevar a cabo análisis forenses para establecer la magnitud del problema y adoptar medidas preventivas como el aislamiento del dispositivo o la intensificación de las medidas de seguridad.

3.2.2.14 Pregunta: ¿Has recibido formación en ciberseguridad en los últimos 12 meses?

Opciones:

1. Sí.
2. No.
3. No es necesario para mi puesto.

3.2.2.14.1 Justificación de la pregunta:

Esta pregunta pretende evaluar si los participantes han recibido formación actualizada en ciberseguridad, un factor clave para garantizar que estén preparados para enfrentar amenazas emergentes. La formación regular es esencial en un entorno donde las tácticas de ataque evolucionan constantemente.

3.2.2.14.2 Respuesta correcta y justificación:

"Sí" es la respuesta más adecuada, ya que refleja que el participante ha recibido la capacitación necesaria para estar al día con las mejores prácticas de ciberseguridad.

3.2.2.14.3 Análisis de las respuestas incorrectas:

1. **"No":** Indica una falta de preparación en un área crítica. Sin formación actualizada, los usuarios pueden no estar al tanto de las últimas amenazas y cómo mitigarlas.
2. **"No es necesario para mi puesto":** Aunque algunos roles pueden no parecer directamente relacionados con la ciberseguridad, todos los empleados tienen un papel en proteger la información organizativa y personal.

3.2.2.14.4 Desarrollo ampliado:

La instrucción continua en el campo de la ciberseguridad no solo salvaguarda a los individuos, sino también a las organizaciones de potenciales deficiencias en la seguridad. Por ejemplo, un empleado que carezca de habilidades para identificar un correo de suplantación de identidad puede constituir el origen de un ataque de mayor envergadura.

Es muy importante que las entidades instauren programas de capacitación periódicos y adaptados a las exigencias particulares de cada puesto. Esto abarca talleres prácticos, simulaciones de ataques y módulos interactivos destinados a facilitar a los usuarios la identificación de amenazas y la acción efectiva ante ellas.

3.2.2.15 Pregunta: ¿Cómo sueles identificar si un correo es de phishing?

Opciones:

1. Reviso la dirección de correo electrónico del remitente.
2. Verifico la gramática y el lenguaje del mensaje.
3. Sospecho si me piden información personal o contraseñas.
4. No estoy seguro/a de cómo identificar un correo de phishing.

3.2.2.15.1 Justificación de la pregunta:

Esta pregunta busca identificar el nivel de conocimiento práctico de los participantes sobre los indicadores comunes de correos de phishing. Reconocer estos signos es crucial para evitar interacciones con mensajes maliciosos.

3.2.2.15.2 Respuesta correcta y justificación:

"Reviso la dirección de correo electrónico del remitente", "Verifico la gramática y el lenguaje del mensaje" y "Sospecho si me piden información personal o contraseñas" son todas respuestas correctas, ya que reflejan acciones efectivas para identificar correos de phishing. Una combinación de estas prácticas es ideal.

3.2.2.15.3 Análisis de las respuestas incorrectas:

1. **"No estoy seguro/a de cómo identificar un correo de phishing"**: Esta respuesta evidencia una falta de conocimiento que puede exponer al usuario y a su organización a riesgos significativos.

Desarrollo ampliado:

Los correos de suplantación de identidad constituyen una de las modalidades más prevalentes de ciberataques. Estos mensajes tienden a incorporar errores en la dirección del emisor, vocabulario de naturaleza urgente o alarmista, y peticiones de información personal o contraseñas.

Por ejemplo, un correo electrónico que aparenta ser originario de una entidad bancaria, pero que presenta errores gramaticales o un enlace de naturaleza sospechosa, debe ser tratado con cautela. Instruir a los usuarios en la identificación de estas señales y en la verificación directa de las solicitudes con la entidad pertinente constituye una estrategia eficaz para la mitigación del riesgo.

Adicionalmente, las entidades pueden implementar filtros avanzados de correo electrónico y campañas de concientización para fortalecer la habilidad de los trabajadores para identificar y administrar correos de carácter sospechoso de forma segura.

3.2.2.16 Pregunta: ¿Has recibido alguna vez un correo de phishing que parecía legítimo?

Opciones:

1. Sí, y casi caigo en la trampa.
2. Sí, pero lo identifiqué a tiempo.
3. No, nunca.
4. No lo sé.

3.2.2.16.1 Justificación de la pregunta:

Esta pregunta evalúa la experiencia personal de los participantes con correos de phishing, un aspecto crucial para entender su nivel de exposición y capacidad para manejar este tipo de amenazas.

3.2.2.16.2 Respuesta correcta y justificación:

No hay una respuesta correcta universal, pero "Sí, pero lo identifiqué a tiempo" es indicativa de una capacidad adecuada para reconocer y evitar este tipo de ataques.

3.2.2.16.3 Análisis de las respuestas incorrectas:

1. **"Sí, y casi caigo en la trampa":** Aunque refleja experiencia, también muestra una vulnerabilidad que debe ser abordada con formación.
2. **"No, nunca":** Puede indicar una falta de exposición, pero también es posible que el participante no haya reconocido intentos de phishing.
3. **"No lo sé":** Refleja una falta de conciencia sobre el tema, lo que puede ser preocupante desde el punto de vista de la ciberseguridad.

3.2.2.16.4 Desarrollo ampliado:

Los correos electrónicos de suplantación de identidad son responsables de una elevada proporción de incidentes de seguridad. La detección temprana de intentos de suplantación de identidad antes de interactuar con ellos es fundamental para prevenir vulnerabilidades en la seguridad.

Por ejemplo, una táctica habitual consiste en un correo electrónico que simula ser de un proveedor de servicios, acompañado de un enlace para "verificar tu cuenta". Identificar indicadores como direcciones de remitente sospechosas o contenido de naturaleza alarmista puede contribuir a prevenir incursiones en dichas trampas.

Adicionalmente, las entidades pueden fortalecer la capacitación mediante ejercicios prácticos, tales como simulaciones de tácticas de phishing, con el objetivo de potenciar la capacidad de los usuarios para detectar estos intentos.

3.2.2.17 . Pregunta: ¿Qué deberías hacer si recibes una llamada telefónica de alguien que dice ser del equipo de soporte técnico pidiéndote datos o credenciales?

Opciones:

1. Le doy los datos si parece legítimo.
2. Cuelgo la llamada inmediatamente.
3. Le pido más información y luego llamo a los que conozco de CIS.
4. No estoy seguro de cómo actuar.

3.2.2.17.1 Justificación de la pregunta:

Esta pregunta busca evaluar la capacidad de los participantes para manejar intentos de ingeniería social por teléfono, un método común para obtener credenciales o información sensible.

3.2.2.17.2 Respuesta correcta y justificación:

"Le pido más información y luego llamo a los que conozco de CIS" es la respuesta más adecuada, ya que permite verificar la legitimidad de la llamada sin proporcionar información sensible de inmediato.

3.2.2.17.3 Análisis de las respuestas incorrectas:

1. **"Le doy los datos si parece legítimo":** Esta respuesta es peligrosa, ya que la ingeniería social se basa en parecer confiable para engañar a las víctimas.

2. **"Cuelgo la llamada inmediatamente"**: Aunque evita el riesgo, no aborda la posibilidad de reportar un intento de fraude al equipo de seguridad.
3. **"No estoy seguro de cómo actuar"**: Indica una falta de preparación frente a un tipo común de amenaza.

Desarrollo ampliado:

Las denominadas prácticas fraudulentas constituyen un método eficaz de ingeniería social, que se fundamenta en la confianza y la insuficiente preparación de las víctimas. Los atacantes frecuentemente se presentan bajo la apariencia de personal de soporte técnico con el objetivo de solicitar credenciales o acceso a sistemas.

Por ejemplo, una notificación que señala "hemos detectado actividad inusual en tu cuenta, necesitamos tu contraseña para resolverlo" debería ser interpretada como sospechoso. Es aconsejable corroborar la legitimidad de la llamada mediante canales oficiales.

Es imperativo que las organizaciones instruyan a sus empleados acerca de estos riesgos y proporcionen directrices explícitas para su respuesta, tales como abstenerse de divulgar credenciales por teléfono y reportar inmediatamente intentos sospechosos.

3.2.2.18 Pregunta: ¿Qué harías si te percatas de que un compañero de trabajo está manejando información sensible de manera insegura?

Opciones:

1. Le informo directamente y le sugiero seguir buenas prácticas.
2. Lo reporto al equipo de CIS responsable o a su jefe directo.
3. No hago nada, bastante tengo con manejar mi información correctamente.
4. No estoy seguro de cómo actuar.

3.2.2.18.1 Justificación de la pregunta:

Esta pregunta evalúa la disposición de los participantes para actuar ante prácticas inseguras en el manejo de información. Identificar y corregir estas situaciones es crucial para mantener un entorno seguro y proteger la información sensible.

3.2.2.18.2 Respuesta correcta y justificación:

"Lo reporto al equipo de CIS responsable o a su jefe directo" es la mejor respuesta, ya que asegura que la situación será abordada por el personal adecuado, pudiendo contar con los recursos necesarios para implementar medidas correctivas.

3.2.2.18.3 Análisis de las respuestas incorrectas:

1. **"Le informo directamente y le sugiero seguir buenas prácticas"**: Aunque demuestra iniciativa, puede no ser suficiente si la situación requiere una intervención más estructurada o si el compañero no corrige su conducta.
2. **"No hago nada, bastante tengo con manejar mi información correctamente"**: Refleja una falta de compromiso con la seguridad colectiva, lo que puede poner en riesgo a toda la organización.

3. **"No estoy seguro de cómo actuar"**: Indica una falta de preparación y conocimiento sobre los procedimientos establecidos para estas situaciones.

3.2.2.18.4 Desarrollo ampliado:

La gestión inapropiada de la información puede resultar en repercusiones severas, tales como la divulgación de información delicada o el acceso no autorizado a sistemas. Es obligación de todos los trabajadores mantener un ambiente seguro y reportar comportamientos que ponen en riesgo la ciberseguridad.

Por ejemplo, si un empleado deja documentos de carácter confidencial a la vista en un espacio compartido, esto debe ser notificado inmediatamente para prevenir la exposición o el uso indebido de información delicada.

Las entidades deben instruir a su personal para identificar dichas circunstancias y ofrecer vías explícitas para su reporte sin temor a represalias. Esta situación fomenta una cultura de seguridad colaborativa y fortalece las defensas domésticas.

3.2.2.19 Pregunta: Si tienes acceso limitado a ciertos sistemas o datos en tu Unidad, ¿has intentado alguna vez acceder a información a la que no tienes permisos?

Opciones:

1. Sí, pero solo por curiosidad.
2. No, nunca.
3. A veces, si lo considero necesario para el trabajo.
4. No, pero podría hacerlo si es una emergencia.

3.2.2.19.1 Justificación de la pregunta:

Esta pregunta busca evaluar el respeto de los participantes hacia las políticas de acceso y privilegios establecidos. Intentar acceder a información sin permisos es una violación de las normas de seguridad y puede tener consecuencias graves para la organización y el individuo.

3.2.2.19.2 Respuesta correcta y justificación:

"No, nunca" es la respuesta más adecuada, ya que demuestra un compromiso con las políticas de seguridad y el respeto hacia las restricciones de acceso implementadas.

3.2.2.19.3 Análisis de las respuestas incorrectas:

1. **"Sí, pero solo por curiosidad"**: Refleja una actitud negligente hacia las políticas de acceso, lo que podría ser explotado por actores malintencionados.
2. **"A veces, si lo considero necesario para el trabajo"**: Aunque podría parecer razonable, actuar fuera de los permisos establecidos sin autorización es una violación de las normas.
3. **"No, pero podría hacerlo si es una emergencia"**: Aunque plantea una excepción, este tipo de decisiones debe ser realizado con la aprobación de superiores o equipos responsables.

3.2.2.19.4 Desarrollo ampliado:

Es imperativo respetar las políticas de acceso para preservar la integridad de los sistemas y salvaguardar la información delicada. El intento de acceder a datos o sistemas sin las autorizaciones pertinentes puede resultar en brechas de seguridad y en sanciones disciplinarias.

Por ejemplo, un trabajador que busca acceder a informes categorizados "por curiosidad" puede poner en riesgo la confidencialidad de la información y exponerla a amenazas externas.

Para prevenir tales circunstancias, las entidades deben instaurar controles de acceso rigurosos y documentar todas las operaciones en los sistemas con el fin de identificar intentos no autorizados. Adicionalmente, resulta esencial cultivar una cultura de cumplimiento en la que los trabajadores comprendan la relevancia de adherirse a las normativas y comunicar cualquier incidente o requerimiento de acceso adicional.

3.2.2.20 Pregunta: Encuentras un dispositivo USB en el suelo. ¿Qué haces?

Opciones:

1. Lo abro para ver si por la información que contiene puedo encontrar a su dueño.
2. Lo tiro a la basura.
3. Lo formateo y lo uso, después de ver que no tiene nada peligroso.
4. No sé qué hacer en esa situación.

3.2.2.20.1 Justificación de la pregunta:

Esta pregunta evalúa la capacidad de los participantes para manejar situaciones relacionadas con dispositivos externos, como los USB, que pueden ser vectores de malware o intentos de ingeniería social.

3.2.2.20.2 Respuesta correcta y justificación:

"No sé qué hacer en esa situación" puede ser válida si se usa como punto de partida para buscar ayuda, pero lo ideal es evitar interactuar con dispositivos encontrados y reportarlo al equipo de TI o seguridad.

3.2.2.20.3 Análisis de las respuestas incorrectas:

1. **"Lo abro para ver si por la información que contiene puedo encontrar a su dueño":** Es una práctica riesgosa, ya que los USB encontrados podrían contener malware diseñado para comprometer el sistema al ser conectado.
2. **"Lo tiro a la basura":** Aunque evita un uso inadecuado, no aborda la posibilidad de reportar el incidente para un análisis adecuado del dispositivo.
3. **"Lo formateo y lo uso, después de ver que no tiene nada peligroso":** Este comportamiento es inseguro, ya que el formateo no siempre elimina malware avanzado y usar dispositivos de origen desconocido puede exponer al sistema a riesgos.

3.2.2.20.4 Desarrollo ampliado:

Los dispositivos USB constituyen un vector habitual para la propagación de software malicioso. Un caso ilustrativo fue la utilización de USB infectados en el ataque Stuxnet, que impactó sistemas de carácter industrial. La conexión con un USB no autorizado puede poner en riesgo datos delicados o inducir la infección de redes completas.

Las entidades deben instruir a su personal acerca de los peligros inherentes a la interacción con dispositivos externos y establecer directrices explícitas, como la comunicación de cualquier USB detectado al departamento de Tecnologías de la Información para su análisis.

3.2.2.21 Pregunta: ¿Qué puedes hacer para mejorar tu privacidad en línea?

Opciones:

1. No usar redes sociales.
2. Usar contraseñas fuertes y no compartir información personal.
3. La seguridad en línea no existe.
4. Tengo dudas sobre cuáles son los pasos a seguir.

3.2.2.21.1 Justificación de la pregunta:

Esta pregunta busca evaluar el conocimiento de los participantes sobre prácticas básicas para proteger su privacidad en línea. También permite identificar áreas donde los usuarios necesitan más educación.

3.2.2.21.2 Respuesta correcta y justificación:

"Usar contraseñas fuertes y no compartir información personal" es la respuesta más adecuada, ya que refleja medidas prácticas y efectivas para mejorar la privacidad.

3.2.2.21.3 Análisis de las respuestas incorrectas:

1. **"No usar redes sociales"**: Aunque limita la exposición, no es una solución práctica ni necesaria si se implementan buenas prácticas de seguridad.
2. **"La seguridad en línea no existe"**: Es una afirmación incorrecta y pesimista que ignora las herramientas y estrategias disponibles para protegerse.
3. **"Tengo dudas sobre cuáles son los pasos a seguir"**: Indica una falta de conocimiento que podría ser abordada con formación específica.

3.2.2.21.4 Desarrollo ampliado:

Optimizar la privacidad en el entorno digital conlleva la implementación de estrategias como el uso de contraseñas únicas y robustas, la habilitación de la autenticación multifactor, la revisión de las configuraciones de privacidad en las plataformas de redes sociales y la restricción de la cantidad de información personal divulgada.

Por ejemplo, un usuario que divulga de manera constante su localización en las plataformas de redes sociales podría estar expuesto a ataques físicos o digitales. La instrucción sobre la relevancia de una gestión meticulosa de la información personal es esencial para la mitigación de riesgos.

Adicionalmente, las entidades pueden proporcionar herramientas como talleres o directrices prácticas para asistir a los empleados y usuarios en la protección efectiva de su privacidad en línea.

3.2.3 Análisis de la muestra.

En la elaboración de esta investigación, se diseñó un examen con el objetivo de evaluar el grado de conocimientos en ciberseguridad y las habilidades en autoprotección digital de las autoridades militares. Para corroborar la validez de esta herramienta, se utilizó como muestra a los componentes del Máster, que constituyen un conjunto homogéneo de profesionales con experiencia avanzada en tecnología. Esta metodología facilitó la evaluación del diseño del examen en un entorno controlado; sin embargo, los resultados no reflejan adecuadamente al público objetivo real, dado que las autoridades militares suelen poseer un grado de conocimientos técnicos considerablemente más diverso.

La realización del test por los estudiantes del Máster proporcionó una evaluación inicial de la eficacia

del cuestionario y facilitó la identificación de áreas particulares de mejora en la formulación de las preguntas, asegurando su pertinencia y eficacia para futuras implementaciones en agrupaciones militares. Este análisis preliminar proporciona una perspectiva inicial sobre cómo un colectivo de alto nivel técnico aborda cuestiones de ciberseguridad, subrayando la necesidad de ajustar las estrategias de sensibilización en función del perfil de los participantes.

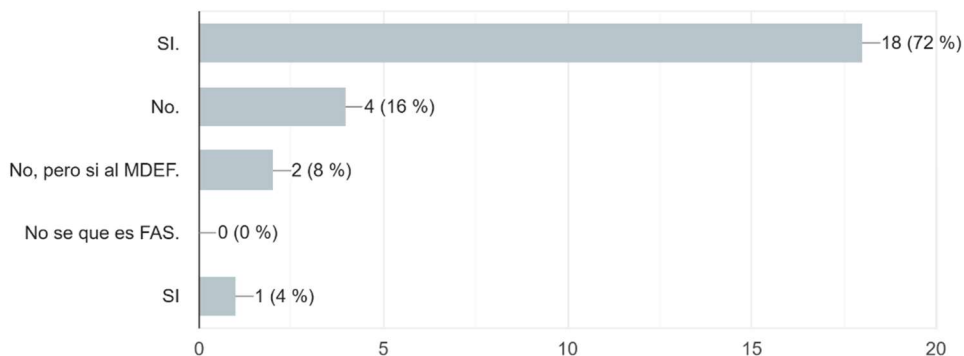
Este segmento expone el contexto de la muestra, complementado con una descripción general del diseño del examen y su ejecución. Los hallazgos derivados serán analizados gráficamente y detallados pregunta por pregunta en la subsiguiente sección, proporcionando una perspectiva exhaustiva del rendimiento de los participantes y estableciendo los cimientos para la optimización de la herramienta antes de su implementación en el público objetivo original.

3.2.4 *Análisis y Grafico de los resultados anónimos de los componentes del Master.*

En este apartado se presentan de forma gráfica los resultados obtenidos en el test realizado a los componentes de la promoción del Master y en un análisis que va pregunta a pregunta se justifican las respuestas menos correctas y queda en evidencia la formación en seguridad y autoprotección incluso entre el personal más preparado técnicamente, como es el caso.

3.2.4.1 ¿Pertenece usted a las FAS?

¿ Pertenece usted de las FAS ?
25 respuestas



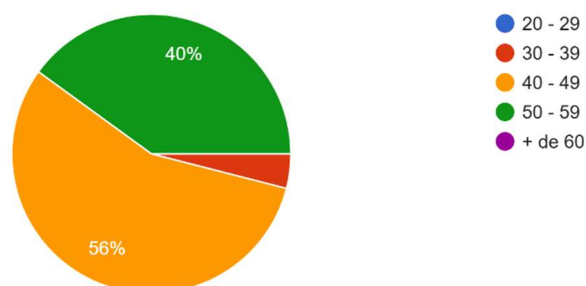
3-1 Grafico 1ª Pregunta

3.2.4.1.1 *Análisis*

Al ser un MASTER organizado por el CUD de Vigo y por CESTIC, el resultado es el esperado.

3.2.4.2 Pregunta: ¿Cuál es su rango de edad?

¿ Cual es su rango de edad?
25 respuestas



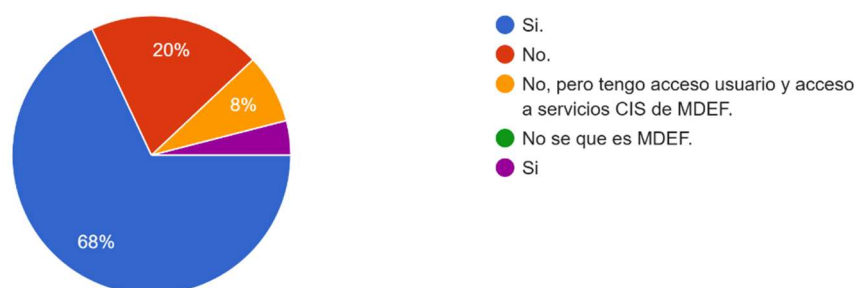
3-2 2ª Pregunta

3.2.4.2.1 Análisis

El rango de edad es casi estándar, por el empleo al que está destinado el Master.

3.2.4.3 Pregunta: ¿Tiene asignado ordenador, teléfono o tablet del MDEF?

¿ Tiene asignado ordenador, teléfono o tablet de MDEF?
25 respuestas



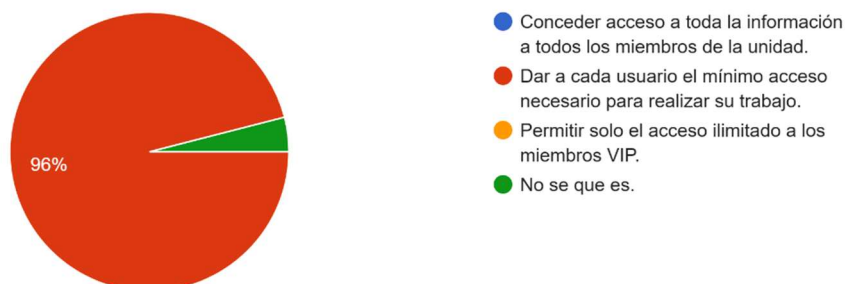
3-3 3ª Pregunta

3.2.4.3.1 Análisis

El nivel de responsabilidad y la vinculación hacen que mayoritariamente la respuesta sea que sí.

3.2.4.4 Pregunta: ¿Qué entiende Ud. por "mínimo privilegio"?

¿Qué entiende ud. por "mínimo privilegio"?
25 respuestas



3-4 4ª Pregunta

3.2.4.4.1 Análisis

El personal del Master en su inmensa mayoría debe de conocer que se entiende por “mínimo privilegio”

3.2.4.5 Pregunta: ¿Utiliza la misma contraseña para diferentes cuentas o servicios?

¿Utilizas la misma contraseña para diferentes cuentas o servicios?
25 respuestas



3-5 5ª Pregunta

3.2.4.5.1 Análisis

Dentro de un colectivo técnico como este, se anticipa una comprensión avanzada de los riesgos vinculados al uso de contraseñas repetitivas. No obstante, las respuestas a la interrogante "¿Utiliza la misma contraseña para diferentes cuentas o servicios?" tienden a oscilar entre "sí" y "no", lo cual pone de manifiesto una heterogeneidad atribuible a factores tanto personales como laborales.

Por un lado, los individuos que responden "sí" pueden dar prioridad a la comodidad y la practicidad. Pese a la comprensión de los riesgos, la administración de múltiples cuentas y servicios induce a ciertos profesionales a seleccionar contraseñas reiteradas para optimizar su gestión. Adicionalmente, puede incidir una percepción del riesgo adaptada al contexto, en la que se considera aceptable la reutilización de contraseñas en servicios de menor impacto, reservando contraseñas exclusivas para cuentas de mayor

sensibilidad. Un elemento adicional es la confianza depositada en contraseñas de alta robustez, postulando que una contraseña técnicamente sólida puede compensar su reutilización. Además, ciertos profesionales aún no han incorporado sistemas de gestión de contraseñas en sus rutinas, ya sea debido a la falta de práctica, resistencia al cambio o una percepción errónea de su complejidad o seguridad.

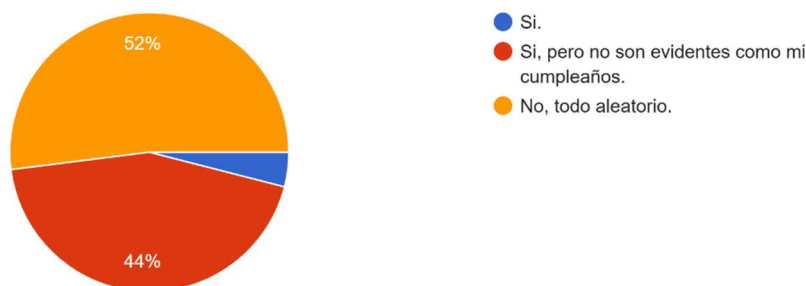
En contraposición, los individuos que responden "no" tienden a aplicar su conocimiento técnico en la praxis. Los profesionales técnicos están más expuestos a ejemplos concretos de vulnerabilidades, tales como el robo de contraseñas, y adoptan contraseñas únicas como estrategia estándar. Adicionalmente, la utilización de administradores de contraseñas promueve la generación y almacenamiento de credenciales únicas, lo que contribuye a la reducción de la carga cognitiva. Su experiencia y capacitación los conciencian acerca de la relevancia de diversificar contraseñas, particularmente si desempeñan roles de liderazgo o reciben formación en ciberseguridad. Para ciertos individuos, experiencias anteriores con ataques cibernéticos también funcionan como catalizador para la implementación de medidas más rigurosas.

A pesar de que poseen una comprensión técnica avanzada, las respuestas evidencian la influencia de factores individuales tales como hábitos previos, carga de cuentas y percepciones de riesgo. Este comportamiento heterogéneo enfatiza la necesidad de fortalecer la sensibilización y fomentar herramientas accesibles, como los gestores de contraseñas, incluso entre expertos, con el objetivo de mitigar la discrepancia entre el conocimiento y la práctica.

3.2.4.6 Pregunta: ¿Tiene su contraseña fechas o nombres que son fáciles de recordar para Ud.?

¿ Tiene su contraseña fechas o nombres que son fáciles de recordar para Ud.?

25 respuestas



3-6 6ª Pregunta

3.2.4.6.1 Análisis

Produce respuestas predominantemente segmentadas entre "no" y "sí, pero no evidentes como mi cumpleaños." Esta diversidad evidencia la persistencia de matices en la implementación de prácticas de seguridad incluso entre expertos en ciberseguridad.

Los individuos que responden "no" tienden a adoptar una metodología más rigurosa en la generación de contraseñas. Este conjunto abarca los peligros vinculados a la inclusión de datos personales, tales como fechas o nombres, que pueden ser fácilmente descifrados a través de técnicas de ingeniería social o ataques de diccionario. Es plausible que se empleen herramientas tales como administradores de contraseñas para generar claves completamente aleatorias, erradicando la necesidad de confiar en datos personales, incluso cuando estos son menos evidentes. Esta respuesta señala una mayor concordancia con las prácticas óptimas en materia de ciberseguridad.

En contraposición, los individuos que responden "sí, pero no evidentes como mi cumpleaños" evidencian una percepción de seguridad moderada. A pesar de que este colectivo admite el peligro de emplear información directamente vinculada a su identidad, tales como fechas significativas o nombres comunes, sostienen que la utilización de variantes menos perceptibles disminuye su exposición de manera significativa. Por ejemplo, podrían recurrir al uso de fechas no vinculadas directamente con ellos o nombres combinados con otros elementos, tales como números y caracteres exclusivos. Esta práctica puede conferir una sensación de seguridad, sin embargo, aún deja margen para vulnerabilidades en caso de que se utilicen métodos de ataque sofisticados, tales como la integración de ingeniería social con herramientas automatizadas.

Esta segmentación de respuestas evidencia que, incluso en perfiles técnicos, se evidencia una tensión entre la implementación de prácticas de seguridad óptimas y la comodidad o confianza percibida en contraseñas "personalizadas pero seguras". Para potenciar la sensibilización, resultaría beneficioso subrayar que, a pesar de que una contraseña fundamentada en información personal menos patente puede parecer segura, las herramientas de ataque contemporáneas son capaces de identificar patrones complejos. Fomentar la utilización de contraseñas completamente aleatorias y resguardadas en administradores de contraseñas continúa siendo la estrategia más eficaz, incluso para aquellos individuos que perciben estar logrando un equilibrio entre la seguridad y la facilidad de uso.

3.2.4.7 Pregunta: ¿Qué hace si recibe un correo electrónico sospechoso de una fuente desconocida?

¿Qué hace si recibes un correo electrónico sospechoso de una fuente desconocida?

25 respuestas



3-7 7ª Pregunta

3.2.4.7.1 Análisis

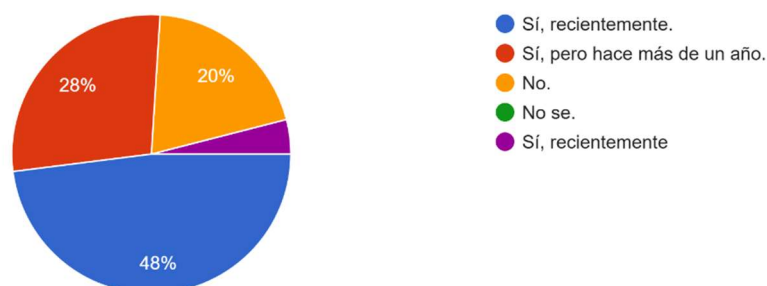
En un colectivo técnico 2, la interrogante "¿Qué hace si recibe un correo electrónico sospechoso de una fuente desconocida?" ha producido una diversidad de respuestas heterogéneas, evidenciando la heterogeneidad en los métodos y prácticas de ciberseguridad incluso entre profesionales de alto nivel. Las alternativas ofrecidas abarcaban desde abrir el correo para corroborar su pertinencia, hasta categorizarlo como spam y su eliminación, reenviarlo a los compañeros de seguridad (CIS) para corroborar su legitimidad, o simplemente ignorarlo.

Esta heterogeneidad en las respuestas pone de manifiesto, una vez más, cómo elementos tales como la percepción individual del riesgo, la experiencia anterior con incidentes análogos y las rutinas personales pueden incidir en las decisiones adoptadas frente a potenciales amenazas. Aunque poseen un dominio técnico avanzado, las conductas evidencian variados grados de concienciación y posturas en relación con la administración de correos electrónicos sospechosos. Esto subraya la imperiosa necesidad de

consolidar las prácticas óptimas y estandarizar los protocolos de respuesta en ciberseguridad, incluso en contextos donde los participantes poseen una formación técnica robusta.

3.2.4.8 Pregunta: ¿Ha recibido alguna formación específica sobre cómo identificar correos de phishing?

¿Ha recibido alguna formación específica sobre cómo identificar correos de phishing?
25 respuestas



3-8 8ª Pregunta

3.2.4.8.1 Análisis

Según si los alumnos han interpretado que se refiere a su entorno laboral o a este Master habrán contestado unas cosas u otras, porque durante el curso se han dado pautas para identificar los correos de phishing.

3.2.4.9 Pregunta: ¿Bloquea su ordenador o móvil cuando se aleja de su puesto de trabajo?

¿Bloqueas tu ordenador o móvil cuando te alejas de tu puesto de trabajo?
25 respuestas



3-9 9ª Pregunta

3.2.4.9.1 Análisis

La respuesta mayoritaria de siempre, deja una evidencia clara de que todos los alumnos están concienciados con esta práctica.

3.2.4.10 Pregunta: ¿Utiliza redes Wi-Fi para acceder a información con los dispositivos de MDEF?

¿Utilizas redes Wi-Fi para acceder a información con los dispositivos de MDEF?
24 respuestas



3-10 10ª Pregunta

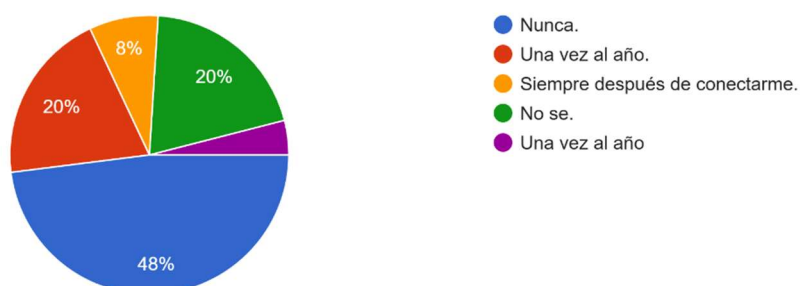
3.2.4.10.1 Análisis

Ha producido respuestas predominantemente positivas en relación con prácticas óptimas de ciberseguridad. Las alternativas abarcan desde la utilización habitual de redes Wi-Fi hasta la abstención total de conexiones "civiles", pasando por respuestas intermedias que incorporan la implementación de VPN para asegurar la seguridad de las comunicaciones.

Estas respuestas evidencian un elevado grado de sensibilización respecto a los peligros vinculados al uso de redes Wi-Fi públicas o no seguras. A pesar de que algunos participantes señalan que se conectan fuera del entorno laboral, suelen adoptar medidas preventivas como la utilización de VPN, mientras que otros optan por evitar el uso de redes no reguladas mediante dispositivos de MDEF. Este comportamiento evidencia una sólida comprensión de las consecuencias de la seguridad y la implementación de estrategias preventivas apropiadas para reducir los riesgos en contextos críticos. Esta afirmación evidencia la aplicabilidad de las prácticas óptimas entre perfiles técnicos que gestionan información delicada.

3.2.4.11 Pregunta: ¿Con qué frecuencia borra el historial de sus conexiones Wi-Fi?

¿ Con que frecuencia borra el historial de sus conexiones WIFI?
25 respuestas



3-11 11ª Pregunta

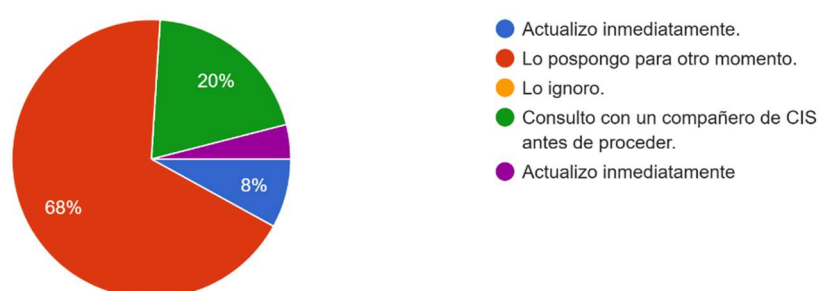
3.2.4.11.1 Análisis

Otra vez, ha producido respuestas diversas, lo que evidencia una notable heterogeneidad en los comportamientos asociados con esta práctica de ciberseguridad. Las alternativas se extienden desde aquellos individuos que nunca borran su historial de conexiones, hasta aquellos que lo hacen de manera regular tras cada uso o al menos una vez al año, mientras que algunos admiten desconocer esta funcionalidad.

Esta heterogeneidad en las respuestas evidencia que, a pesar del alto nivel de conocimiento técnico de los participantes, no todos perciben esta acción como una prioridad en su rutina de seguridad. Esta situación podría atribuirse a una percepción de riesgo reducido vinculada al historial de conexiones o a una insuficiente sensibilización específica sobre cómo esta práctica puede prevenir accesos no autorizados en dispositivos de importancia crítica. En consecuencia, esta interrogante evidencia la necesidad de intensificar la relevancia de la administración proactiva de configuraciones fundamentales, como el historial de redes Wi-Fi en los dispositivos empleados para propósitos delicados y sensibles.

3.2.4.12 Pregunta: ¿Qué haces si tu dispositivo de trabajo te pide una actualización de software en medio de tu jornada laboral?

¿Qué haces si tu dispositivo de trabajo te pide una actualización de software en medio de tu jornada laboral?
25 respuestas



3-12 12ª Pregunta

3.2.4.12.1 Análisis

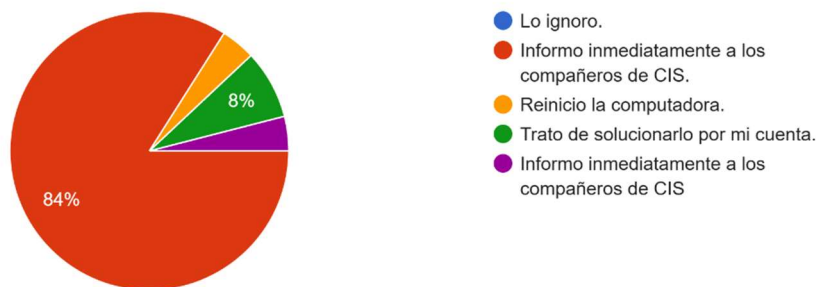
Ha producido respuestas que, en su mayoría, evidencian la inclinación hacia la postergación de la acción para un momento posterior. Esta conducta pone de manifiesto una postura común incluso entre perfiles técnicos, en los que la administración de prioridades operativas tiende a prevalecer sobre la actualización inmediata del dispositivo.

Esta propensión a postergar las actualizaciones podría atribuirse a la percepción de que el proceso constituye una perturbación para el flujo de trabajo o a la suposición de que no constituye un riesgo inmediato. No obstante, tal comportamiento podría obstaculizar la implementación de parches de seguridad esenciales, exponiendo tanto el dispositivo como los sistemas a potenciales vulnerabilidades. A pesar de que numerosos participantes reconocen la relevancia de mantener el software actualizado, esta interrogante pone de manifiesto que, incluso entre expertos, las obligaciones laborales inmediatas tienden a relegar prácticas efectivas de ciberseguridad a un segundo plano. Este hecho enfatiza la necesidad de potenciar la concienciación acerca de la importancia de las actualizaciones oportunas como una estrategia preventiva fundamental.

3.2.4.13 Pregunta: Si ves una actividad sospechosa en tu computadora (por ejemplo, ventanas emergentes o software no autorizado), ¿Qué haces?

Si ves una actividad sospechosa en tu computadora (por ejemplo, ventanas emergentes o software no autorizado), ¿Qué haces?

25 respuestas



3-13 13ª Pregunta

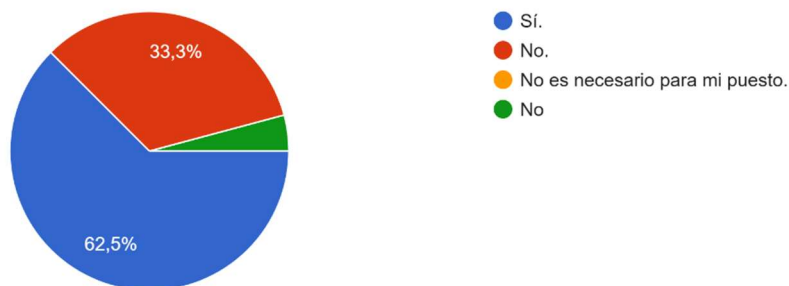
3.2.4.13.1 Análisis

La respuesta mayoritaria de informar a los expertos, evidencia una correcta percepción del riesgo.

3.2.4.14 Pregunta: ¿Has recibido formación en ciberseguridad en los últimos 12 meses?

¿Has recibido formación en ciberseguridad en los últimos 12 meses?

24 respuestas



3-14 14ª Pregunta

3.2.4.14.1 Análisis

Todo el personal ha recibido formación en ciberseguridad durante el curso, las repuestas negativas son debidas a considerar que el test se refleja es sobre su entorno laboral habitual.

3.2.4.15 Pregunta: ¿Cómo sueles identificar si un correo es de phishing?

¿Cómo sueles identificar si un correo es de phishing?
25 respuestas



3-15 15ª Pregunta

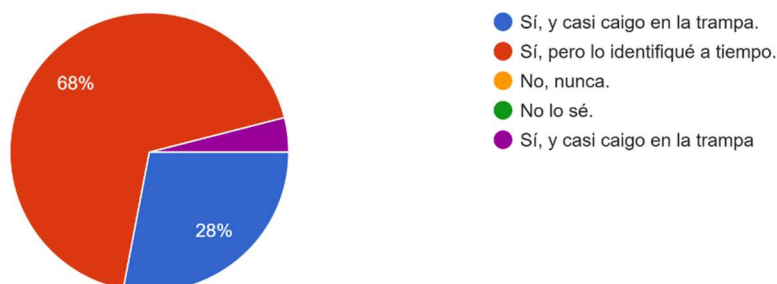
3.2.4.15.1 Análisis

Una amplia mayoría de respuestas acertadas en su totalidad, aunque había múltiples opciones correctas disponibles. Este hallazgo evidencia un elevado grado de sensibilización y capacitación en la detección de correos electrónicos malintencionados, subrayando la habilidad de los participantes para aplicar criterios técnicos y pragmáticos al examinar potenciales tácticas de suplantación de identidad.

Los participantes evidenciaron una sólida comprensión de los indicadores habituales de suplantación de identidad, tales como enlaces de carácter sospechoso, errores gramaticales, remitentes desconocidos o solicitudes atípicas. Esta consistencia en las respuestas correctas evidencia que los conocimientos adquiridos en el contexto del máster han demostrado ser eficaces en la concienciación sobre esta amenaza particular, y que los estudiantes son capaces de aplicar estos conocimientos en un contexto real, lo que contribuye a una reducción significativa de los riesgos vinculados a estos ataques.

3.2.4.16 Pregunta: ¿Has recibido alguna vez un correo de phishing que parecía legítimo?

¿Has recibido alguna vez un correo de phishing que parecía legítimo?
25 respuestas



3-16 16ª Pregunta

3.2.4.16.1 Análisis

Ha generado respuestas predominantemente centradas en las opciones afirmativas, con una distinción entre aquellos que "casi caen en la trampa" y aquellos que "lo identificaron a tiempo." Esto pone de manifiesto que, a pesar de que los participantes poseen un grado avanzado de conocimientos en ciberseguridad, las estrategias de phishing cada vez más sofisticadas logran, al menos en sus fases iniciales, suscitar incertidumbre incluso entre perfiles técnicos.

La prevalencia de respuestas afirmativas subraya la reiteración con la que estos correos electrónicos son recibidos por los usuarios, incluso en entornos profesionales, y cómo su diseño puede ser persuasivo. Los individuos que admiten haber detectado el intento a tiempo evidencian una robusta habilidad para implementar los conocimientos de ciberseguridad en contextos reales. Además, los individuos que "casi caen en la trampa" evidencian que, a pesar de su formación técnica, el phishing puede aprovechar vulnerabilidades humanas o momentos de distracción, lo que enfatiza la necesidad de continuar con el fortalecimiento de la concienciación.

Este estudio evidencia que, a pesar de la importancia de los conocimientos técnicos, el phishing continúa siendo una amenaza efectiva debido a su habilidad para emular comunicaciones auténticas. Este hecho subraya la relevancia de entrenamientos prácticos y simulaciones especializadas para capacitar a los usuarios, incluso en contextos técnicos, para identificar y gestionar estos intentos con confianza y celeridad.

3.2.4.17 Pregunta: ¿Qué deberías hacer si recibes una llamada telefónica de alguien que dice ser del equipo de soporte técnico pidiéndote datos o credenciales?

¿Qué deberías hacer si recibes una llamada telefónica de alguien que dice ser del equipo de soporte técnico pidiéndote datos o credenciales?
25 respuestas



3-17 17ª Pregunta

3.2.4.17.1 Análisis

La mayoría de las respuestas han sido precisas, focalizadas en las alternativas "Cuelgo la llamada inmediatamente" y "Le pido más información y luego llamo a los que conozco de CIS". Esto evidencia un alto grado de sensibilización respecto a los peligros vinculados al vishing (phishing telefónico) y una estrategia proactiva para la protección de información delicada.

Los participantes que seleccionaron la opción de colgar inmediatamente evidencian una comprensión explícita de la prohibición de interactuar con potenciales agresores, erradicando cualquier riesgo de exposición. Por otro lado, aquellos individuos que optan por recopilar más datos antes de establecer

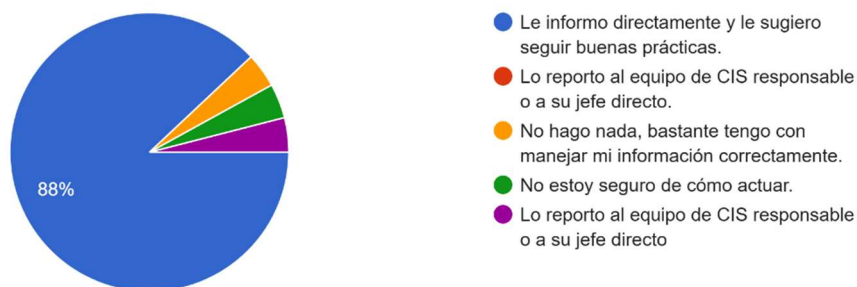
contacto con un equipo de soporte conocido, tal como CIS, manifiestan una postura prudente, pero adoptando un enfoque más colaborativo y analítico que puede resultar beneficioso para la investigación de posibles incidentes.

Este comportamiento evidencia que, a pesar de la validez de ambos enfoques, el nivel técnico del grupo facilita la comprensión de que cualquier solicitud de datos delicados debe ser abordada con desconfianza y medidas de verificación. Esto enfatiza la relevancia de mantener una comunicación transparente y accesible con los equipos internos de apoyo técnico, además de la necesidad de fortalecer políticas organizativas que orienten dichas respuestas en todos los estratos, incluyendo perfiles no técnicos.

3.2.4.18 Pregunta: ¿Qué harías si te percatas de que un compañero de trabajo está manejando información sensible de manera insegura?

¿Qué harías si te percatas de que un compañero de trabajo está manejando información sensible de manera insegura?

25 respuestas



3-18 18ª Pregunta

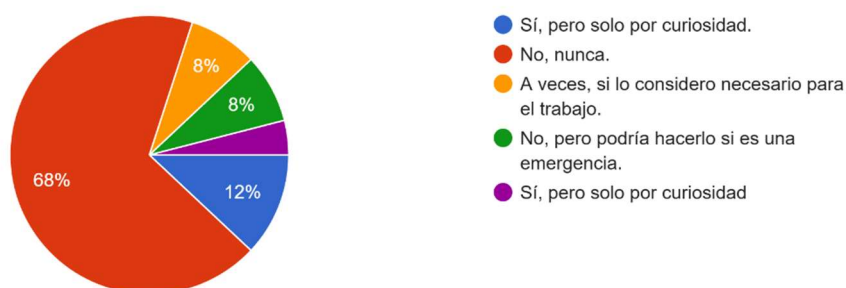
3.2.4.18.1 Análisis

Por el nivel de los empleos de los alumnos, y que la mayoría tienen responsabilidades relacionadas con los CIS, la respuesta ha sido informarle y sugerirle buenas practicas, correcta, aunque también había otras correctas.

3.2.4.19 Pregunta: Si tienes acceso limitado a ciertos sistemas o datos en tu Unidad, ¿has intentado alguna vez acceder a información a la que no tienes permisos?

Si tienes acceso limitado a ciertos sistemas o datos en tu Unidad, ¿has intentado alguna vez acceder a información a la que no tienes permisos?

25 respuestas



3-19 19ª Pregunta

3.2.4.19.1 Análisis

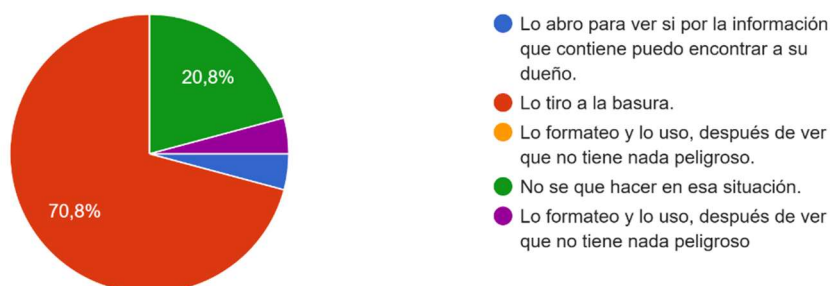
Ha producido una mayoría de respuestas negativas, con una marcada tendencia hacia la opción "No, nunca", mientras que una minoría, representada por el 12% de los participantes, ha indicado que sí han intentado acceder a información sin permisos, motivados por la curiosidad. Esto pone de manifiesto una sólida comprensión y adhesión a los principios de ética profesional y cumplimiento normativo entre la mayoría, aunque también resalta la existencia de conductas contrarias que podrían representar un riesgo de seguridad.

Los participantes que eligieron "No, nunca" evidencian un alto nivel de compromiso con las políticas de acceso y la confidencialidad de la información, lo que refleja una cultura organizacional orientada a la seguridad y el respeto a los permisos establecidos. Este comportamiento está alineado con las mejores prácticas de seguridad informática, que destacan la importancia de mantener la integridad y la confianza en el manejo de datos sensibles.

Por otro lado, el 12% de los encuestados que afirmaron haber intentado acceder a información por curiosidad evidencia una brecha en la concienciación sobre las implicaciones éticas y legales de estas acciones. Este fenómeno podría atribuirse a la falta de capacitación específica o a la percepción de que dichos comportamientos no implican consecuencias graves, especialmente cuando la motivación no responde a una intención maliciosa.

3.2.4.20 Pregunta: Encuentras un dispositivo USB en el suelo. ¿Qué haces?

Encuentras un dispositivo USB en el suelo. ¿Qué haces?
24 respuestas



3-20 20ª Pregunta

3.2.4.20.1 Análisis

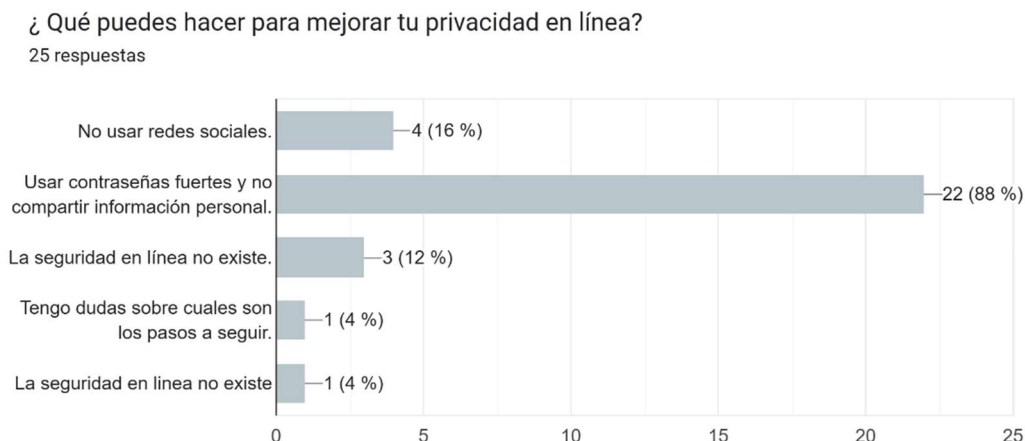
Ha producido una mayoría de respuestas correctas, con una marcada tendencia hacia la opción "Lo tiro a la basura", mientras que el resto de respuestas se inclina hacia "No sé qué hacer en esa situación". Esto pone de manifiesto una comprensión sólida de los riesgos vinculados a los dispositivos USB desconocidos, aunque también manifiesta cierta incertidumbre entre aquellos individuos que carecen de claridad sobre cómo actuar.

Los participantes que optan por tirar el USB a la basura evidencian un alto grado de sensibilización respecto a los riesgos asociados a la conexión con dispositivos no autorizados, tales como la potencial introducción de software malicioso o la activación de scripts malintencionados. Esta conducta se alinea con las prácticas óptimas de ciberseguridad, las cuales subrayan la relevancia de eludir cualquier interacción con hardware de procedencia incierta.

Además, aquellos individuos que indicaron desconocimiento de cómo actuar evidencian una carencia de formación o experiencia especializada en tales circunstancias, a pesar de su perfil técnico. Este fenómeno podría atribuirse a la ausencia de protocolos explícitos o a que dichos escenarios no se tratan siempre en los programas de capacitación en ciberseguridad.

Este estudio subraya la relevancia de fortalecer la conciencia en la gestión de dispositivos físicos desconocidos, incluso entre los profesionales técnicos. Adicionalmente, enfatiza la necesidad de incorporar estas circunstancias en los entrenamientos prácticos, tales como simulaciones de escenarios, con el objetivo de disminuir la incertidumbre y asegurar que las respuestas se alineen con las prácticas de seguridad más efectivas.

3.2.4.21 Pregunta: ¿Qué puedes hacer para mejorar tu privacidad en línea?



3-21 21ª Pregunta

3.2.4.21.1 Análisis

Se ha producido una mayoría de respuestas que se alinean con la opción "Usar contraseñas fuertes y no compartir información personal", mientras que una minoría se decantó por "La seguridad en línea no existe". Esto evidencia un alto grado de sensibilización respecto a las prácticas óptimas de privacidad digital, combinado con un grado de escepticismo en una proporción reducida del conjunto.

La mayoría, al optar por la segunda alternativa, evidencia un entendimiento explícito de que la privacidad digital puede ser optimizada de manera significativa a través de estrategias pragmáticas, tales como la implementación de contraseñas robustas y la restricción de la divulgación de información personal. Esta conducta se alinea con el perfil técnico de los participantes, quienes están plenamente conscientes de los peligros vinculados a la exposición excesiva en línea y los beneficios de implementar estrategias de autoprotección.

En contraste, los individuos que seleccionaron la tercera alternativa manifiestan una percepción más fatalista o escéptica respecto a la eficacia de las medidas de privacidad, posiblemente atribuible a experiencias anteriores con filtraciones o al conocimiento de vulnerabilidades sistémicas en plataformas digitales. A pesar de que esta perspectiva es menos frecuente, subraya la necesidad de consolidar la noción de que, aunque la seguridad absoluta puede no ser alcanzable, la instauración de prácticas óptimas puede disminuir considerablemente los riesgos.

Este comportamiento enfatiza la necesidad de continuar promoviendo estrategias de privacidad proactivas y concientizar sobre cómo incluso acciones elementales pueden ejercer un efecto positivo en la salvaguarda de los datos personales y profesionales en un contexto digital.

3.3 Taller de Sensibilización sobre Ciberseguridad para Autoridades Militares

El Taller que se presenta a continuación es un compendio de herramientas de software desarrolladas para el ámbito civil, cada una de ellas para reforzar aspectos concretos de la ciberseguridad, se han escogido aplicaciones o programas que están al alcance de todo el mundo, con unos interfaces sencillos y que precisamente por esa sencillez se consideran los más adecuados para realizar un taller tipo laboratorio de ciberseguridad para autoridades militares.

El entorno donde debe ser realizado este taller es en un aula próximo a las propias unidades militares que disponga de una conexión a internet “libre”, no filtrado por las herramientas de seguridad gubernamentales, dotada con unos equipos informáticos también “libres” sin necesidad de características especiales y con sistema operativo Windows. Debe ser tutorizado por personal técnico con una capacidad docente en lo relacionado con estas técnicas de autoprotección, la formación concreta de este personal docente no es materia de desarrollo para este trabajo. El taller está enfocado en que no genere rechazo por parte de las autoridades, se debe adaptar a la capacidad técnica de cada uno, no siendo tan importante realizar las practicas concretas como comprender los conceptos que aquí se describen y generar la correspondiente preocupación en las conciencias de las autoridades.

Inspirado en el ejercicio de la OTAN, este Taller es una mezcla de escenarios prácticos con capacitación según el nivel de partida del alumno, adoptando un enfoque que ha evidenciado su eficacia en la preparación de equipos para afrontar ciberataques, desde los más básicos hasta los que son de alta complejidad. Además, se integra la visión de los kits de sensibilización elaborados por el INCIBE, que proporcionan una base pedagógica robusta para tratar las amenazas más prevalentes desde un enfoque práctico y accesible para los diferentes perfiles técnicos de las autoridades.

3.3.1 Objetivo del Taller

El objetivo del Taller de Concienciación en Ciberseguridad es suministrar a altos cargos y oficiales militares las herramientas indispensables para identificar, prevenir y reaccionar ante amenazas cibernéticas diseñadas específicamente para su posición de liderazgo, tales como el phishing, spear-phishing y whaling. Estas estrategias de ataque se valen de su acceso a información delicada y sistemas críticos, lo que enfatiza la necesidad de robustecer su habilidad para identificar y mitigar estos riesgos de forma eficaz.

El taller se enfoca no solo en la salvaguarda de sistemas críticos, sino también en la protección de la información personal de los funcionarios, reconociendo que ambos componentes constituyen metas prioritarias para los ciberdelincuentes. Mediante la integración de simulaciones de situaciones reales con tácticas de autoprotección, se aspira a dotar a los participantes de habilidades que superen el dominio técnico, incorporando elementos operativos y estratégicos indispensables para asegurar la seguridad cibernética en todos los estratos.

En conclusión, el propósito primordial de este laboratorio es convertir el conocimiento teórico en acciones prácticas, facultando a las autoridades militares para abordar con confianza las amenazas emergentes en el ciberespacio y asegurar la resiliencia de los sistemas bajo su jurisdicción. Este enfoque holístico surge en respuesta a la sofisticación progresiva de los ataques cibernéticos y a la exigencia de que los líderes militares estén capacitados para dirigir la defensa en este emergente escenario bélico.

Recordad que el objetivo principal del Laboratorio de Concienciación en Ciberseguridad es formar a altos cargos y oficiales militares en la identificación, prevención y reacción ante ciberataques orientados hacia ellos, tales como phishing, spear-phishing y whaling. Estas amenazas están concebidas para aprovechar su posición de liderazgo y acceso a información vital, por lo que es crucial potenciar su

habilidad para identificar y minimizar estos riesgos. El laboratorio se enfoca en brindar competencias estratégicas y prácticas, que les faciliten salvaguardar tanto sus datos personales como los sistemas delicados bajo su responsabilidad.

3.3.2 Elementos de la Prueba de Laboratorio

El laboratorio se organiza en módulos sofisticados que fusionan simulaciones dinámicas, capacitación teórica y ejercicios en ambientes regulados, se necesitará un aula con equipo informático y red con acceso a internet, es muy recomendable que los equipos tengan una capacidad suficiente de RAM y procesador que permita el funcionamiento de máquinas virtuales.

A continuación, se muestran los elementos clave:

3.3.3 Simulaciones de Ataques Expuestos en Situaciones Reales

Escenarios a medida: Las simulaciones están concebidas para replicar sucesos reales que podrían involucrar puestos militares de alto nivel, incluyendo correos malintencionados dirigidos y falsificación de identidad de aliados estratégicos.

Ataques en conjunto: Incluir varios vectores de ataque, como la utilización conjunta de phishing y llamadas de ingeniería social para impulsar decisiones rápidas.

Esta parte está orientada a concienciar y es más una exposición de situaciones para que las propias autoridades reflexionen sobre las vulnerabilidades de forma muy general, comenzando a relacionarse con el vocabulario técnico propio de la ciberseguridad.

3.3.4 Búsqueda de exposición digital

La exploración del fingerprinting y footprinting digital, incluso para individuos con escasa actividad en las redes sociales, constituye una práctica reveladora que puede proporcionar una perspectiva más precisa de nuestra presencia en el ámbito digital. A pesar de que numerosos individuos sostienen que una interacción reducida en plataformas sociales conlleva una huella digital restringida, en realidad, la simple presencia de datos tales como nombres, alias, correos electrónicos o interacciones esporádicas en internet puede ser suficiente para elaborar un mapa detallado de nuestra actividad en línea. Este análisis se inicia comprendiendo que el footprinting, también conocido como huella digital, se refiere a la totalidad de información pública que dejamos en internet, ya sea de forma intencionada o involuntaria. Por otro lado, el fingerprinting se refiere a las características únicas que nos identifican técnicamente, tales como configuraciones de navegador, direcciones IP y otras características digitales que podemos no estar conscientes de haber expuesto.

Para rastrear nuestra huella digital, es esencial efectuar una recolección inicial de los datos que seamos conscientes de haber difundido en el entorno digital. Un nombre completo, un alias empleado en alguna plataforma, una dirección de correo electrónico o un número telefónico son suficientes para iniciar el proceso de búsqueda. Frecuentemente menospreciamos el número de sitios en los que hemos dejado huellas; sin embargo, incluso los comentarios en blogs o foros antiguos pueden permanecer accesibles si no han sido eliminados manualmente. La primera etapa consiste en emplear motores de búsqueda como Google para llevar a cabo una búsqueda fundamental. La introducción completa de nuestro nombre, tal como "Juan Pérez", puede desvelar referencias precisas en páginas web, documentos o incluso publicaciones en plataformas de redes sociales. Si el nombre es frecuentemente utilizado, la

inclusión de términos adicionales como la ciudad en la que residimos o nuestra ocupación profesional puede contribuir al filtrado de los resultados. Por ejemplo, el término "Juan Pérez Marin ingeniero informático" presenta una mayor especificidad y puede resultar en resultados de mayor relevancia. Es igualmente beneficioso llevar a cabo esta búsqueda en motores de búsqueda alternativos como DuckDuckGo o Bing, dado que poseen algoritmos distintos y pueden exhibir información que Google no indexa. Específicamente, DuckDuckGo no ajusta los resultados en función del historial de búsqueda, lo que podría resultar ventajoso para la localización de datos más objetivos.

Además de estas búsquedas iniciales, existen herramientas especializadas que pueden resultar de gran utilidad, particularmente si nuestra presencia en redes sociales es limitada y hemos empleado internet para inscribirse en servicios o participar en foros. Una de las herramientas propuestas es Have I Been Pwned [29], que posibilita la verificación de si nuestras direcciones de correo electrónico han estado implicadas en actos de filtración de datos. Por ejemplo, si introducimos un correo electrónico utilizado para nuestro registro en un foro hace años, podríamos detectar que dicha cuenta se encuentra en una brecha de seguridad. Esta situación no solo nos alerta acerca de un posible compromiso de dicha entidad, sino que también puede señalar qué tipo de servicios hemos empleado. Esta categoría de instrumento puede funcionar como un punto de partida para el seguimiento de nuestras actividades, incluso en sitios que ya no evocan memoria.

Un método valioso es indagar en las plataformas de redes sociales en las que podríamos haber establecido un perfil, aunque su uso haya sido insuficiente o incluso olvidado. Numerosos individuos establecen cuentas en plataformas digitales como Facebook, LinkedIn o Twitter por razones particulares, tales como la búsqueda de empleo o la interacción con familiares, pero no las emplean de manera habitual. No obstante, la información fundamental de estos perfiles puede ser accesible para cualquier individuo, en función de las configuraciones de privacidad establecidas. La realización de una indagación de nuestro nombre en dichas plataformas puede desvelar perfiles, publicaciones o incluso imágenes etiquetadas que no recordamos haber difundido previamente. Adicionalmente, herramientas como TinEye [32] o Google Reverse Image Search [33] pueden resultar beneficiosas si hemos capturado imágenes personales en algún momento. Estas herramientas posibilitan la ejecución de una búsqueda inversa de imágenes con el objetivo de identificar posibles ubicaciones en las que nuestras fotografías podrían haber sido empleadas, un recurso particularmente valioso para identificar perfiles duplicados o aplicaciones no autorizadas de nuestras imágenes.

El estudio del footprinting no se circunscribe únicamente a las plataformas de redes sociales. Las comunidades virtuales y los foros constituyen una fuente significativa de información. A pesar de que ciertos individuos no exhiben una participación activa en las redes sociales, pueden haber interactuado en foros especializados, dejado comentarios en blogs o participado en comunidades de debate. La identificación de nombres de usuario o alias utilizados en estos contextos puede resultar en hallazgos sorprendentes. Por ejemplo, si hemos empleado un alias como "TechFan1980" en un foro tecnológico, es posible que dicha identidad esté vinculada con otras plataformas. Instrumentos como Namechk [34] facilitan la búsqueda de un nombre de usuario en diversas páginas web y servicios para identificar su ubicación registrada. Esta metodología puede facilitar la cartografía de nuestra actividad, incluso si consideramos que hemos actuado con prudencia al no emplear nuestro nombre real.

Una fuente significativa para el footprinting son los registros públicos y las bases de datos. A pesar de la ausencia de plataformas de redes sociales, nuestra información podría ser localizada en directorios telefónicos, registros de propiedad o bases de datos ocupacionales. En el contexto de la audiencia objetivo, por ejemplo, los boletines oficiales de defensa frecuentemente divulgan información relativa a convocatorias, premios o menciones administrativas que incorporan nombres completos. La ejecución de indagaciones con nuestro nombre en dichas fuentes puede desvelar información que desconocíamos que se encontraba accesible públicamente. Adicionalmente, servicios como Internet Archive, también

conocido como Wayback Machine [35], facilitan el rastreo de versiones anteriores de páginas web, lo cual puede resultar beneficioso para identificar información que ha sido suprimida del sitio original pero que continúa almacenada en este archivo digital.

A pesar de la relevancia de la huella digital perceptible, no debemos desatender el fingerprinting técnico, que tiene la capacidad de identificarnos incluso sin poseer perfiles digitales. Nuestro navegador, nuestras preferencias lingüísticas, las extensiones instaladas y la resolución de pantalla constituyen algunos de los datos que se recopilan de manera automática durante la navegación en línea. Instrumentos como Privacy Badger [36], creado por la Electronic Frontier Foundation, facilitan el análisis de la unicidad de nuestro navegador y la utilización de dicha información para rastrearnos. Esta modalidad de fingerprinting técnico, aunque menos perceptible, mantiene su relevancia, dado que puede asociarnos con actividades en línea a pesar de no proporcionar información personal de manera explícita.

Una vez recopilada la totalidad de esta información, se puede iniciar el análisis de patrones. Por ejemplo, se podría evidenciar que un correo electrónico que consideramos seguro ha sido empleado en una mayor cantidad de servicios de la que se tiene memoria. Esto podría representar una ocasión para implementar acciones correctivas, tales como la modificación de contraseñas o la activación de autenticación de dos factores en las cuentas de mayor sensibilidad. Adicionalmente, si detectamos perfiles en plataformas de redes sociales o foros que ya no se emplean, se aconseja su eliminación o garantizar que estén configurados como privados. Este procedimiento no solo contribuye a la disminución de nuestra exposición, sino que también obstaculiza la recolección de información sobre nosotros sin nuestro consentimiento.

En última instancia, incluso los individuos con una actividad reducida en las redes sociales pueden asombrarse ante la abundancia de información disponible sobre ellas en la red. El procedimiento de rastrear nuestra huella digital constituye un ejercicio valioso para una comprensión más profunda de nuestra exposición y para adquirir habilidades para salvaguardar nuestra privacidad. Mediante el uso de herramientas de fácil acceso, tales como motores de búsqueda, servicios de análisis de datos filtrados y plataformas de búsqueda inversa de imágenes, es posible construir un mapa preciso de nuestra presencia digital. A pesar de que técnicas como el footprinting y el fingerprinting pueden parecer sofisticadas, cualquier individuo con paciencia y curiosidad puede emplearlas para ejercer control sobre su identidad digital.

3.3.5 Capacitación en la Detección de Amenazas

El laboratorio está concebido con el objetivo de instruir a los participantes, particularmente a aquellos con habilidades restringidas en informática, sobre la identificación de correos electrónicos de suplantación de identidad y el análisis de potenciales amenazas mediante el uso de herramientas especializadas. El propósito primordial es inculcarles competencias prácticas que les habiliten para identificar indicadores de advertencia, emplear herramientas tecnológicas y cultivar una postura crítica ante cualquier comunicación digital de naturaleza sospechosa.

Uno de los componentes fundamentales del laboratorio consiste en adquirir habilidades para reconocer las señales de alerta presentes en los correos electrónicos. Inicialmente, se instruye a los participantes en la evaluación del remitente. Con frecuencia, los ciberdelincuentes procuran replicar direcciones auténticas con el objetivo de ganar la confianza de la víctima. Sin embargo, suelen introducir ligeras modificaciones en las direcciones de correo electrónico. Por ejemplo, un correo electrónico que aparenta ser de `atencionalcliente@banco.com` podría, en realidad, ser emitido desde `atencionalcliente@banco-seguro.com` o incluso desde un dominio completamente distinto, tal como `soporte@banc0.com` (en el que la "o" se sustituye por un "0"). Durante esta etapa, los participantes son sometidos a una serie de

ejemplos prácticos para identificar dichas discrepancias, adquiriendo habilidades para prestar atención a los detalles mínimos que podrían permanecer inadvertidos.

Tras el análisis del emisor, se procede a examinar el contenido del correo electrónico. Los mensajes de suplantación de identidad suelen incorporar líneas de asunto alarmantes, tales como "Problema urgente con su cuenta" o "Última oportunidad para evitar el bloqueo de su tarjeta". Estos mensajes están concebidos con el objetivo de inducir una sensación de urgencia que induce a los individuos a tomar medidas inmediatamente. Se instruye a los participantes en la evaluación de estas líneas de asunto, solicitando que examinen correos electrónicos representativos para identificar patrones sospechosos.

El contenido del mensaje constituye otro aspecto de relevancia significativa. Frecuentemente, los correos electrónicos de suplantación de identidad presentan errores gramaticales o un tono poco profesional que no se alinea con los estándares de una organización legítima. Adicionalmente, estos frecuentemente incorporan saludos genéricos como "Estimado cliente" en lugar de un nombre personalizado. En el entorno de laboratorio, se suministran ejemplos comparativos de correos auténticos y correos falsificados para facilitar la diferenciación entre ambos. Además, se aborda cómo las entidades corporativas legítimas raramente requieren información delicada, tales como contraseñas o información financiera, mediante correos electrónicos.

El examen de los enlaces y archivos adjuntos constituye un componente crucial del laboratorio, y en este contexto se introduce la utilización de Virus Total [37] como un instrumento indispensable. Virus Total es una plataforma digital que facilita el análisis de archivos y URLs sospechosos en la búsqueda de software malicioso y otras amenazas cibernéticas. Se instruye a los participantes que, previo a seleccionar cualquier enlace presente en un correo electrónico, deben desplazar el cursor sobre él para visualizar la URL completa. En caso de que la dirección URL no se alinee con el sitio oficial o parezca sospechosa, como la inclusión de caracteres foráneos o dominios desconocidos, es imperativo actuar con prudencia.

Durante el ejercicio práctico, los participantes adquieren la habilidad de copiar los enlaces sospechosos y a pegarlos en la interfaz de análisis de URLs de Virus Total. Se proporciona una guía detallada para la utilización de esta herramienta: inicialmente, deben acceder al sitio web de Virus Total en su navegador. Posteriormente, optan por la opción "URL" en el menú principal, introducen el enlace sospechoso en el cuadro de texto y seleccionan "Analizar". Virus Total realiza un escaneo de la URL empleando diversos motores de detección de software malicioso y bases de datos de sitios de suplantación de identidad. Los hallazgos se exponen en una tabla explícita que señala si alguno de los motores de búsqueda ha clasificado el enlace como malintencionado. Si se manifiesta en rojo, indica la posibilidad de un riesgo asociado al enlace, y se instruye a los participantes a evitar interactuar con él.

Los participantes adquieren habilidades para analizar archivos adjuntos sospechosos. Si un correo electrónico contiene un archivo que suscita interrogantes, tal como un archivo.zip,.pdf o.exe, se proporciona una guía para subir el archivo a Virus Total para su análisis. Se subraya que nunca deben abrir un archivo sospechoso en su sistema informático antes de proceder a su verificación. En el ejercicio práctico, se suministra un archivo de ejemplo para su subida a Virus Total, y se orienta en la interpretación de los resultados obtenidos. Los participantes adquieren habilidades para identificar qué motores de búsqueda han identificado amenazas y qué categorías de software malicioso podrían estar presentes. Esto contribuye al desarrollo de un entendimiento más profundo de los riesgos vinculados a los archivos adjuntos en correos electrónicos.

Además de la implementación de Virus Total, se incorpora PhishTank [38], una base de datos colaborativa en la que los participantes tienen la capacidad de verificar si un enlace sospechoso ya ha sido reportado como táctica de phishing. Esta herramienta se vuelve especialmente valiosa cuando los

hallazgos de VirusTotal no son definitivos. Los participantes introducen enlaces en PhishTank y adquieren habilidades para interpretar los resultados con el objetivo de corroborar si el enlace ha sido previamente identificado como malintencionado.

A lo largo del proceso de laboratorio, se subraya la relevancia de emplear múltiples capas de protección. Los navegadores contemporáneos, tales como Google Chrome y Mozilla Firefox, incorporan filtros de seguridad que emiten alertas al intentar acceder a sitios identificados por actividades de suplantación de identidad. Se instruye a los participantes en el funcionamiento de estas advertencias y en su configuración para garantizar su activación constante. Además, se procede a la instalación y prueba de la extensión Netcraft Anti-Phishing, la cual realiza un análisis automático de las páginas web visitadas y proporciona alertas en caso de identificar actividades sospechosas.

Con el objetivo de finalizar la experiencia práctica, los participantes llevan a cabo simulaciones de correos electrónicos sospechosos en un ambiente seguro proporcionado por el laboratorio. En estas simulaciones, es imperativo implementar los conocimientos adquiridos para identificar indicadores de suplantación de identidad, examinar enlaces y archivos mediante VirusTotal, y corroborar la legitimidad de los correos electrónicos mediante PhishTank y otras herramientas. Adicionalmente, se aborda la relevancia de establecer comunicación directa con las empresas identificadas en los correos electrónicos sospechosos para corroborar su autenticidad. Se les instruye en la búsqueda de los datos de contacto oficiales en las páginas web de las organizaciones y en la formulación de consultas claras y exactas.

En última instancia, se fortalecen las estrategias preventivas que los participantes pueden implementar para reducir su susceptibilidad a correos de suplantación de identidad. Se proporciona una explicación detallada sobre cómo mantener sus sistemas en constante actualización, activar la autenticación de dos factores en sus cuentas y generar contraseñas seguras y singulares para cada servicio. Además, se les incentiva a divulgar los conocimientos adquiridos entre colegas y familiares, contribuyendo así a la formación de una cultura de seguridad digital en su contexto.

Este laboratorio no solo capacita a los participantes con las competencias técnicas requeridas para la identificación de correos de phishing, sino que también promueve una mentalidad crítica y proactiva en relación con la seguridad en la red. Con la adquisición de conocimientos y la práctica en herramientas como VirusTotal y PhishTank, los participantes estarán más capacitados para resguardarse de amenazas digitales y tomar decisiones fundamentadas al interactuar con correos electrónicos sospechosos.

3.3.6 4. Manejo de Credenciales y Accesos Importantes

La gestión segura de credenciales y accesos es una labor esencial para cualquier individuo que tenga acceso a información delicada o confidencial, particularmente para aquellos que desempeñan roles de responsabilidad en entidades públicas o privadas. Frecuentemente, las contraseñas constituyen la primera barrera frente a intrusiones no autorizadas; sin embargo, si no se administran adecuadamente, pueden transformarse en una vulnerabilidad significativa. Este laboratorio está concebido para instruir a los participantes, sin importar su nivel de habilidades técnicas, sobre cómo salvaguardar sus credenciales de manera eficaz a través de la generación de contraseñas sólidas, la utilización de instrumentos contemporáneos para su gestión y la aplicación de protocolos avanzados como la autenticación multifactor. Mediante este procedimiento, se garantizará que cada participante pueda implementar los conocimientos adquiridos en su cotidianidad, tanto en el contexto personal como profesional.

El laboratorio inicia exponiendo el concepto de credenciales digitales y su relevancia esencial. Las credenciales están fundamentalmente compuestas por un nombre de usuario y una contraseña, aunque en numerosos casos pueden incorporar elementos adicionales como códigos de autenticación o certificados digitales. En un contexto digital cada vez más interconectado, donde los ciberdelincuentes

emplean técnicas sofisticadas para infiltrarse en sistemas y datos delicados, resulta esencial comprender que una contraseña insuficiente puede comprometer no solo una cuenta individual, sino también sistemas completos. Además, se subraya que una de las actividades más habituales y peligrosas es la reutilización de contraseñas en diversos servicios, lo cual propicia el acceso no autorizado en caso de que una de ellas sea comprometida.

La actividad inicial en el laboratorio se enfoca en la generación de contraseñas de alta seguridad. Se expone que una contraseña sólida debe constar de al menos doce caracteres, abarcando una combinación de letras mayúsculas y minúsculas, números y símbolos, evitando patrones de identificación fácil como nombres, fechas de nacimiento o palabras frecuentemente utilizadas. No obstante, también se admite que la memorización de contraseñas complejas para diversos servicios puede representar un desafío considerable. Para tratar esta problemática, los participantes adquirirán habilidades para desarrollar un diccionario personalizado de contraseñas, un procedimiento que facilita la creación de combinaciones únicas y seguras, ajustadas a sus requerimientos particulares.

El procedimiento se inicia con la elección de términos clave de relevancia para cada participante. Estas palabras deben ser personales, pero no obvias ni accesibles públicamente, tales como el nombre de un lugar de preferencia, una obra literaria o cinematográfica preferida, o un término asociado con una experiencia personal significativa. Por ejemplo, un individuo podría seleccionar los términos "Montaña", "Café" y "Estrella". Tras su selección, se les instruye en la transformación de estas palabras en variantes más seguras a través de la sustitución de letras por números y símbolos, una técnica denominada lenguaje leet. Por lo tanto, "Montaña" podría ser redefinida como "M0nt@ñ@" y "Café" como "C@f3!". Este procedimiento no solo aumenta la seguridad de las contraseñas, sino que también complica su descifrado.

Tras la generación de estas variantes, los participantes adquirirán habilidades para fusionarlas con el objetivo de producir contraseñas más extensas y singulares. Mediante la utilización de un editor de texto como Notepad, se solicita que redacten combinaciones de dos o tres palabras clave separadas por símbolos distintivos. Como ilustración, "M0nt@ñ@_C@f3!" o "Estrella-M0nt@ñ@". Se propone la implementación de herramientas como Crunch [39], que facilita la creación de listas completas de contraseñas basadas en parámetros personalizados, o scripts sencillos en Python para automatizar este proceso. A pesar de que estas herramientas demandan un nivel elemental de interacción con la tecnología, los instructores detallan minuciosamente cada etapa, garantizando que todos los participantes puedan emplearlas con confianza.

Una vez que las contraseñas han sido generadas, la siguiente etapa consiste en su evaluación para garantizar su seguridad efectiva. En este contexto, se introduce la utilización de instrumentos como Have I Been Pwned y Password Meter [40]. Have I Been Pwned facilita a los participantes la verificación de si una contraseña particular ha sido comprometida en alguna brecha de seguridad identificada. Se expone que las contraseñas expuestas en bases de datos públicas presentan una vulnerabilidad significativa, a pesar de su apariencia de robustez. Alternativamente, Password Meter mide la robustez de una contraseña en función de su complejidad, longitud y diversidad de caracteres, ofreciendo recomendaciones para su optimización. Los participantes realizan pruebas de las contraseñas generadas durante la sesión en dichas herramientas, comprendiendo cómo modificaciones mínimas pueden tener un impacto significativo en la seguridad.

A continuación, el laboratorio se centra en el almacenamiento y gestión segura de contraseñas mediante la utilización de gestores de contraseñas. Estos instrumentos no solamente almacenan credenciales de manera encriptación, sino que también facilitan la generación de contraseñas únicas para cada cuenta. Se exponen alternativas como Bitwarden [41], LastPass [42], 1Password [43] y KeePass [44], subrayando sus atributos fundamentales y beneficios. Por ejemplo, Bitwarden se caracteriza por ser gratuito, de código abierto y su compatibilidad con múltiples dispositivos, factores que lo posicionan

como una opción sobresaliente para usuarios de nivel inicial y avanzado. A lo largo del periodo de práctica, los participantes instalan Bitwarden y establecen una cuenta principal con una contraseña de alta seguridad. Es importante destacar que esta contraseña maestra constituye la clave de acceso a todas las demás credenciales, por lo que debe ser singular y sólida.

Los participantes ejercitan su habilidad introduciendo manualmente credenciales en su administrador de contraseñas, generando nuevas contraseñas para servicios ya existentes y agrupándolas por categorías para optimizar su acceso. Además, se les instruye en la sincronización del gestor entre diversos dispositivos, tales como ordenadores y dispositivos móviles, garantizando que sus credenciales estén accesibles en todo momento sin poner en riesgo la integridad de la información.

Para consolidar la salvaguarda, el laboratorio implementa la autenticación multifactor (MFA), una estrategia que añade un nivel adicional de seguridad al exigir un segundo factor de autenticación, tal como un código temporal generado por una aplicación o transmitido por mensajes de texto. Los participantes configuran una medida de autenticación (MFA) en una cuenta personal mediante el uso de herramientas como Authy [45], adquiriendo habilidades para incorporar esta medida en sus rutinas cotidianas para optimizar la protección de sus cuentas.

En última instancia, el laboratorio culmina con una representación de intentos de acceso no autorizado. Se exhiben ejemplos de cómo los perpetradores emplean estrategias como ataques de fuerza bruta y ataques de diccionarios para descifrar contraseñas débiles, y se realiza una comparación entre los tiempos estimados de descifrado de contraseñas simples y robustas. Esto subraya la relevancia de implementar los conocimientos adquiridos para salvaguardar información delicada. Adicionalmente, se sintetizan buenas prácticas en la gestión de credenciales, tales como la abstención de la reutilización de contraseñas, la actualización periódica de las mismas y la utilización constante de gestores y autenticación multifactor.

Este laboratorio ofrece a los participantes las herramientas y conocimientos requeridos para administrar sus credenciales de manera segura y confiable, garantizando que puedan salvaguardar tanto su información personal como los sistemas a los que tienen acceso. La integración de teoría aplicada y la aplicación de herramientas contemporáneas asegura que los participantes estén mejor equipados para enfrentar los retos inherentes al actual contexto digital.

3.3.7 Acceso a redes y destinos inseguros.

La gestión de comunicaciones seguras resulta esencial para las autoridades militares, particularmente aquellas con acceso a información de carácter clasificado o que operan en contextos operativos de alta sensibilidad. Los ataques de tipo Man-in-the-Middle (MitM) constituyen una de las amenazas de mayor relevancia, dado que posibilitan a los atacantes la interceptación y, potencialmente, la alteración de comunicaciones cruciales sin que las partes involucradas lo detecten. El propósito de este laboratorio es no solo elucidar la definición de un ataque MitM, sino también impartir medidas prácticas y herramientas tangibles para su prevención. Se fundamenta en un escenario simulado en el que las autoridades involucradas deben establecer comunicación segura desde emplazamientos distantes, empleando redes potencialmente inseguras.

El laboratorio inicia exponiendo de manera explícita la definición de un ataque MitM. Fundamentalmente, se refiere a una circunstancia en la que un atacante se sitúa entre el emisor y el receptor de una comunicación, interceptando y, en determinadas circunstancias, manipulando los datos transmitidos. Este fenómeno puede manifestarse a través de estrategias como el envenenamiento de la tabla ARP, la configuración de puntos de acceso Wi-Fi falsos o la interceptación de tráfico en redes desprovistas. Se subraya la peligrosidad de los ataques MitM en redes Wi-Fi públicas o en redes privadas

mal configuradas, lo que convierte a estas redes en el principal blanco de las simulaciones de laboratorio.

Para ilustrar de manera más concreta el concepto, se propone un escenario práctico: una autoridad militar que requiere establecer una conexión con su correo institucional desde un hotel durante una misión internacional. En el presente escenario, el establecimiento hotelero proporciona una red Wi-Fi sin costo; sin embargo, dicha red podría haber sido comprometida por un ataque cibernético que intercepta todas las comunicaciones efectuadas a través de ella. Los participantes asumen la función de dicha autoridad y se esfuerzan en identificar las amenazas existentes e implementar contramedidas correspondientes.

La actividad práctica inicial se enfoca en ilustrar cómo un atacante puede interceptar comunicaciones en una red no segura. Se emplea un software específico como Wireshark [46], un analizador de tráfico de red, para simular un ataque controlado. En esta actividad experimental, se establece una red Wi-Fi abierta en el laboratorio, y los participantes conectan un dispositivo de prueba a dicha red. A medida que los participantes navegan por sitios web simulados, los instructores registran el tráfico mediante Wireshark y demuestran cómo la información transmitida en texto plano, tales como nombres de usuario, contraseñas o correos electrónicos, puede ser fácilmente accesible para un atacante. Esta evidencia subraya la relevancia de salvaguardar las comunicaciones, particularmente cuando se emplea una red con potenciales amenazas.

La etapa subsecuente consiste en implementar el protocolo de encriptación HTTPS como una medida fundamental de protección. Los participantes adquieren habilidades para discernir si una página web emplea encriptación HTTPS mediante la observación del candado en la barra de direcciones del navegador y la verificación del certificado del sitio web. Se explica que HTTPS encapsula los datos transmitidos entre el navegador y el servidor, obstaculizando la posibilidad de que un atacante pueda acceder a ellos, incluso si consigue interceptarlos. Con el objetivo de consolidar este concepto, los participantes realizan visitas a versiones seguras y no seguras de la misma página web, examinando cómo Wireshark presenta el tráfico cifrado como caracteres incomprensibles en el contexto de HTTPS, en contraposición a los datos legibles provenientes de una página HTTP no segura.

Se procede a introducir el concepto de redes privadas virtuales (VPN) como una estrategia avanzada para la prevención de ataques MitM. Se expone que una Red Privada Virtual (VPN) configura un túnel cifrado entre el dispositivo del usuario y un servidor ubicado en un lugar remoto, garantizando la protección de todo el tráfico que circula a través de la red. Esta medida no solo garantiza la inaccesibilidad de los datos, sino que también oculta la dirección IP del usuario, obstaculizando la identificación del origen de la comunicación. Los participantes proceden a la instalación y configuración de una VPN comercial sugerida, tales como NordVPN [47] o ProtonVPN [48], siguiendo un proceso detallado proporcionado por los instructores.

En el transcurso de la práctica, los participantes se conectan a la red Wi-Fi insegura previamente configurada, pero en esta ocasión mediante la VPN. Los instructores ilustran cómo, incluso ante el intento de captura del tráfico por parte de un atacante, los datos se manifiestan en cifrado y no pueden ser leídos. Además, se les instruye en la selección de servidores VPN apropiados, dando prioridad a aquellos situados en naciones con normativas rigurosas sobre privacidad o próximos a su ubicación para reducir la latencia. Adicionalmente, se aborda la relevancia de elegir proveedores de servicios de VPN fiables que no registren el historial de navegación ni almacenen información personal, un aspecto particularmente pertinente para actividades militares.

Una herramienta adicional exhibida en el laboratorio es ARP Guard [49], un software que supervisa en tiempo real el estado de la red y percibe intentos de envenenamiento de la tabla ARP, una estrategia habitual en ataques MitM. Los participantes instalan ARP Guard en dispositivos de prueba y examinan la manera en que el software emite alertas cuando identifica actividad sospechosa en la red. Además,

adquieren habilidades para interpretar dichas alertas y adoptar acciones inmediatas, tales como la desconexión de la red o la activación de la VPN.

Además de la implementación de herramientas, se subraya la relevancia de establecer redes seguras en contextos operativos. Los participantes ejercitan el establecimiento de una red Wi-Fi protegida mediante el cifrado WPA3, empleando contraseñas sólidas y desactivando funcionalidades como la difusión del SSID. Además, se les instruye en la verificación manual de los certificados digitales de las páginas web para garantizar que no han sido manipulados por un agente malintencionado. En el presente contexto, se exponen ejemplos de certificados auténticos y certificados dudosos, proporcionando instrucciones para identificar discrepancias tales como errores en los nombres de dominio o la falta de una autoridad certificadora de confianza.

El laboratorio culmina con una actividad de integración en la que los participantes implementan todas las medidas adquiridas en un contexto simulado. En el presente ejercicio, se requiere establecer una conexión segura a un sistema institucional desde una localización distancia, empleando instrumentos como la VPN, ARP Guard y verificaciones manuales de seguridad. Además, es imperativo reaccionar ante alertas simuladas, identificando y mitigando potenciales intentos de ataque MitM en tiempo real. Esta metodología pragmática garantiza que los participantes posean un entendimiento no solo de las herramientas, sino también de su incorporación en su rutina cotidiana para salvaguardar las comunicaciones.

Finalmente, se proporcionan a los participantes una serie de recomendaciones fundamentales: abstenerse de utilizar redes Wi-Fi públicas sin medidas de protección, dar prioridad a la utilización de VPN para comunicaciones delicadas, verificar manualmente los certificados de sitios web críticos y mantener una vigilancia activa frente a comportamientos sospechosos en la red. Además, se incentiva la divulgación de los conocimientos adquiridos entre sus equipos, promoviendo una cultura de seguridad que reduzca los riesgos vinculados a los ataques MitM y robustezca las comunicaciones en situaciones críticas. Mediante la implementación de estas herramientas y prácticas, incluso las autoridades con conocimientos técnicos restringidos estarán mejor equipadas para resguardarse frente a esta amenaza en contextos operativos delicados.

4 CONCLUSIONES Y LÍNEAS FUTURAS

4.1 Conclusiones.

Este Trabajo Fin de Máster (TFM) examina el desafío de la sensibilización en ciberseguridad para las autoridades militares y gubernamentales que operan en contextos donde la transición digital se encuentra en su apogeo. La realidad que los técnicos de CIS tenemos la evidencia que, pese a los progresos notables en la puesta en práctica de estrategias técnicas y pedagógicas de concienciación, aún subsisten áreas críticas que demandan una mayor atención para consolidar una cultura robusta de ciberseguridad.

Con respecto a los objetivos propuestos al comienzo del Trabajo Fin de Master, se puede postular lo siguiente:

La meta de identificar los riesgos en el área ciber predominantes que amenazan a las autoridades militares ha sido alcanzada de manera satisfactoria. Casos representativos conocidos y los incidentes de suplantación de identidad analizados han proporcionado un marco práctico que evidencia la necesidad imperante de reforzar las habilidades de detección y prevención. La ausencia de estrategias proactivas, tales como la segmentación eficiente de la necesidad de conocer y sus recursos de acceso a los datos, la red o los sistemas de información junto a la administración avanzada de accesos, se ha manifestado como un vector de ataque relativamente frecuente en los ataques conocidos examinados.

El test de competencia en ciberseguridad aplicado a las autoridades militares permite evaluar el grado actual de sensibilización. Este propósito también se logra, poniendo de manifiesto discrepancias notables en la interpretación de conceptos tan fundamentales como el principio de mínimo privilegio y las prácticas óptimas en la administración de contraseña. Incluso con una muestra controlada de alumnos, con altos conocimientos técnicos, se enfatiza la necesidad de fortalecer la capacitación en campos específicos.

El desarrollo de talleres de concientización y la propuesta de uno tipo laboratorio de ciberseguridad militar fueron concebidos como una propuesta factibles y aplicables. Estas iniciativas no solo se orientan hacia la provisión de herramientas pedagógicas, sino que también buscan potenciar la resiliencia ante amenazas emergentes a través de la simulación de situaciones reales, pretendiendo no ser algo aburrido para las autoridades y concienciando mediante la práctica de la sencillez de algunos ataques, y de cómo unas mínimas medidas de autoprotección dificultan de forma exponencial la explotación de ciertos vectores de ataque, sobre todo aquellos que necesitan de la colaboración de alguien que ya esté dentro de la organización.

Para concluir, el TFM evidencia que la concienciación en ciberseguridad para las autoridades analógicas constituye un elemento crucial para asegurar la seguridad nacional en el actual escenario tecnológico. Los objetivos propuestos para este trabajo se alcanzaron en gran medida, aunque persiste la necesidad de perfeccionar determinados aspectos vinculados con la formación básica en todos los niveles, especialmente en los más altos donde la brecha tecnológica fruto de la edad de las autoridades obliga a tener un enfoque pedagógico adaptado los intereses de las autoridades para mantener la atención en las herramientas mostradas, que aunque han sido elegidas unas de fácil acceso y sencillez, pueden no estar desarrolladas para un entorno de conocimientos muy bajos, aun así la mera asistencia al taller, aunque no se completen todos los objetivos de este, aumentara la autoprotección de las autoridades o como mínimo genera preocupación en lo relacionado con su vulnerabilidad ante un ataque dirigido contra ellos mismos.

4.2 Líneas futuras dirigidas

A partir de los hallazgos obtenidos y las áreas de mejora identificadas, se proponen las siguientes directrices futuras para proseguir con la labor desarrollada en este Trabajo Fin de Máster:

Ampliar la extensión y continuar actualizando con las nuevas amenazas el examen de competencias: El objetivo es diseñar e implementar evaluaciones más rigurosas que no solo engloben conceptos teóricos, sino también ejercicios prácticos. Esta metodología facilitará la evaluación de la habilidad de los participantes para responder a incidentes en tiempo real y la adaptación de los programas educativos en función de los resultados obtenidos.

Elaborar laboratorios de simulación de alto nivel: Se diseñarán laboratorios especializados en ciberseguridad para las fuerzas armadas y las autoridades gubernamentales. Estos laboratorios podrían incorporar la realización de simulaciones de ataques dirigidos a infraestructuras esenciales y contextos de control y mando, fomentando la experiencia práctica bajo condiciones controladas.

Fomentar la constante actualización del programa de concienciación: Implementar un sistema dinámico para la actualización de los contenidos educativos en respuesta a las emergentes amenazas y tendencias en el campo de la ciberseguridad. Esto podría implicar la integración de tecnologías en desarrollo, tales como la inteligencia artificial y el análisis predictivo, con el objetivo de prever riesgos potenciales.

Evaluar la repercusión de las iniciativas implementadas: Elaborar investigaciones de carácter transversal que cuantifiquen el impacto de las formación y los talleres sugeridos. Esto facilitará la adaptación de las estrategias y asegurará que los objetivos de sensibilización se materialicen en transformaciones concretas en la cultura organizativa.

Extender la capacitación a sectores civiles vinculados: La implementación de programas de capacitación y concientización debería extenderse a actores externos que interactúan con las fuerzas armadas, tales como miembros de ISDEFE y proveedores, garantizando así una protección holística de la cadena de apoyo y suministro.

Estas propuestas tienen como objetivo no solo consolidar los resultados obtenidos en este Trabajo de Fin de Master, sino también asegurar una evolución continua en la capacitación cibernética de las autoridades analógicas, adaptándose a los desafíos inherentes a un entorno digital en perpetua y rápida transformación.

5 BIBLIOGRAFÍA

- [1] Instituto Nacional de Ciberseguridad (INCIBE), “Guía de buenas prácticas en ciberseguridad,” INCIBE, 2023.
- [2] Centro Criptológico Nacional, “Ciberseguridad en administraciones públicas,” Gobierno de España, 2022.
- [3] Europol, *FACC case study: A targeted whaling attack*, 2016. [Online]. Disponible: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf. Recuperado el 20 de enero de 2025.
- [4] TechCrunch, “Snapchat employee data leaks out following phishing attack,” *TechCrunch*, 29 de febrero de 2016. [Online]. Disponible: <https://techcrunch.com/2016/02/29/snapchat-employee-data-leaks-out-following-phishing-attack/>. Recuperado el 20 de enero de 2025.
- [5] Phineas Fisher, *Milica Leaks: Revelaciones*, 2019.
- [6] El Economista, “¿Qué es Guacamaya, el grupo que hackeó a la Sedena?,” *El Economista*, 30 de septiembre de 2022. [Online]. Disponible: <https://www.eleconomista.com.mx/tecnologia/Que-es-Guacamaya-el-grupo-que-hackeo-a-la-Sedena-20220930-0064.html>. Recuperado el 20 de enero de 2025.
- [7] Financial Times, “Synthetic voice scams in the corporate sector,” *Financial Times*, 2020. [Online]. Disponible: <https://www.ft.com/content/308c42af-2bf8-47e4-a360-517d5391b0b0>. Recuperado el 20 de enero de 2025.
- [8] Symantec Corporation, *Annual Threat Report*, 2023.
- [9] J. García, “Cero confianza en la ciberseguridad moderna,” *Editorial Seguridad Digital*, 2021.
- [10] Instituto Nacional de Ciberseguridad (INCIBE), “Guía para la gestión de amenazas cibernéticas,” INCIBE, 2023.
- [11] Microsoft Corporation, *Be Cyber Smart Kit*. [Online]. Disponible: <https://info.microsoft.com/ww-landing-be-cybersmart-toolkit.html?LCID=es>. Recuperado el 20 de enero de 2025.
- [12] BM, “Ciberseguridad - IBM SkillsBuild.” [Online]. Disponible: <https://skillsbuild.org/es/adult-learners/explore-learning/cybersecurity-analyst>. Recuperado el 20 de enero de 2025.
- [13] Tecbound Technology, “7 riesgos de phishing: Cómo proteger a tu empresa contra los ciberataques.” [Online]. Disponible: <https://www.tecbound.com/es/7-riesgos-de-phishing/>. Recuperado el 20 de enero de 2025.
- [14] Centro Criptológico Nacional, “Buenas prácticas de ciberseguridad en el ámbito militar,” Gobierno de España, 2022.
- [15] K. Zetter, “Inside the cunning, unprecedented hack of Ukraine’s power grid,” *Wired*, 2016. [Online]. Disponible: <https://www.wired.com/story/inside-cunning-unprecedented-hack-ukraines-power-grid/>. Recuperado el 20 de enero de 2025.

[16] NATO Cooperative Cyber Defence Centre of Excellence, “Locked Shields 2024 demonstrated the real power of cooperative defence,” 2024. [Online]. Disponible: <https://ccdcoe.org/news/2024/locked-shields-2024-demonstrated-the-real-power-of-cooperative-defence/>. Recuperado el 20 de enero de 2025.

[17] Joint Advanced Distributed Learning (JADL), “Comprehensive Cybersecurity Modules for Defense Training,” 2023.

[18] Instituto Nacional de Ciberseguridad (INCIBE), “Informe anual de actividades y estrategias de ciberseguridad,” INCIBE, 2023.

[19] Instituto Nacional de Ciberseguridad, “Kit de concienciación.” [Online]. Disponible: <https://www.incibe.es/empresas/formacion/kit-concienciacion>. Recuperado el 20 de enero de 2025.

[20] E. Nakashima y J. Tate, “Cyber-intruder sparks massive federal response — and debate over dealing with threats,” *The Washington Post*, 8 de diciembre de 2011. [Online]. Disponible: https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-massive-federal-response--and-debate-over-dealing-with-threats/2011/12/06/gIQAxLuFgO_story.html. Recuperado el 20 de enero de 2025.

[21] BBC News Mundo, “Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México,” *BBC News Mundo*, 6 de octubre de 2022. [Online]. Disponible: <https://www.bbc.com/mundo/noticias-america-latina-63167331>. Recuperado el 20 de enero de 2025.

[22] P. Baker, “Cronología del ciberataque a SolarWinds,” *Computerworld*, 23 de junio de 2021. [Online]. Disponible: <https://www.computerworld.es/article/2119675/cronologia-del-ciberataque-a-solarwinds.html>. Recuperado el 20 de enero de 2025.

[23] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown Publishing Group, 2014.

[24] BBC News Mundo, “Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a Estonia,” *BBC News Mundo*, 27 de abril de 2017. [Online]. Disponible: <https://www.bbc.com/mundo/noticias-39800133>. Recuperado el 20 de enero de 2025.

[25] M. Á. Méndez, “El Ministerio de Trabajo sufre un segundo ciberataque con el virus que tumbó el SEPE,” *El Confidencial*, 9 de junio de 2021. [Online]. Disponible: https://www.elconfidencial.com/tecnologia/2021-06-09/ministerio-trabajo-ransomware-ryuk-sepe_3123219/. Recuperado el 20 de enero de 2025.

[26] Kaspersky Lab, “‘Red October’ Diplomatic Cyber Attacks Investigation,” 14 de enero de 2013. [Online]. Disponible: <https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36855/>. Recuperado el 20 de enero de 2025.

[27] BBC News Mundo, “Colonial Pipeline: qué se sabe del ciberataque que llevó al cierre del mayor oleoducto de Estados Unidos,” *BBC News Mundo*, 10 de mayo de 2021. [Online]. Disponible: <https://www.bbc.com/mundo/noticias-internacional-57045133>. Recuperado el 20 de enero de 2025.

[28] BBC News Mundo, “El Parlamento de Noruega sufre un ciberataque y varias cuentas de correo electrónico son hackeadas,” *BBC News Mundo*, 1 de septiembre de 2020. [Online]. Disponible: <https://www.bbc.com/mundo/noticias-internacional-53993589>. Recuperado el 20 de enero de 2025.

- [29] The Guardian, “Revealed: leak uncovers global abuse of cyber-surveillance weapon,” *The Guardian*, 18 de julio de 2021. [Online]. Disponible: <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-pegasus-nso-group>. Recuperado el 20 de enero de 2025.
- [30] La Voz de Galicia, “Estafan más de 9 millones de euros a la farmacéutica Zendal de O Porriño,” 1 de diciembre de 2020. [Online]. Disponible: <https://www.lavozdeg Galicia.es/noticia/galicia/2020/12/01/estafan-9-millones-euros-farmaceutica-zendal-porrino/00031606859793345268851.htm>. Recuperado el 20 de enero de 2025.
- [31] Have I Been Pwned, “Check if your email has been compromised in a data breach.” [Online]. Disponible: <https://haveibeenpwned.com/>. Recuperado el 20 de enero de 2025.
- [32] TinEye, “Reverse image search engine.” [Online]. Disponible: <https://tineye.com/>. Recuperado el 20 de enero de 2025.
- [33] Google Reverse Image Search, “Search by image.” [Online]. Disponible: <https://images.google.com/>. Recuperado el 20 de enero de 2025.
- [34] Namechk, “Check your username across platforms.” [Online]. Disponible: <https://namechk.com/>. Recuperado el 20 de enero de 2025.
- [35] Internet Archive, “Wayback Machine.” [Online]. Disponible: <https://archive.org/web/>. Recuperado el 20 de enero de 2025.
- [36] Electronic Frontier Foundation, “Privacy Badger: Stop tracking with smart blocking.” [Online]. Disponible: <https://www.eff.org/pages/privacy-badger>. Recuperado el 20 de enero de 2025.
- [37] VirusTotal, “Analyze suspicious files and URLs to detect malware.” [Online]. Disponible: <https://www.virustotal.com/>. Recuperado el 20 de enero de 2025.
- [38] PhishTank, “PhishTank: Join the fight against phishing.” [Online]. Disponible: <https://www.phishtank.com/>. Recuperado el 20 de enero de 2025.
- [39] Crunch, “Crunch password generator.” [Online]. Disponible: <https://crunch-wordlist-generator.en.softonic.com/>. Recuperado el 20 de enero de 2025.
- [40] Password Meter, “Test the strength of your passwords.” [Online]. Disponible: <https://www.passwordmeter.com/>. Recuperado el 20 de enero de 2025.
- [41] Bitwarden, “Open source password management solutions.” [Online]. Disponible: <https://bitwarden.com/>. Recuperado el 20 de enero de 2025.
- [42] LastPass, “Password manager for effortless security.” [Online]. Disponible: <https://www.lastpass.com/>. Recuperado el 20 de enero de 2025.
- [43] 1Password, “Password manager built for security.” [Online]. Disponible: <https://1password.com/>. Recuperado el 20 de enero de 2025.
- [44] KeePass, “The Open Source Password Manager.” [Online]. Disponible: <https://keepass.info/>. Recuperado el 20 de enero de 2025.

[45] Authy, “Secure two-factor authentication.” [Online]. Disponible: <https://authy.com/>. Recuperado el 20 de enero de 2025.

[46] Wireshark, “The world's foremost network protocol analyzer.” [Online]. Disponible: <https://www.wireshark.org/>. Recuperado el 20 de enero de 2025.

[47] NordVPN, “Secure and private internet access.” [Online]. Disponible: <https://nordvpn.com/>. Recuperado el 20 de enero de 2025.

[48] ProtonVPN, “Secure VPN for privacy and freedom online.” [Online]. Disponible: <https://protonvpn.com/>. Recuperado el 20 de enero de 2025.

[49] ARP Guard, “Monitor and protect against ARP spoofing.” [Online]. Disponible: <https://arpguard.net/>. Recuperado el 20 de enero de 2025.