COMILLAS
UNIVERSIDAD PONTIFICIA

Facultad de Ciencias Económicas y Empresariales

CIBERSEGURIDAD EMPRESARIAL: Análisis de la efectividad de las políticas de concienciación a la hora de reducir brechas de seguridad en ataques dirigidos

Autor: Claudia Fernández Ventura

Tutor: María José Martín Rodrigo

Clave Académica: 201906424

MADRID | Febrero 2024

Declaración de Uso de Herramientas de Inteligencia Artificial Generativa en Trabajos Fin de Grado

ADVERTENCIA: Desde la Universidad consideramos que ChatGPT u otras herramientas similares son herramientas muy útiles en la vida académica, aunque su uso queda siempre bajo la responsabilidad del alumno, puesto que las respuestas que proporciona pueden no ser veraces. En este sentido, NO está permitido su uso en la elaboración del Trabajo fin de Grado para generar código porque estas herramientas no son fiables en esa tarea. Aunque el código funcione, no hay garantías de que metodológicamente sea correcto, y es altamente probable que no lo sea.

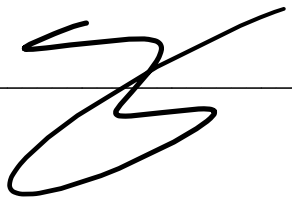
Por la presente, yo, **Claudia Fernández Ventura**, estudiante de **ADE + Business Analytics** de la Universidad Pontificia Comillas al presentar mi Trabajo Fin de Grado titulado "**CIBERSEGURIDAD EMPRESARIAL: Análisis de la efectividad de las políticas de concienciación a la hora de reducir brechas de seguridad en ataques dirigidos**", declaro que he utilizado la herramienta de Inteligencia Artificial Generativa ChatGPT u otras similares de IAG de código sólo en el contexto de las actividades descritas a continuación:

1. **Brainstorming de ideas de investigación:** Utilizado para idear y esbozar posibles áreas de investigación.

Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para que se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.

Fecha: **16/02/2024**

Firma: _____



Resumen

Este trabajo de fin de carrera se centra en la evaluación de la efectividad de las políticas de concienciación en ciberseguridad a la hora de reducir el número de brechas de seguridad que se producen. El conocimiento de las amenazas cibernéticas que pueden acontecer en las organizaciones y como sobrellevarlas, resulta de gran importancia a la hora de evitar consecuencias a gran escala, por ello, es necesario controlar como de actualizados están los empleados. El estudio para conocer el efecto del nivel de capacitación de los empleados comprende un análisis de la bibliografía apoyado de documentos elaborados por organizaciones líderes en la materia y pretende abordar el tema de la ciberseguridad desde el origen de los ataques y sus tipos, hasta cómo evitar las consecuencias de un ataque que pudiera llegar a ser exitoso.

Palabras clave

Ciberseguridad, ciberataque, brecha de seguridad, *malware*, concienciación, medidas de concienciación, políticas de concienciación, ingeniería social, habilidades, cultura en ciberseguridad, *human firewall*, evolución.

Abstract

This thesis focuses on the evaluation of the effectiveness of cybersecurity awareness policies in reducing the number of security breaches that occur. Knowledge of the cyber threats that can occur in organizations and how to deal with them is of great importance in order to avoid large-scale consequences, which is why it is necessary to know how up to date employees are. The study to determine the effect of the level of employee training includes an analysis of the literature supported by documents produced by leading organizations in the field and aims to address the issue of cyber security from the origin of attacks and their types, to how to avoid the consequences of an attack that could be successful.

Keywords

Cybersecurity, cyberattack, security breach, malware, awareness, awareness measures, awareness policies, social engineering, skills, cybersecurity culture, human firewall, evolution.

Índice

PARTE 2 – Estudio Empírico

PARTE 3 – Recomendaciones y conclusión

Capítulo 1: Introducción

En este primer capítulo se presentará el objeto de estudio del trabajo poniendo el foco en la situación que ha disparado la alerta de las compañías, debido al papel que desempeñan los empleados a la hora de "permitir" el acceso de manera inintencionada de los ciber atacantes a los sistemas donde se almacena la información.

1.1 Estado de la cuestión

El factor humano constituye el eslabón más débil de la cadena en relación con la ciberseguridad. El *modus operandi* de los atacantes (los cuales solían dirigir sus ataques a los sistemas) ha variado debido a la infinidad de información sensible de la que se puede disponer y a la facilidad de interconexión. Esto sitúa a las personas como foco del ataque (Castillo, 2022) y constituye la estimación de que más del noventa por ciento de los ataques exitosos son propiciados por errores humanos (ThriveDX, 2022). Ante esta situación, todo tipo de compañías ha comenzado a plantearse como mantener un nivel de madurez óptimo respecto a la ciberseguridad entre sus empleados y no solo a contar con la seguridad que proporcionan los elementos tecnológicos a la hora de mantener los sistemas robustos.

El Instituto Nacional de Ciberseguridad (INCIBE) recoge en uno de sus informes que "La cadena de ciberseguridad será tan fuerte como su eslabón más débil sea". Con este tipo de alegaciones el factor humano pasa a situarse en primer plano debido a que sus actuaciones comprometen en gran medida a las compañías y por lo tanto, las mismas deberían actuar en consecuencia. Es por ello por lo que términos como concienciación y formación se encuentran a la orden del día en lo que a esta materia refiere.

Reforzar aquello que las debilita pasa a ser una de las tareas principales de las organizaciones, cuyo objetivo es contar con empleados comprometidos que supongan la primera línea de defensa frente a las amenazas de ciberseguridad, también conocido como *"human firewall"* o "cortafuegos humano" (Sushir, 2023). Para conseguir este nivel de protección, optar por la configuración de una Política de Concienciación en ciberseguridad, e implementar y llevar a cabo numerosas medidas relativas a la misma, es la opción que la mayoría de las empresas desarrolla.

1.2 Objetivo del estudio

El objetivo de este estudio es evidenciar la eficacia de las Políticas de Concienciación en Ciberseguridad, que implementan las empresas, en cuanto a la reducción de las brechas de seguridad derivadas de ataques exitosos dirigidos a los destinatarios de estas políticas.

1.3 Metodología de la investigación y estructura

El trabajo contará con una parte descriptiva que servirá de introducción para contextualizar el análisis y como preludio de este. Estos capítulos contendrán información referente a los ciberataques, la cultura de ciberseguridad, la concienciación en ciberseguridad, la disposición de la estructura organizacional y la figura de la alta dirección en materia del tema.

Los tipos de ataques existentes han variado según la evolución de la digitalización y con ello, a quien van dirigidos los mismos. Por esto, aun contando con un gran abanico de ataques, este trabajo se restringirá a aquellos en los que el factor humano es determinante en todas las instancias para que se produzca una brecha de seguridad. Quedarán recogidas las variedades de ataques dirigidos a las personas, mientras que los ataques dirigidos a sistemas o en los cuales el factor tecnológico dicta la posibilidad de éxito, aunque nombrados, no serán fruto de análisis. Con esta focalización será preciso determinar que existe una evaluación objetiva de la reducción de brechas de seguridad debido exclusivamente a la implantación de políticas de concienciación en ciberseguridad.

Será necesario asegurarse, a su vez, de qué sectores cuentan con políticas de concienciación, para lo cual, se llevará a cabo una segmentación por sectores de actividad atendiendo a la obligatoriedad impuesta por regulación de la aplicación de políticas de concienciación (Infraestructuras críticas) o la no obligatoriedad. Esto nos proporcionará una visión más certera de la aplicación de políticas.

Como corolario se incluirán los resultados obtenidos por una infraestructura crítica nacional en base a una serie de ciber ejercicios recogidos en su política de concienciación, los cuales esclarecerán de manera más acotada el funcionamiento y resultado de éstas. Para lo cual, se han usado herramientas como visualizaciones y datos aportados por la compañía que han podido ser triangulados con sus responsables de seguridad de la información.

Incluir la visión de profesionales permitirá contextualizar aún mejor todo lo analizado en los capítulos anteriores y conocer de primera mano lo que está ocurriendo en el mundo laboral actual, por lo cual, una serie de *"Chief Information Security Officers"* (En adelante, *CISOs*), directores de seguridad de la información y responsables de velar por la ciberseguridad dentro de las compañías (García, 2023) ofrecerán su perspectiva como cumbre de la pirámide y moderadores de estos movimientos. Para lo cual, se ha confeccionado un documento compuesto por 12 preguntas obtenidas tras recabar información tanto de los resultados obtenidos como de la literatura.

Para concluir el trabajo es pertinente incluir recomendaciones prácticas sobre el plan de concienciación a desarrollar y, fundamentalmente, la necesidad de mantener actualizados a los empleados por la vigencia y continua evolución de los ataques. Estas recomendaciones están respaldadas por informes redactados por multinacionales tecnológicas como Aggity.

La razón de esta metodología se debe al carácter del objeto de estudio y a la brecha de información que existe en la actualidad e impide obtener datos que puedan ser generalizados. Por esta razón, lo más pertinente supone una triangulación de datos procedentes de las tres fuentes mencionadas a lo largo del epígrafe, una parte obtenida del estudio bibliográfico, recabando toda la información accesible, un doble estudio de caso (con uno de ellos de carácter más global y otro genérico) y finalmente, una entrevista a los profesionales en la materia, para cerrar una metodología muy acorde al carácter inédito del tema en cuestión.

PARTE 1 – Marco Teórico

Capítulo 2: Los incidentes de ciberseguridad

Este segundo capítulo se adentra en el mundo de los ciberataques, distinguiendo por tipos, a quien van dirigidos y cuál es la razón por la que pueden llegar a culmen de manera que beneficie a los delincuentes. Teniendo una visión más clara de los ataques que existen y su categorización, se puede concretar qué tipo de mecanismos usar para evitarlos.

2.1 Los ciberataques

En las organizaciones existen vulnerabilidades que explotan individuos con fines delictivos cuya intención es obtener algún beneficio (principalmente económico). Estos ciberdelincuentes llevan a cabo intentos de obtención de acceso a sistemas informáticos, de manera deliberada, dirigida y sin autorización, sirviéndose de técnicas y métodos muy diversos (INCIBE, 2020a).

La "*Ciber Kill Chain*" (Anexo 1) es el ciclo de vida de un ciberataque y recoge la secuencia organizada de fases en que los delincuentes ejecutan su agresión para así alcanzar su objetivo final. La sucesión cíclica de siete pasos está compuesta por (INCIBE, 2020b):

1. Reconocimiento, en esta primera fase el individuo con fines maliciosos pretende recopilar información sobre su objetivo y realizar las primeras asunciones sobre cómo actuar y que técnicas se adecuarían al ataque.
2. Preparación, una vez especificadas y aterrizadas las asunciones de la fase anterior se confecciona el método del ataque.
3. Distribución, supone la transmisión del ataque.
4. Explotación, una vez comprometido el equipo y red a la que el mismo pertenece se produce la "materialización" del ataque en sí. Se suele llevar a cabo por medio de la explotación de una vulnerabilidad conocida.
5. Instalación, esta fase puede ocurrir o no dependiendo de las circunstancias del ataque y si el mismo refiere disposición de un malware o no (no en todos los ataques es necesaria la instalación de un malware)

6. Comando y control, en este punto, el atacante tiene control sobre el sistema y ejecutará acciones maliciosas como el robo de documentación confidencial y la sustracción de credenciales.
7. Acciones sobre los objetivos, esta última fase supone una vuelta al inicio, pues busca expandir el ataque buscando más objetivos, repitiendo la cadena para infectar más sistemas.

2.2 La diferencia entre un ciberataque y una brecha de seguridad

El conjunto mundial de organizaciones recibe una media aproximada de 6.687.872 ataques al día (KasperskyLab, 2023), lo cual no quiere decir que todos ellos acaben siendo exitosos, algunos de estos son desmantelados antes de provocar cualquier tipo de daño. La multinacional líder en soluciones y servicios de ciberseguridad, Fortinet, recoge en uno de sus informes acerca de la insuficiencia de habilidades en ciberseguridad, que el 86% de las empresas mundiales ha sufrido, como mínimo, una brecha de seguridad posiblemente atribuible a la falta de concienciación y conocimiento (Fortinet, 2022). Esto sitúa el número de ataques fructíferos en un alto porcentaje y supone la vulneración de cantidades ingentes de información sensible de las compañías.

Una brecha de seguridad se trata de un incidente fruto de un ciberataque exitoso en el cual los datos de carácter personal u organizacional se ven comprometidos, esto supone el acceso no autorizado y, por consiguiente, el robo, la codificación y la alteración de estos (AEPD, 2019). Generalmente se produce cuando el atacante es capaz de sortear los mecanismos de seguridad de la empresa y se debe, en su mayoría, a errores humanos.

Para que se produzca una brecha de seguridad es necesario que la organización sufra un ciberataque. Distinguiremos entre ataques exitosos, aquellos capaces de corromper los sistemas de seguridad de las compañías e infiltrarse en los sistemas (nos situaríamos en la fase cuatro dentro del ciclo de vida de un ciberataque, la explotación), y aquellos que no lo son, fallidos, los cuales se frenan en una de las primeras fases de ejecución sin llegar a vulnerar los sistemas. Una vez se produce un ataque exitoso, este puede traducirse en una brecha de seguridad (en la mayor parte de las ocasiones, pues suele ser el objetivo) o no llegar a concluirse.

Para aterrizar debidamente lo explicado nos serviremos de una situación en la cual iremos desarrollando los pasos del *Anexo 2* explicando qué ocurriría en las diferentes casuísticas.

Una empresa del sector financiero sufre un ciberataque, se trata de una empresa grande y con numerosos recursos los cuales destina, en gran medida, a la prevención y protección de ciberataques, cuenta con un equipo de empleados preparados que detecta con rapidez la amenaza y evita que se produzca la brecha de seguridad. Por otro lado, una Pyme, las cuales se encuentran en el foco de mira de los atacantes (UEStudio, 2023) puede no contar con sistemas de protección o que los mismos no sean algo primordial en lo que esta invierte. La misma sufre un ciberataque y este es exitoso por lo que el atacante accede a los sistemas y a la red de la pequeña empresa. En este momento se pueden dar dos escenarios: Que se produzca una brecha de seguridad, el ciberdelincuente accede sin autorización a los datos personales, obtiene credenciales y otro tipo de información sensible de carácter personal u organizacional. Que no se produzca una brecha de seguridad, pues su finalidad sea distinta, como la denegación de servicios (DoS) que imposibilita el acceso a la red, con esto se concluye que no todos los ciber incidentes suponen una brecha de seguridad (AEPD, 2021).

2.3 Tipología de ciberataques

La variedad de ciberataques es diversa y se reparte, principalmente, en cuatro categorías que engloban diferentes metodologías bajo un término más genérico: Ataques a contraseñas, ataques por ingeniería social, ataques por *malware* y finalmente, ataques a las conexiones (INCIBE, 2020c).

Los ataques a contraseñas tienen su foco en la obtención de credenciales de usuarios por medio de distintos tipos de ataques de fuerza bruta. Con el uso de un software específico, el ciberdelincuente intenta entrar en un sistema utilizando combinaciones de diferentes caracteres cada vez y de manera reiterada hasta dar con la composición correcta. Entre las variantes de este tipo de ataque aparecen; el ataque de diccionario, que para obtener las combinaciones se sirve de diccionarios de palabras (desde palabras comunes, hasta una recopilación de datos personales del usuario a atacar). El relleno de credenciales, una vez se ha producido una brecha de seguridad en la que las mismas se han robado, se prueban las diferentes combinaciones de usuario y contraseña hasta dar con las correctas. Y el ataque de pulverización de contraseñas, con programas más especializados que tienen en cuenta la

posibilidad de que existan barreras de seguridad (como la opción de restringir la cuenta si la contraseña se introduce cierto número de veces de manera incorrecta) y utiliza numerosas contraseñas robadas en un grupo de cuentas seleccionadas buscando probar si se obtiene acceso (García, 2022).

Los ataques por ingeniería social utilizan técnicas de manipulación para explotar vulnerabilidades humanas y así conseguir que las víctimas difundan datos sensibles de carácter personal, financiero u organizacional (Bodnar, 2020). Estas ofensivas se pueden producir por medio de mensajes, tanto verbales como digitales, diseñados para engañar a la víctima y confundirla con el fin de que divulgue cierta información, los canales por los cuales se puede transmitir el mensaje divergen entre: el correo electrónico (*phishing*), por llamada telefónica (*vising*) o por mensaje de texto o SMS (*smising*). Aunque en todos estos tipos de ataque el estafador busca hacerse pasar por otra persona o entidad reconocido por el atacante, existe una variante llamada *spear phishing*, cuyo foco suele ser una víctima en específico (altos cargos o personas con poder) y pretende emular un mensaje cuya procedencia es una persona del círculo de la víctima, a la que conoce y en quien confía (haciendo mucho más difícil su detección). El *baiting* supone la introducción de un malware por medio de descargas de contenido infectado o incluso el uso de unidades USB de dudosa procedencia (la estafa nigeriana). Otras formas de ataque por medio de ingeniería social serían el *pretexting*, el atacante simula una situación falsa y ofrece una solución a cambio de información (la cual comenta es necesario para proceder a solucionar el problema), el *scareware*, cuyo estilo de manipulación se caracteriza por inducir miedo a la víctima y el ataque de abrevadero (*watering hole*), en el que por medio de un código malicioso en alguna página web frecuentada por la víctima se puede producir tanto el robo de credenciales como la descarga de malwares (IBM, s. f.).

Los softwares que se utilizan como medio de ataque dependen de la finalidad de este, los ataques por *malware* disponen de un software malicioso el cual está diseñado para corromper los equipos y las redes a las que estos están conectados causando daños o invadiendo sistemas y así poder secuestrar, alterar o cifrar datos comprometidos (Malwarebytes, 2018). Los ataques pueden ser de diferente índole, desde los virus, que pueden destruir sistemas operativos y desplegar cargas útiles, hasta los gusanos, los cuales agotan los recursos. Se pueden producir a su vez por medio de anuncios malintencionados (*adware*) o *softwares* que recopilan información y se la mandan al atacante, haciendo las veces de espía (*spyware*) (Proofpoint, 2022). Un tipo de *malware* que destaca debido al tipo de perturbación que ocasiona, su alcance y las nefastas consecuencias que puede acarrear es el *ransomeware*. Esta

variedad de troyano se descarga en los equipos y se distribuye por la red cifrando los datos de manera que inhabilita los sistemas y todo lo almacenado. La evolución de este malware avanza a un ritmo vertiginoso llegando a propiciar tres extorsiones diferentes con el mismo ataque, una para la descodificación y recuperación de la información, otra para evitar la difusión de los datos robados y finalmente para evitar otro tipo de ataque, como la denegación de servicios (Valenzuela, 2023)

La última modalidad de ataque es el ataque a las conexiones, entre sus objetivos destaca el de situarse entre el usuario y el servicio web monitorizando los movimientos y el intercambio de información (*man in the middle*). El *spoofing* (existen varios ejemplos según el canal) se encuentra dentro de este grupo de ataques y se centra en la suplantación de páginas web, por medio del cambio de direcciones IP reales por otras de carácter fraudulento, del mismo modo, se pueden crear redes trampa por medio de una red wifi de apariencia similar, pero de carácter fraudulento. La inhabilitación de equipos por medio de un ataque de denegación de servicios (DOS) o denegación distribuida de servicios (DDOS) compromete a su vez las conexiones. La única diferencia entre ellos es el número de atacantes al sistema (Fortinet, 2023), ambos emiten una alta cuantía de peticiones para incapacitar el funcionamiento del servidor web. Se puede a su vez introducir líneas de código malicioso pues muchas páginas webs están soportadas por lenguaje SQL (Inyección SQL) y producirse un escaneo de puertos abiertos por los que entrar (INCIBE, 2020d).

2.4 Los ataques dirigidos a personas o a sistemas

Muchos ataques comparten finalidad, pero no por ello llegan a su objetivo de la misma manera, dentro de la tipología de ataques se considera también quien es el receptor de la vulneración. Los ataques a conexiones y los malware van esencialmente dirigidos a sistemas, por su modalidad de actuación, el factor humano no intercede ni supone un eslabón en la cadena del desarrollo del ataque. Los ataques por ingeniería social van siempre dirigidos a los seres humanos, la descripción de este destaca el poder de manipulación y engaño que ejercen los ciber delincuentes sobre sus víctimas. Los ataques a contraseñas, a primera vista, podrían confundirse con ataques dirigidos a personas, pero si se analiza con detalle el "modus operandi", es el uso de programas específicos de listas los que se usan para perpetrar un acceso. El factor humano aparece en un segundo plano como figura que confecciona y protege las

credenciales, pero el ataque, en cualquier instancia, no pasa por ningún individuo para poder desarrollarse.

2.5 Principales causas por las que se producen los ciberataques

La existencia de ciberataques de tipologías variadas, y en especial, a quien van dirigidos cada uno de ellos hace evidente la disonancia entre las causas que los producen, bien es cierto que la gran mayoría dependen del destinatario, pero no todas ellas.

Las causas con independencia del destinatario se centran por lo general en el extravío o robo de dispositivos tecnológicos (los mismos contienen información que queda expuesta) o en la divulgación, tanto intencionada como no intencionada, de información y datos de carácter sensible (Jiménez, 2022).

Entre las causas con dependencia del destinatario, los cuales hemos dividido con anterioridad en personas y sistemas, se encuentran las siguientes: En primer lugar y respecto a los sistemas destacan las deficiencias, vulnerabilidades y fallos en los mismos lo cual suele ocurrir cuando los desarrolladores diseñan de manera errónea o se produce algún problema en los programas, resultando en un blanco fácil de perpetuar debido a las deficientes medidas de seguridad (García, 2022). En segundo lugar, hay que tener en cuenta las líneas de conexión que existen entre la organización y otras empresas, en estos casos se utiliza el término "caballo de Troya" que hace referencia a la infección de sistemas introduciéndose por canales de enlace o puertas abiertas que existen entre compañías con lazos de relación u otro tipo de contacto por red (Muñoz, 2022). Las razones por las que se produce un ataque dirigido al factor humano no dependen de las fallas de los sistemas ni de la vulneración de las medidas de seguridad, dependen de la actuación del ser humano a la hora de detectar y permitir la ocurrencia de un ciberataque. La falta de formación y concienciación respecto al tema supone uno de los principales factores que propician el desarrollo de un ciberataque, ya que está en manos humanas su control y sin el conocimiento suficiente, su identificación no será posible y puede suponer un alto riesgo para la compañía (MacKay, 2018).

Una vez conocidas las causas resulta más fácil la creación de medidas para evitar que estos incidentes se produzcan, en el caso de los sistemas resulta evidente que conforme más seguros sean los servidores y mayores sean las revisiones para cerciorarse que todo está correctamente ejecutado y protegido, la vía de entrada se reducirá en gran medida. Mientras

que estas causas se pueden solventar con ayuda de equipos informáticos y profesionales y dependen generalmente de un grupo reducido de personas, cuyo trabajo precisamente es asegurarse del correcto y seguro funcionamiento de los sistemas, los ataques dirigidos al ser humano impactan a la organización en su conjunto y las medidas para evitarlos deben ir dirigidas a todos los empleados, pues todos ellos son susceptibles de ser atacados. Los programas de concienciación y formación buscan principalmente mitigar esta causa y educar al groso de la compañía con razón de reducir el número de ataques fructíferos (recordemos que el factor humano es el eslabón más débil de la cadena).

Capítulo 3: Cultura en ciberseguridad, madurez de las organizaciones

La tipología de ciberataques hace que la cultura en ciberseguridad de las organizaciones sea muy complicada de suplir del todo. El nivel de madurez de las organizaciones difiere entre los diferentes tipos de empresas y acorde a los tipos de ataque, pero por lo general es muy reducido.

3.1 Las carencias en el comportamiento ante las tecnologías cibernéticas

La Agencia Europea de Ciberseguridad (ENISA) define, en su informe elaborado en dos mil diecisiete, la cultura en ciberseguridad o CSC como "El conjunto de conocimientos, creencias, percepciones, actitudes, suposiciones, normas y valores de las personas en relación con la ciberseguridad y cómo se manifiestan en el comportamiento de los individuos con las tecnologías de la información". Se pretende que las consideraciones en seguridad de la información comiencen a formar parte del día a día en el entorno laboral de manera que queden integrados en las acciones cotidianas (ENISA, 2017). En cambio, la situación actual que se vive en las organizaciones se encuentra alejada de este escenario, según recoge el Informe del estado de la cultura de ciberseguridad en el entorno empresarial elaborado por la consultora PricewaterhouseCoopers (PWC), el ochenta y seis por ciento de las organizaciones no cuenta con una cultura de ciberseguridad o la misma debe mejorarse sustancialmente. Con razón de aterrizar los datos de una forma más cuantitativa, según un rango de valores entre uno y cinco (de carácter orientativo y definido por la consultora), el nivel de CSC de las empresas actuales no supera el tres, quedándose en un dos con ocho sobre cinco, esto determina un largo margen de mejora y sitúa el Dominio de comportamiento de los empleados como el factor con una puntuación menor dentro del conjunto de los analizados (PWC, 2020). Toda esta información se alimenta también de los datos e indicaciones recabados por el Foro Nacional de Ciberseguridad (FNC) con ayuda del Departamento de Seguridad Nacional, la Fundación Borredá y la asociación ISMS. Estos organismos destacan la ignorancia frente a los desafíos de la digitalización, y con ello la falta de protección ante futuras amenazas cibernéticas, la incompetencia generalizada y la carencia de aptitudes de los trabajadores (con esto resalta la incipiente necesidad de canales de difusión y medidas de concienciación que respalden el tema) (FNC, 2021)

Las entidades con conocimiento en el campo repiten de manera insaciable la precariedad en la que se encuentran las compañías y las deficiencias de sus trabajadores en la

materia, por lo que para tener medidas de cuantificación comunes del sentido de la cultura en ciberseguridad entre los empleados y para poder elaborar hipótesis con un principio asentando, existen unos perfiles basados en dos competencias cuyo conjunto configura los niveles de madurez.

3.2 Los perfiles conductuales de madurez basados en actitud y capacidad

Existen innumerables modelos de medición de madurez en ciberseguridad, pero cada uno de estos está dirigido a un área en específico, no es lo mismo medir la madurez de los sistemas que la de la cultura de los empleados, así como dentro de la cultura de los empleados existe diferencia según el departamento, pues aquellos que trabajan en sistemas lidian a menudo con temas de ciberseguridad mientras que en otros departamentos, al no ser su trabajo *per se*, quede completamente relegada.

La conocida empresa de ciberseguridad MITRE, desarrolló "MITRE ATT&CK" o matriz Mitre, un modelo de conocimientos de uso universal y actualización continua que permite detectar, modelar y combatir las ciber amenazas por medio de una extensa base de datos que recoge los comportamientos de los ciberdelincuentes en cada uno de los posibles ciberataques (*MITRE ATT&CK®*, 2015), cuenta a su vez con marco en cultura de ciberseguridad. El Marco en Cultura de ciberseguridad o "Ciber-Security Culture Framework" desarrollado en dos mil veinte por la compañía, pretende evaluar de manera individualizada a los empleados posicionándolos en ciertos niveles de acuerdo con ciertas dimensiones relacionadas con la cultura en ciberseguridad y a su vez estimar y valorar la posición de la organización en su conjunto (Georgiadou et al., 2021).

Para entender en qué nivel se debe situar a cada uno de los empleados se utiliza la Matriz de medición de la cultura en ciberseguridad (ver Anexo 3) la cual en su eje horizontal representa la actitud y en el vertical la capacidad. Esta matriz por tanto se compone de cuatro cuadrantes donde cada uno de ellos, dependiendo de los niveles de capacidad y actitud, cuentan con un nombre definido y cualidades diferentes. El cuadrante inferior izquierdo es el más desprovisto de ambas competencias y por tanto está compuesto por los empleados con mayor propensión a ser víctimas de ataques de ingeniería social, el nombre de este grupo es *Human Security Breach* o brecha de seguridad humana (haciendo alusión a que son los mismos los que permiten que este incidente suceda). A continuación, el cuadrante superior izquierdo, conformado por personas con suficientes capacidades, pero con una actitud negativa frente a

la seguridad, aparece el término *Firewall* del que hablamos con anterioridad, pero en este caso se podría decir que el mismo está "desactivado", por ello se conoce a este conjunto como "*Human Firewall Disabled"* que supone la existencia de potencial junto a desinterés. Los dos grupos restantes cuentan con una actitud feroz respecto a la ciberseguridad. Mientras los "*Rookie Defenders"* no cuentan con conocimiento suficiente suponiendo un riesgo a pesar de mostrar mucho interés, el "*Firewall* Humano" ocupando el cuadrante superior derecho con máxima puntuación en ambas aptitudes, representa al colectivo de personas aptas para la gestión eficaz de la ciberseguridad (Georgiadou et al., 2021a).

Para hacer una división certera se preparan cuestionarios dirigidos con los cuales se conoce la posición de cada empleado en la matriz, se puede personalizar y adaptar el tipo de formación dependiendo de las necesidades y se puede conocer por medio de un cómputo global la situación en la que se encuentra la compañía.

3.3 Niveles de madurez de la cultura de la ciberseguridad basados en los perfiles

Tras el desempeño de un estudio individualizado en el que se posiciona a cada uno de los empleados en la casilla correspondiente según la proporción de actitud y capacidad que demuestren, se desarrolla un análisis a mayor escala otorgando niveles de madurez en cultura de ciberseguridad a la organización como conjunto.

Infinidad de modelos permiten obtener el nivel de madurez respecto a la cultura en ciberseguridad de las compañías, pero en este caso continuaremos con el marco desarrollado por MITRE. Este establece que el porcentaje de empleados que componga cada uno de los cuadrantes en la Matriz de medición de la cultura en ciberseguridad de los empleados esclarecerá la visión global y permitirá la evaluación de la compañía en cuatro niveles.

De acuerdo con los siguientes niveles, cuyo valor aumenta a medida que la compañía cuenta con más madurez, las empresas pueden encontrarse en (Georgiadou et al., 2021):

- **Nivel 1**, destaca el predominio de perfiles con un grado de actitud y capacidad muy reducido y existe cierto nivel de oposición ante las medidas de seguridad por ser consideradas un freno para la productividad. Prevalecen las prácticas inseguras.
- **Nivel 2**, los empleados cumplen la normativa establecida, pero no todos ellos desarrollan prácticas seguras según qué motivos.

- **Nivel 3**, la aplicación de políticas de seguridad es defendida por la gran mayoría de los trabajadores y a su vez, existen grupos que se implican en mayor medida para monitorizar el correcto y seguro desarrollo.
- **Nivel 4**, se produce una activa participación del total de los empleados por lo que los índices de seguridad de los que goza la compañía son de carácter elevado.

En el *Anexo 4* se representa una situación ficticia en la que cada uno de los puntos de color anaranjado en la primera matriz simboliza a cada uno de los empleados de un supuesto departamento de una compañía (se puede hacer división por departamentos, por cargos desempeñados…) y en la matriz de la derecha el porcentaje que supone cada uno de los perfiles y a partir de los cuales se clasifica en los niveles expuestos en el párrafo anterior. En este caso la mayor parte de los empleados son catalogados como "*Human Firewall*" pero existe cierto número de individuos en los otros cuadrantes suponiendo un potencial riesgo para la organización. Se revisamos los niveles, podemos observar que aquel que se acerca más a la descripción es el nivel dos, por lo tanto, esta supuesta compañía tendría un Nivel 2 de madurez en la cultura de ciberseguridad.

Una vez se determina el nivel, daría por concluida la evaluación inicial respecto a la cultura de la organización en materia de ciberseguridad. A partir de aquí se determinarían las medidas a desarrollar para subir de nivel y finalmente con las mismas se compondrá el Plan de Concienciación y Formación en ciberseguridad. Este programa pretende capacitar a los empleados y prepararlos para enfrentarse a posibles ciber amenazas, recopilando al efecto, tanto medidas a desempeñar y ejercicios, como objetivos y alcance (Orrantia, 2021).

Capítulo 4: La concienciación en la ciberseguridad

La falta de madurez en ciberseguridad hace que las compañías no estén cubiertas del todo en materia de ciberseguridad, permitiendo que los ataques que reciben acaben concluyendo en una brecha de seguridad. Para evitar esto se desarrollan planes de concienciación que sirven para adecuar y capacitar al empleado para evitar estos incidentes.

4.1 La importancia de las políticas de concienciación y su aplicación en ciberseguridad

Toda política de concienciación cuenta con un fin concreto que se basa en aumentar el conocimiento de aquellos a los que va dirigida, capacitándolos para actuar según las bases de seguridad apropiadas para un desarrollo de negocio seguro. Las políticas suelen quedar recogidas en los planes de concienciación y la ejecución de estas se lleva a cabo por medio de las medidas de concienciación (Araujo, 2021)

El Diccionario de la lengua española (RAE, 2021) define la palabra concienciación como; "Hacer que alguien sea consciente de algo, adquirir consciencia de algo". Por lo tanto, este tipo de programas buscan hacer a todos los miembros de influencia en la empresa conocedores de la situación de manera que puedan actuar consecuentemente y de forma sensata al estar dotados de la información pertinente y actualizada.

Respecto a la concienciación en ciberseguridad, existen principalmente dos líneas de actuación muy relacionadas y que deben complementarse para asegurar el resultado esperado. La primera de ellas se centra más en el ámbito de la formación, por medio de la realización de actividades, ya sean cursos o talleres, en las cuales se adquiere conocimiento en la materia. Esta forma de concienciar suele ser más específica y pretende explotar temas más complejos y muchas veces dirigidos a sectores o estructuras de actuación diversas. En segundo lugar, y mucho más distendida y general, destaca la "concienciación *per se*", esta se centra en la divulgación de conocimientos básicos que de no saberlos podrían poner en peligro al usuario o a la organización y que van de la mano con los niveles de digitalización que se experimentan en la actualidad. De esta manera no solo se informa, sino que se verifica que las medidas están dando su fruto (Ortega, 2021).

4.2 Tipología de políticas; herramientas y medidas

Existen numerosas prácticas bajo el paraguas de las dos líneas de actuación propuestas en el párrafo anterior. El Instituto Nacional de Ciberseguridad (INCIBE, 2019) aporta una visión generalizada de las mismas a las que se les pueden incluir ciertos matices:

1. **Kit de concienciación**, recoge recursos que permiten la elaboración de un plan de formación integral en seguridad de la información, puede contar con elementos de diferentes tipos (píldoras de información, talleres, carteles, verificaciones…). Con él se pretende mantener al empleado al tanto de la situación y llevar a cabo buenas prácticas en su trabajo diario (ateniéndose a aquello que el Kit de concienciación determina).
2. **Formación**, consiste en cualquier tipo de actividad que incluya la adquisición de conocimiento relevante y de un carácter más específico. Se puede realizar por medio de cursos, vídeos, lecciones, charlas con profesionales, etc. Y puede extrapolarse a los distintos sectores empresariales (formación sectorial) centrándose en adecuar principalmente las medidas al campo pertinente de manera que se optimice el proceso de formación y concienciación.
3. **Ciber ejercicios**, configuran ciertos retos o pruebas que pretenden "entrenar" a aquellos que las lleven a cabo y así conocer tanto el nivel de madurez de estos como su posible actuación ante la situación expuesta. Estos ciber ejercicios se pueden dividir en:
    a. *Roleplay*, estos se centran en potenciar de manera lúdica el conocimiento de los empleados. Para ello se utilizan situaciones ficticias en las que los trabajadores deben actuar de cierta manera.
    b. Simulaciones, recreación de incidentes a diferente escala cuyo desenlace debe ser mantener el ataque controlado (de nuevo de carácter ficticio)
    c. Ataque dirigido, se trata de un ataque real que se puede enviar desde dentro o fuera de la organización y que se centra en la búsqueda de vulnerabilidades y el desarrollo de las capacidades de los afectados ante una situación "aparentemente real".

Todas estas medidas tienen un punto en común, aumentar la madurez en ciberseguridad y asegurarse que el desempeño de las tareas diarias se hace de la forma más segura posible.

Cabe destacar a su vez que para que la concienciación sea los más efectiva posible es necesario tener en cuenta factores como: Resultados de evaluaciones continuas, fomento de la cultura en ciberseguridad, claridad a la hora de exponer cambios o incluso a la hora de adoptar las políticas por primera vez y sensaciones de aquellos a los que van dirigidas (feedback, consecuencias de incumplimiento…) (Tuñón, 2023)

4.3 La función del CISO y la alta dirección en la administración de las políticas

Todos los componentes de la organización deben estar al tanto de los avances en la tecnología y de cómo hacer un uso responsable de la misma. Pero existen figuras que deben estar aún más concienciadas pues serán las que impulsarán la cultura en ciberseguridad y todos los planes de concienciación. De manera jerárquica respecto al nivel de responsabilidad y difiriendo en la forma de actuar de cada rol, podemos diferenciar entre (INCIBE, 2023):

El CEO, que ostenta el cargo más alto en la organización debe liderar el movimiento de concienciación y colaborar con la alta administración en su conjunto para velar por el correcto desempeño de cada una de las tareas sin mermar la seguridad informática.

El CISO, responsable de la seguridad de la información se consideraría el líder impulsor y gestor en el tema. Ciertos eslabones por debajo se encuentran los artífices de las medidas y políticas que en última instancia son evaluadas y aceptadas por el CISO, estos son los miembros pertenecientes al departamento de seguridad (que se puede a su vez subdividir en el equipo de seguridad de la información o ciberseguridad).

El Equipo de concienciación en ciberseguridad, no se trata de una figura individual, sino que se refiere más a la unión de diferentes responsables cuya función es la gestión de las medidas de concienciación en diferentes escalas (equipos, departamentos…) y velar por el cumplimiento de las políticas acordadas. Esta alianza suele estar conformada por un representante de ciberseguridad, de comunicación, de tecnologías de sistemas de la información, de respuestas a incidentes y de recursos humanos. Su colaboración es esencial para asegurar el funcionamiento correcto de la ciberseguridad.

A pesar de que las políticas de concienciación suelen proceder generalmente del departamento de ciberseguridad, y por ende, sean ellos los que principalmente velan por su cumplimiento y el aumento de la concienciación, cabe destacar el papel que ejerce a su vez el departamento de recursos humanos tanto como integrante del Equipo de concienciación en

ciberseguridad, como con sus propios medios. La naturaleza de este departamento le permite llevar a cabo acciones de colaboración, de formación y de retención de todo ese conocimiento que es crucial para el auge de la cultura y su divulgación por toda la compañía (Greenlee, 2023).

PARTE 2 – Estudio empírico

Capítulo 5: Análisis del caso de estudio

Las herramientas que aportan las medidas de concienciación en ciberseguridad son consideradas útiles a la hora de aumentar la seguridad, pero por medio de este caso de estudio que se expone a continuación, se estudiará el efecto certero de las políticas.

5.1 Planteamientos preliminares

El caso de estudio se dividirá en diferentes análisis en los que se busca probar la certeza de que la aplicación de políticas de concienciación en ciberseguridad favorece la reducción de ataques fructíferos que desembocan en brechas de seguridad.

Los datos han sido recogidos de "*HACKMAGEDDON*". Se trata de una web que recopila de manera actualizada datos respecto a los ciberataques que acontecen, en forma de líneas del tiempo, los que han producido brechas de seguridad y también datos en relación con incidentes en Cloud. El artífice de estos informes es el Profesional en seguridad de la información Paolo Passeri, director y referente de seguridad, y encargado de la ciber inteligencia en empresas como Cisco o Netskope. La recopilación de datos se ha producido tanto por medio de la carga de los mismo a partir de la web de "*HACKMAGEDDON*" como por medio de documentos enviados por el propio Sr. Passeri.

Respeto a la muestra seleccionada del total de ciberataques producidos desde que se han podido recopilar datos fiables, se han seleccionado los ocurridos entre 2021 y 2023. El número de ataques no se ha filtrado de ninguna manera obteniendo el total de estos en ese periodo. Respecto a las brechas de seguridad, la muestra seleccionada comprende a su vez el periodo entre 2021 y 2023 y recoge aquellas que han tenido mayor envergadura habiendo capado aquellas que no supusieron un gran efecto.

5.2 Tratamiento de los datos

La base de datos en cuestión viene sin procesar ni limpiar, por lo que para ser apta para el análisis será sometida a ciertos procesos. Esta cuenta con dos tablas: La tabla "Ataques", que recoge la información de todos los ataques que tuvieron lugar en el periodo de estudio. Y la tabla "Brechas" que distingue cuales de los registros de la primera tabla han concluido en una brecha de seguridad. Las tablas serán unidas por medio de una unión uno-a-uno, ya que cada registro solo aparece una vez en cada una de ellas (registros únicos).

Las variables de la tabla "Ataques" son: *Fecha, Compañía, Tipo de Ataques, País y Sector*. A esta tabla se le van a añadir tres variables más de carácter binario (0 o 1), la primera de ellas se denominará "Brechas de seguridad" y será fruto de la unión de ambas tablas, se indicará con un 1 aquellos ataques que hayan producido brecha de seguridad y un 0 en caso contrario. La segunda será "Ataques de Ingeniería Social", es decir, aquellos que son caso de estudio por ir dirigidos a las personas. Se indicará con un 1 todos aquellos ataques que pertenezcan al segmento filtrado de tipos de ataques y de nuevo 0 en caso contrario. La última variable se conoce como "Sectores regulados – Infraestructuras Críticas", a partir de otra selección como en el caso anterior, se denotará con un 1 aquellos ataques dirigidos a este tipo de sectores y con un 0 a los no regulados.

5.3 Análisis de resultados

El estudio, la explicación y desarrollo de este, va a seguir la siguiente estructura: En primer lugar, se analizarán todos los ataques y la procedencia de cada uno de ellos. A continuación, se comenzará a distinguir por tipo de ataque, con foco en los ataques de Ingeniería Social o Dirigidos a las personas, se introducirá también el conjunto de brechas de seguridad, con y sin dependencia del tipo de ataque que las ha provocado. Se procederá a una división entre sectores y se analizarán las diferencias entre aquellos que son regulados y no. Como broche final se compararán todos los factores en común para así determinar de manera más precisa el resultado conjunto. A lo largo de toda la investigación se incluirán hipótesis concretadas y dificultades acaecidas.

El total de ciberataques recogidos en los datos es de 5236, estos están presentes en todos los continentes y se distribuyen a lo largo de 142 países entre los que destacan Estados Unidos, con un total de 2565 ataques de 62 tipos diferentes. El continente europeo, con un promedio

aproximado de 65 ataques por país, suma 700 ataques contando únicamente con los países pertenecientes a la Unión Europea. El resto de los continentes no resaltan tanto por sus cifras.

Gráfico 1

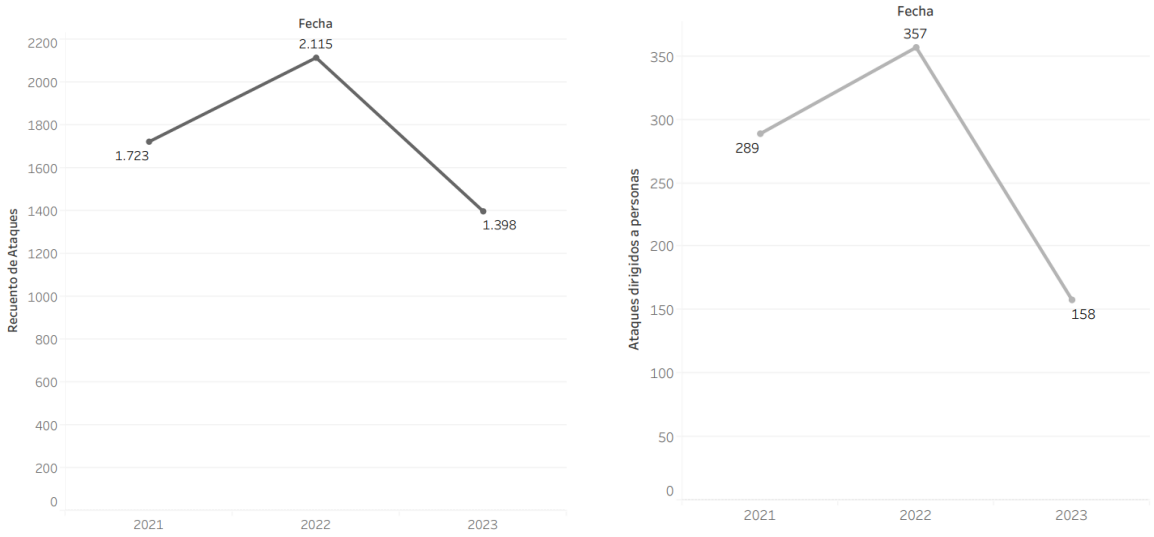
Distribución de los Ciberataques por país

Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri,2011)

El análisis global de los ataques enfatiza el pico producido en 2022 con un total de 2115 ataques, seguido por 2021 con 1723 y destacando la caída en 2023 con 1398. Los ataques de Ingeniería Social suponen el 22,17% del total de los ataques con una cifra de 1161 y siguen una evolución prácticamente similar a la del conjunto de los ataques, pero algo más acentuada, pues la caída en 2023 en de algo más de un 55% en comparación con el 34% de los ataques en total.

Gráficos 2 y 3

Evolución de los Ciberataques y de los Ciberataques de Ingeniería Social (2021-2023)



Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

Para la elaboración del Gráfico 3 se ha tenido en cuenta la hipótesis que en adelante será considerada como primera pues será la que se tenga en cuenta a la hora del análisis. Esta hipótesis considera que ningún tipo de ataque "Unknown", que se trata de uno de los registros que componen el campo "Tipos de Ataques", pertenece a la categoría de ataque de Ingeniería Social. Estos tipos de ataque no están catalogados por falta de información.

Una hipótesis (que quedará definida como hipótesis descartada) se trata de incluir un porcentaje de estos registros al conjunto de ataques dirigidos a las personas. Para ello sería necesario hacer un recuento del porcentaje de ataques por año que van dirigidos a personas en comparación con el total del año sin tener en cuenta los "UnKnown". El porcentaje en cada uno de los años es, 22%, 26% y 19% respectivamente, el promedio es muy parecido al del total considerando todos los registros, un 22%, por lo que ese porcentaje de "Unknowns" podrían considerarse Ingeniería Social. Otro problema que se encuentra en esta hipótesis es la selección de los registros para recategorizar, pues dependerá de factores como: El número de este tipo de registros cada año, el porcentaje por año, el criterio de selección, la aleatorización, etc.

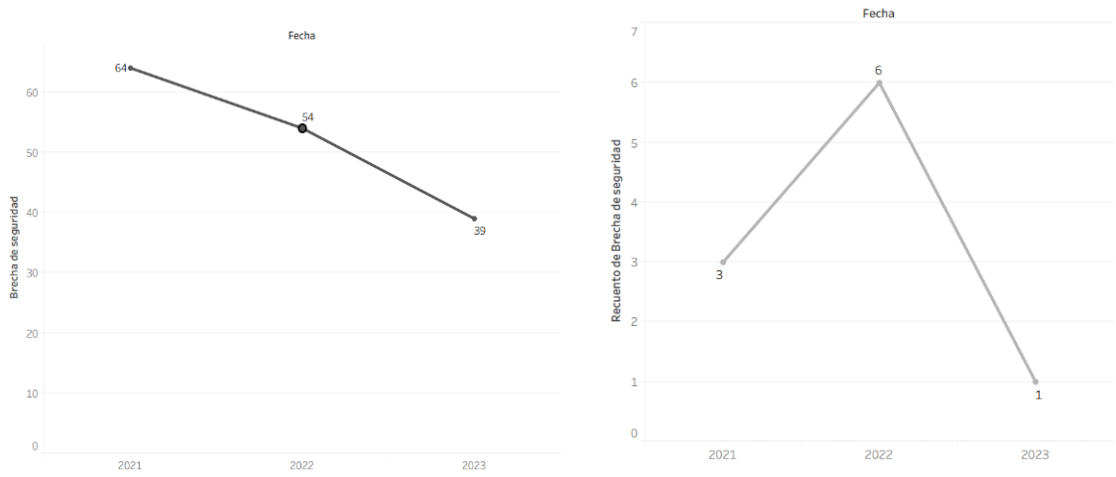
Finalmente se ha concluido que la hipótesis primera será la predominante en el estudio y los valores "Unknown" quedarán catalogados como ataques a sistemas. Bien es cierto que

esta hipótesis cuenta con carencias que pueden afectar al estudio, tales como la cantidad de registros de este tipo. Pero la hipótesis descartada aportaba aún más ruido al estudio y por lo tanto no se considerará en adelante.

La dinámica en la evolución de las Brechas de Seguridad difiere atendiendo al tipo de ataque que se represente, mientras que las brechas en su conjunto experimentan una tendencia a la baja, al enfocarse únicamente en aquellas producidas por ataques de Ingeniería Social repuntan sustancialmente en 2022, no por su cifra en si (reducida en comparación con el resto de los ataques), sino por duplicar la cifra del año anterior. Por otro lado, la bajada en 2023 sitúa la cifra cinco puestos por debajo de los registrado el año anterior. En el reporte que hizo Fortinet en 2023 sobre "La Brecha de Habilidades en Ciberseguridad a Nivel Mundial 2023" (*Fortinet, 2023a)*, refleja que la subida en las brechas se seguridad del 53% se debe a la escasez de talento y conciencia en el tema. Si consideramos este estudio de manera inversa, la reducción de las brechas de seguridad tiene una correlación positiva (de más o menos fuerza) con el aumento de habilidades y conocimiento procedente de la aplicación de políticas de concienciación en ciberseguridad.

Gráficos 4 y 5

Evolución de las Brechas de Seguridad en el global de los ataques y en los ataques de Ingeniería Social (2021-2023)



Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

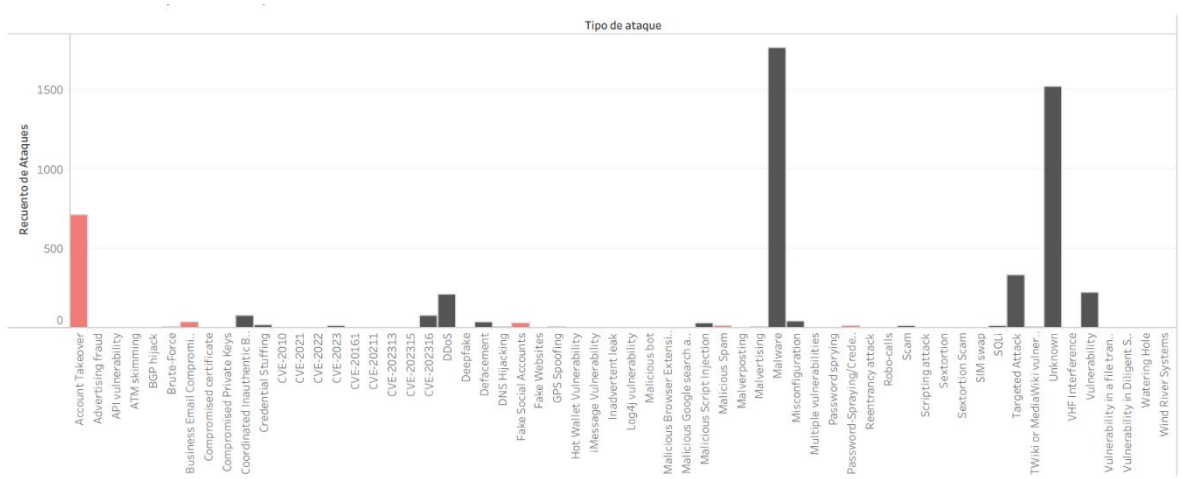
Estos datos recogen 82 tipos de ataques diferentes que se pueden categorizar en los cuatro tipos que existen y dentro de las dos categorías de tipos de objetivos en los diferentes ataques. Dentro de los ataques dirigidos a sistemas se recogen ejemplos de malwares, de

ataques a contraseñas como *Password-Spraying/Credential Stuffing* y de ataques a conexiones como *Malicious Browser Extension o DDos.* Entre los ataques de Ingeniería Social destacan ejemplos como *Account Takeover o Fake Social Accounts*.

Para diferenciar por objetivos del ataque se ha seleccionado el rojo para los ataques de Ingeniería Social y el Gris Oscuro para los dirigidos a sistemas.

Gráfico 6

Recuento de los Tipos de Ataques

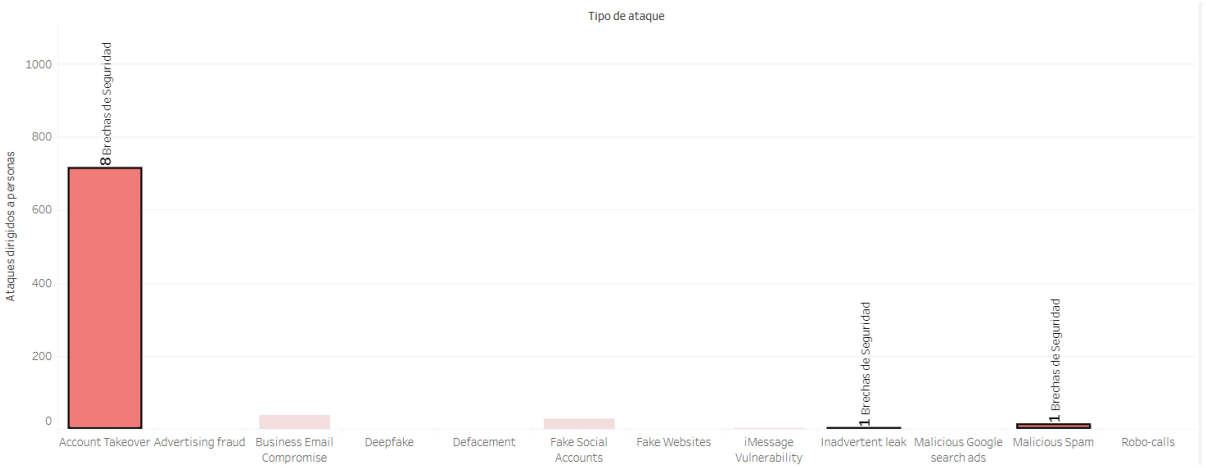


Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

Aproximadamente el 78% de los ataques van dirigidos a sistemas y destacan en especial los de malware superando las cuatro cifras. Los ataques desconocidos son el segundo tipo con más cantidad, el próximo tipo de ataque que se produce con gran frecuencia su pone algo menos del 50% de este, por lo que es un gran gap. Predominan por tanto los ataques dirigidos a sistemas, tanto por cantidad de tipos como por frecuencia de algunos en especial. Los ataques de Ingeniería Social (en rojo) destacan algo menos y su máximo no supera las cuatro cifras y se trata de *Account Takeover*.

Gráfico 7

Brechas producidas en los ataques de Ingeniería Social

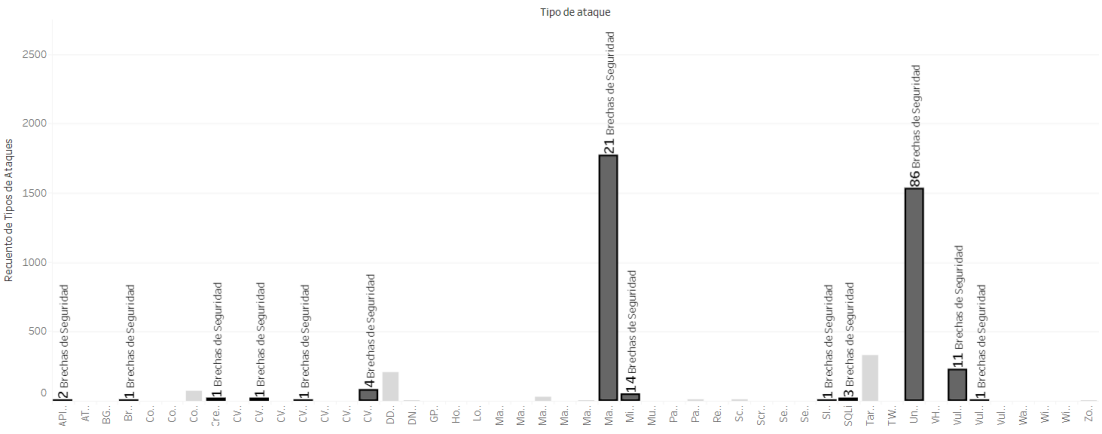


Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

De las 10 brechas de seguridad que se han producido por ataques de Ingeniería Social, 8 de ellas se han producido en ataques de robo de cuenta, por lo que el 80% de las brechas han sido por este medio. Este tipo de ataque se produce cuando por medio de algún tipo de manipulación, el empleado entrega de manera inconsciente sus credenciales y permite al atacante acceder al sistema y obtener la información que desea. Algo más del 1% de los ataques de Ingeniería Social se traduce en una brecha de seguridad, parece una cifra reducida, pero cabe tener en cuenta la facilidad con que un delincuente puede mandar esos ataques y la cantidad de estos si lo considera oportuno. Un único individuo puede comprometer a toda una compañía.

Gráfico 8

Brechas producidas en los ataques dirigidos a Sistemas



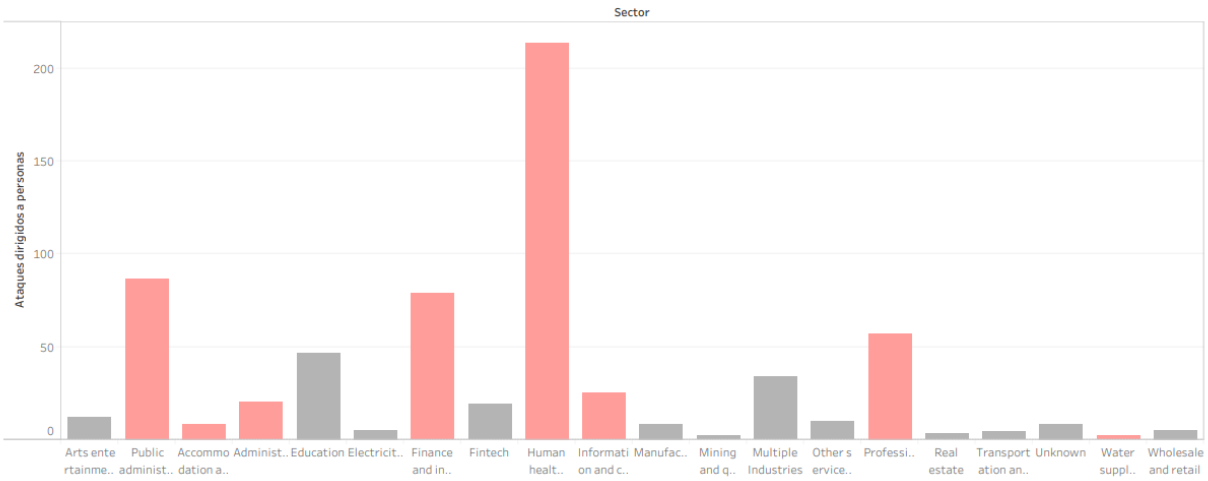
Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

El resto de las brechas de seguridad del total recogido se produce en los ataques dirigidos a sistemas, destacando los no conocidos con el mayor número de brechas en comparación con el resto de los tipos de ataque sin tener en cuenta a quien va dirigido el mismo.

A continuación, se procede a realizar el mismo planteamiento con los diferentes tipos de sectores, con un gris más claro se representan los sectores no regulados, aquellos que no so primordiales. Con un color rosáceo las Infraestructuras Críticas, sectores que por sus características esenciales tiene la obligación de adoptar medidas de concienciación en ciberseguridad.

Gráfico 9

Ataques de Ingeniería Social por sectores

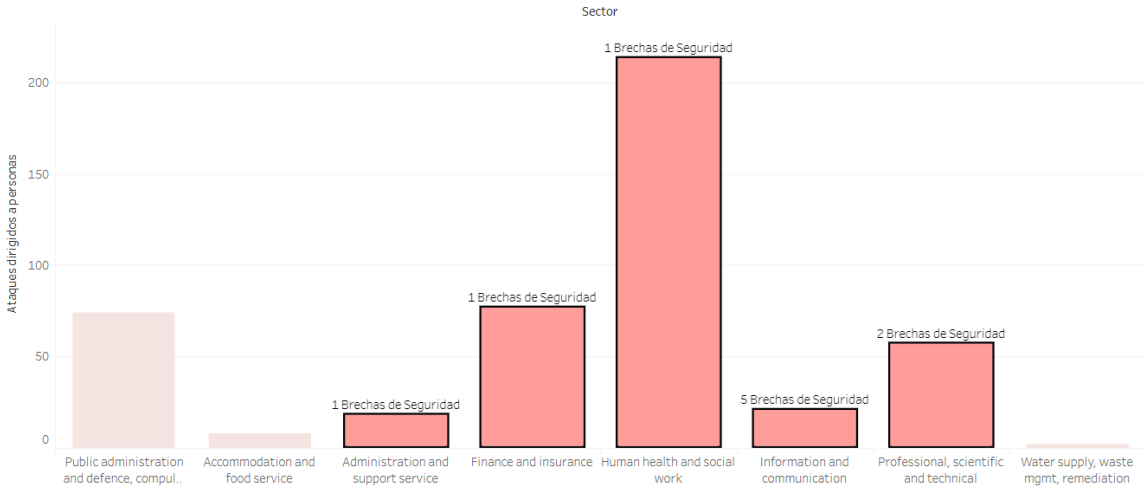


Fuente: Elaboración propia, basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

El gráfico se encuentra teñido fundamentalmente de rosa, esto se debe a que los ataques de Ingeniería Social buscan utilizar la manipulación para obtener el mayor beneficio, y debido al carácter de estos sectores, su información cobra más valor y por tanto desata el interés de los ciber delincuentes y se convierten en objetivo de más ataques. En proporción, cada uno de los sectores considerado como Infraestructura Crítica tiene un 12% de probabilidad de recibir un ataque en *ceteris paribus*, frente al 8% de los sectores no regulados.

Gráfico 10

Brechas de Seguridad producidas por ataques de Ingeniería Social dirigidos a las Infraestructuras Críticas

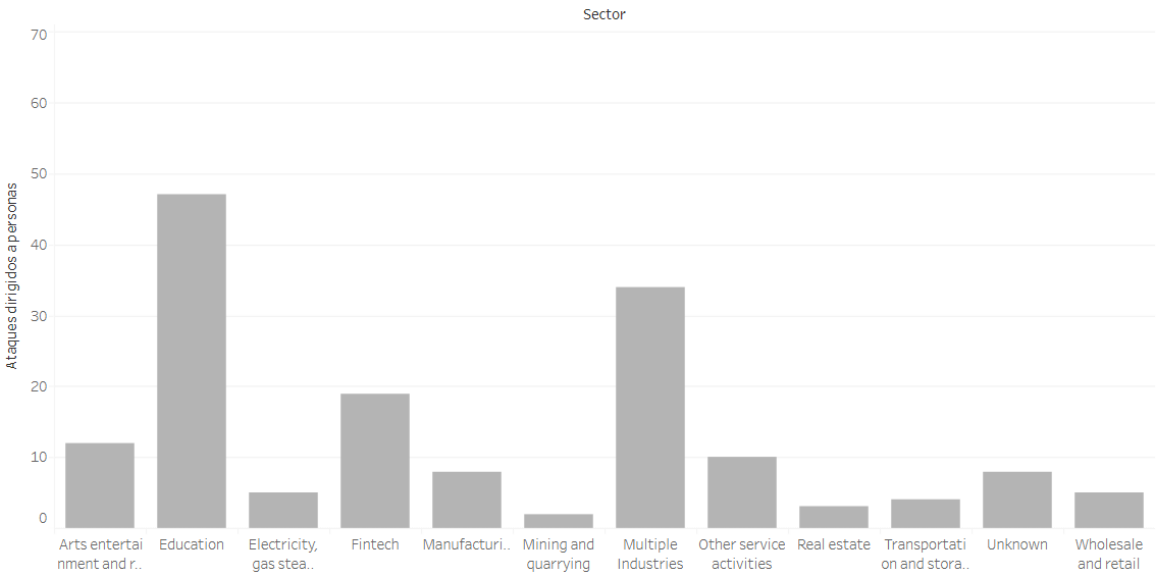


Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

El total de Brechas de Seguridad en los ataques dirigidos a personas era de 10, este número se repite cuando nos referimos a estos ataques, pero cuyo foco son las Infraestructuras Críticas. Esto se debe a diversas razones, en primer lugar, el carácter de la información que mueven este tipo de sectores se trata de información muy sensible y privada, cuanto más valor tiene la información, más posibilidades de que ese sector sea atacado. En segundo lugar, la aparición de nuevos ataques más dirigidos, que va de la mano con el tercer punto que se refiere al perfeccionamiento de los ataques para así obtener el máximo rendimiento. Con ataques de mejor calidad y eficacia, y con destinatarios predeterminados o de una manera menos general y más planificada, las posibilidades de sufrir una brecha de seguridad si no se cuenta con planes de concienciación aumenta exponencialmente.

Gráfico 11

Brechas de Seguridad producidas por ataques de Ingeniería Social dirigidos a las Infraestructuras Críticas

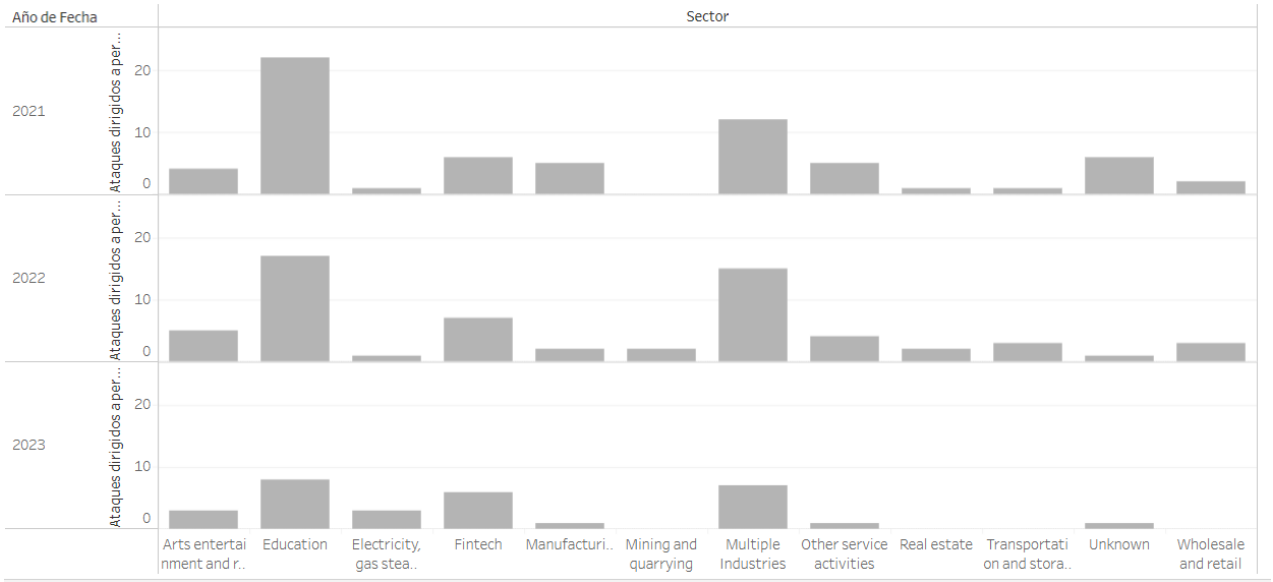


Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

Como oposición a lo que ocurre con las Infraestructuras Críticas, los sectores no regulados no superan los 30 ataques de media, esto supone que el interés de los ciberdelincuentes en estos sectores no se equipara al de aquellos que están regulados. Estos sectores, si sufren algún tipo de brecha de seguridad, no compromete a aquellos atacados de la misma manera que en el caso anterior. Para cotejar aún más esta reducción de ataques en este tipo de sectores, la comparación entre los años transcurridos deja ver claramente esta bajada.

Gráfico 12

Evolución de las Brechas de Seguridad en los Ataques de Ingeniería Social en los sectores no regulados



Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

Las Infraestructuras Críticas, sin embargo, han experimentado otra serie de acontecimientos respecto a la cantidad de ataques recibidos y las Brechas de Seguridad. La diferencia de ataques entre los años 2021 y 2023 es muy reducida, una de las únicas variaciones es en el sector sanitario. En este primer año el porcentaje de Brechas de Seguridad superaba el 1,5%, mientras que en 2023 no llegaba al 0,7%. Si suponemos que en 2023 se hubiera llegado a la misma cifra de ataques y teniendo en cuenta los porcentajes, la cifra se situaría en un 1%, un tercio menos de lo logrado en 2021. Acudiendo de nuevo al informe de Fortinet (Fortinet, 2023a), la subida en número de Brechas de seguridad experimentada entre 2021 y 2022 por la falta de concienciación se tradujo en el siguiente año en una bajada del 83,3% debido a la eficaz implementación de políticas de concienciación sobre la ciberseguridad. Si asumiéramos constancia en el porcentaje de Brechas de seguridad y se llevara a cabo de nuevo la métrica anterior, con 312 ataques en 2022, el 2% supusieron brechas, mientras que, si eso hubiera ocurrido en 2023, el porcentaje sería de 1,7%.

Gráfico 13

Evolución de las Brechas de Seguridad en los Ataques de Ingeniería Social en las Infraestructuras Críticas

Fuente: Elaboración propia basado en los datos sobre ataques y brechas de seguridad (Passeri, 2011)

Siguiendo el hilo de los capítulos anteriores, la definición e implantación de políticas de concienciación parece tener un efecto positivo en la reducción de las brechas de seguridad especialmente en las Infraestructuras Críticas. Un análisis más exhaustivo podría extrapolarse a las brechas de seguridad propias de ataques dirigidos a sistemas en los cuales sería necesario focalizar la aportación que ofrecen las políticas de concienciación, frente al porcentaje frenado por la configuración de sistemas y *firewalls* robustos.

Capítulo 6: Análisis de una política aplicada en una infraestructura crítica

La evidencia de que las políticas de concienciación reducen las brechas de seguridad es clara atendiendo a los datos globales, pero en el siguiente análisis, se busca demostrar a su vez, cuáles son los efectos de apartar las medidas durante un corto periodo de tiempo y así, hacer ver cómo de importante, o no, es la continua actualización de las políticas.

6.1 Determinación de la política; Los Ciber Ejercicios

De la tipología de políticas de concienciación en ciberseguridad, una de las prácticas en las que se materializa son los ciber ejercicios pues ofrecen resultados más objetivos. Por medio de la gamificación del aprendizaje y la consecución de actividades las cuales incluyen un resultado al ser finalizadas, permite determinar niveles, concretar valoraciones e incluso hacer comparaciones entre sectores, competidores o en especial, entre infraestructuras críticas (debido esencialmente a su regulación).

El centro de respuesta a incidentes de ciberseguridad (INCIBE-CERT) del Instituto Nacional de Ciberseguridad (INCIBE) actúa desde 2012 como anfitrión en la ejecución de Ciber Ejercicios o "CyberEX" entre las compañías del sector privado. Su papel de coordinador le dota de tareas como la configuración de las actividades a realizar, la revisión de la ejecución de estas y su evaluación.

Para valorar los diferentes aspectos de madurez sobre la concienciación en ciberseguridad existen tres pruebas diferentes que son: *Roleplay*, Simulación de incidente y Ataque dirigido (características de este tipo de políticas). Las funciones primordiales de estas intervenciones son la mejora de las capacidades, el refuerzo de la concienciación y la mejora reputacional de la compañía (INCIBE, 2022).

6.2 Ejecución de la política

Los Ciber Ejercicios evaluados se llevaron a cabo en el año 2018. En esta edición participaban 26 entidades pertenecientes a 4 sectores críticos diferentes (aquellos responsables de servicios esenciales de una sociedad).

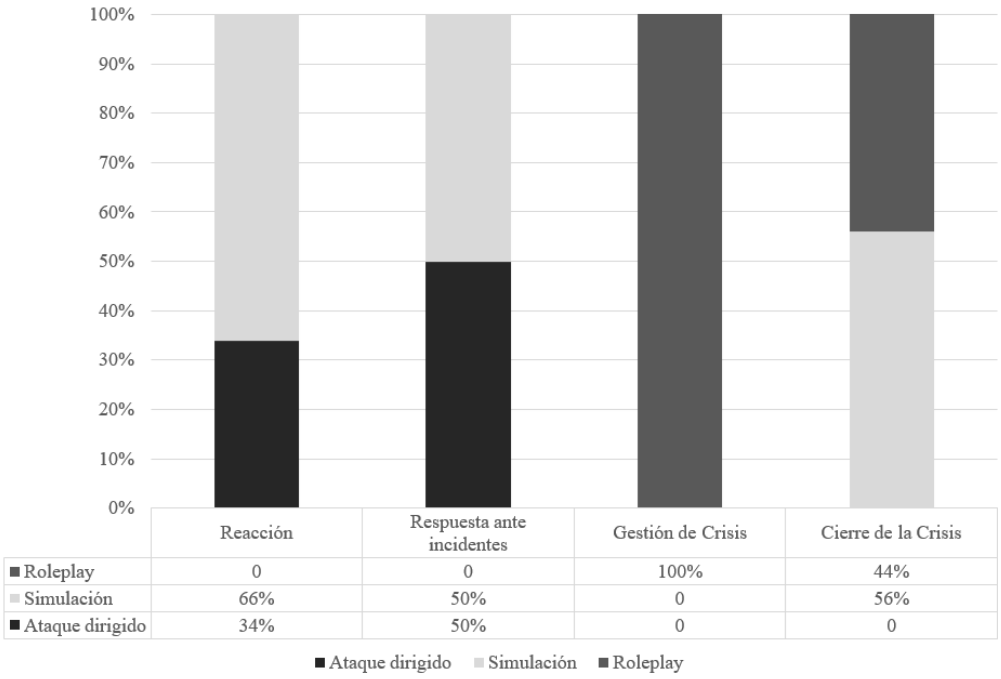
La temática de las pruebas, dentro de los tres tipos mencionados con anterioridad consistían en los siguiente: Una prueba de ingeniería social, específicamente *spear phishing*,

junto con el envío de un USB con un malware. Una simulación basada en técnicas avanzadas y por último un *roleplay* enfocado a la gestión de una crisis (no solo prevenir, sino identificar y solventar). La evaluación de estas actividades se centra en determinar las capacidades de los participantes, conocer su alcance y su estado de madurez.

La distribución de la puntuación atiende a 128 controles agrupados en cuatro categorías, desde La Reacción, Respuesta ante incidentes y Gestión de crisis, hasta El Cierre de la crisis. No todas las categorías se evalúan de manera equitativa en cada ciber ejercicio, sino que reciben más o menos peso respecto a lo que cada ejercicio pretende demostrar.

Gráfico 14

Distribución de las puntuaciones por prueba y categoría



	Reacción	Respuesta ante incidentes	Gestión de Crisis	Cierre de la Crisis
Roleplay	0	0	100%	44%
Simulación	66%	50%	0	56%
Ataque dirigido	34%	50%	0	0

Fuente: Elaboración propia basada en la distribución de puntos en los "CyberEX" (INCIBE, 2022)

6.3 Análisis de los resultados obtenidos por la infraestructura crítica

Por motivos de confidencialidad, en el siguiente párrafo no podrá incluirse el nombre de la Infraestructura Crítica y es posible que ciertos datos no sean desvelados o estén cifrados de cierto modo. El análisis que se va a llevar a cabo es el resultado de una de las infraestructuras críticas que desempeñó los "CyberEX" o ciber ejercicios durante los años 2016 y 2018. Con

esta ventana de dos años se realizará una comparación entre ambos resultados atendiendo a la situación de la empresa y a su vez una comparación con el sector en el que ésta, opera.

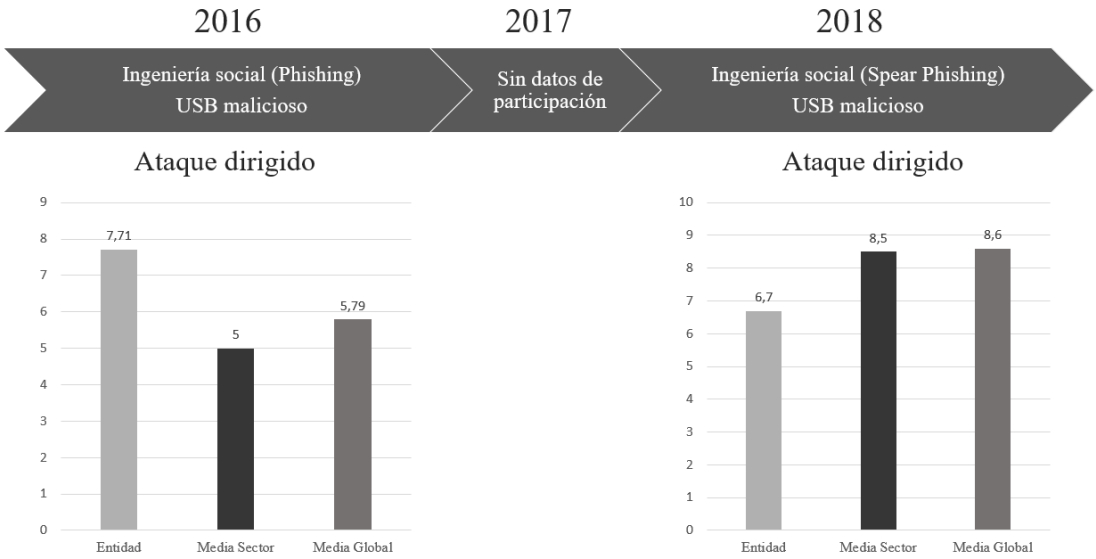
El Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) define el concepto como "Una infraestructura estratégica que proporciona servicios esenciales y cuyo funcionamiento no permite alternativas al ser indispensable". Por lo tanto, cualquier tipo de perturbación que acontezca puede influir de manera muy negativa y afectar incluso globalmente. En esta situación cabe resaltar la obligatoriedad de la imposición de políticas de concienciación en estos sectores para evitar cualquier tipo de contingencia.

En el caso de la Infraestructura crítica que será analizada, esta se encuentra dentro del sector financiero, se trata de una empresa que destaca por liderar sus avances en materia de ciberseguridad (en todos sus ámbitos). Para focalizar este análisis aún más y debido a las diferencias que existen entre los ciber ejercicios de cada año, el análisis se centrará en el Ataque Dirigido, pues ambos eran de ingeniería social y muy enfocados al conocimiento general procedente de la instauración de políticas de concienciación, mientras que los otros ejercicios, en este caso, mostraban un carácter más técnico dirigido a sistemas. La elección de este ciber ejercicio en concreto se debe a que, como ha quedado expresado a lo largo del estudio completo, la forma primordial en la que se pueden reducir las brechas de seguridad procedentes de ejercicios de ingeniería social (aquellos dirigidos a personas) es por medio de políticas de concienciación.

El contexto que acontecía y que esclarecerá la situación es el siguiente: Esta compañía obtuvo unos resultados favorables con un desempeño satisfactorio en los ciber ejercicios de 2016, por lo que en esa ventana de dos años no modificó su política ni incluyó medidas de concienciación. Por otro lado, la media del sector era mucho más reducida, pues hasta el momento no tenían en cuenta la necesidad de implantar este tipo de políticas. A partir de estos resultados, destacó la decisión generalizada de llevar a cabo este tipo de medidas en los años venideros.

Gráfico 15

Resultados del ciber ejercicio "Ataque dirigido" entre los años 2016 y 2018



Fuente: Elaboración propia basada en los resultados de los ejercicios CyberEX proporcionados por la en entidad (Datos confidenciales)

Como se puede observar en el Anexo 6 los resultados de la entidad han disminuido un punto mientras que la media tanto del sector como global han aumentado significativamente. Esto se debe a la implantación de las políticas de concienciación, mientras que la entidad de estudio, como ha sido corroborado por su CISO en cuestión, no adoptó medidas debido al resultado obtenido en la primera prueba y la superioridad que denotaba en comparación con el resto de los participantes. Por lo que la no adopción de medidas propició una reducción en el nivel de preparación con el que contaban los empleados. Por otro lado, el resto de las compañías ante las cifras obtenidas decidieron aplicarse en la materia obteniendo así un brillante resultado en el año venidero.

Este ejercicio muestra una prueba específica dentro del patrón global que explica que la incorporación de este tipo de políticas verdaderamente prepara a los empleados y les educa para intervenir en situaciones y ser consciente de ellas por ende reduciendo riesgos y brechas de seguridad. Mientras que aquellos que quedan rezagados o no prestan atención se muestran desactualizados y más vulnerables al no considerar la aplicación de las medidas de concienciación.

Capítulo 7: Opiniones de los expertos

A pesar de que el análisis se encuentre en línea con toda la evaluación anterior al mismo, las opiniones de profesionales en la materia que se presenta a continuación buscan aportar una visión más certera de lo que está ocurriendo en las entidades y si cada una de ellas difiere en situación.

7.1 Introducción, definición de las preguntas y entrevista

La valoración y opinión de expertos en este ámbito aporta una visión más cercana a la situación actual que se presenta en las empresas. Para ello, se ha contactado con tres profesionales de diferentes sectores, para atender las necesidades e inversiones de distintas entidades y así obtener un marco lo más completo posible.

La interacción ha consistido en una entrevista de en torno a una hora en la cual se exponían temas más enfocados en la compañía como objeto individual, con sus medidas propias, y a su vez una orientación más global, con la evaluación de empresas consideradas Infraestructuras Críticas y el desarrollo general de las políticas de concienciación.

Para desarrollar el repositorio de preguntas que configurarían la entrevista se han tenido en cuenta, en primera instancia, los resultados procedentes de ambos análisis, tanto el global como el focalizado. Y, en segundo lugar, toda aquella información en la que existe una pequeña brecha dentro de la literatura, o aquellas cosas en las que sea preciso ahondar un poco más. Una vez obtenida la información requerida e identificados los datos que necesitaban mayor desarrollo, se procede a la configuración de preguntas que dieran respuesta a estas cuestiones.

Entrevista

Cuestionario dirigido a los directores de Seguridad de la Información

1. ¿Cuál es la labor que desempeña la figura del CISO en referencia a concienciar a los empleados sobre la ciberseguridad?

2. ¿Qué medidas ha implementado la organización de la que forma parte para fomentar la concienciación entre sus empleados?

3. En una escala del uno al diez, ¿cómo puntuaría la eficacia de las medidas adoptadas por su organización y como evaluarías el cómputo de las medidas de concienciación en general?

4. ¿Cómo evalúa la efectividad de las campañas de concienciación en ciberseguridad?

5. En términos de adopción, ¿cómo describiría el grado de concienciación sobre ciberseguridad entre los empleados de la organización? ¿Ha notado mejoras en los últimos años?

6. ¿Existe algún proceso en particular para comunicar a los empleados modificaciones en las políticas o la introducción de nuevas medidas? Si es así, ¿Cuáles son los medios?

7. ¿Las políticas o medidas suelen variar mucho en el tiempo o se mantienen estables?

8. ¿Qué nivel de correlación consideras que existe entre la evolución en las tecnologías y la variación en las políticas?

9. ¿Qué estrategias utiliza la organización para evaluar la madurez de la concienciación en ciberseguridad de sus empleados? ¿Existen evaluaciones periódicas o programas de formación continuada?

10. ¿Cuál es el papel de la alta dirección en la promoción de la concienciación en ciberseguridad? ¿Cómo se asegura de que los líderes de la organización respalden y participen en estas iniciativas?

11. ¿Cómo evalúa usted como CISO el nivel de concienciación en ciberseguridad a nivel global, considerando las tendencias y amenazas emergentes?

12. ¿Considera que existen áreas específicas de mejora identificadas en el ámbito de la concienciación en ciberseguridad a nivel organizacional?

Fuente: Elaboración propia

7.2 Miguel Ángel Fernández, CISO de Redsys *(formerly)*

Miguel Ángel Fernández ostentó el puesto de CISO de la compañía Redsys hasta el año 2023. Como CISO, el destacaba que las labores primordiales a desarrollar en su trabajo se basaban en revisar y confeccionar las políticas de concienciación debido a que su posición le permitía ajustarlas a las necesidades de la empresa, al ser conocedor de las carencias que la misma pudiera tener.

En la compañía en la que operaba, desarrolló un estudio para conocer las amenazas de ciberseguridad que pudieran afectar a cada una de las áreas de la entidad, siendo conocedor de esto, confeccionó junto a su equipo un plan a tres años que incluía medidas de dificultad progresiva y orientadas a los diferentes tipos de ataques de Ingeniería Social. Como conocía las amenazas ante las que formar a los empleados, evalúo con un 8 la eficacia de las pruebas, mientras que, ante otro tipo de incidentes, destaca la falta de conocimiento. Afirma que la implementación de políticas de concienciación siempre aumenta la escala de salvaguardas en mayor o menor valor, dependiendo de la proyección de la entidad.

Para evaluar cómo está evolucionando la madurez entre los empleados se analizan los resultados de diferentes prácticas, se segmenta por departamentos y por empleados para obtener *insights* más completos. Tras la misma, el Sr. Fernández considera que el nivel de concienciación entre la plantilla es entre medio y alto y difiere entre los departamentos (de ahí la necesidad de estudio por segmentos), centrándose en los más tecnológicos y los más operativos. Advierte que los ejercicios más complejos siguen obteniendo resultados negativos.

Las medidas que aplica, al igual que las políticas, siguen una línea de evolución continua, pero bastante por detrás de la que siguen las nuevas tecnologías, esto, es un punto negativo, pues no se va a la par, pero eso permite a la empresa estar preparada y tener tiempo para evaluar los cambios y adecuar las medidas.

La labor de la alta dirección la considera fundamental, y menciona la evolución que se ha producido en el rol de estos, de mantenerse al margen, a ser precursores y expandir los conocimientos entre sus equipos. Comenta que se han elaborado planes dirigidos únicamente para ellos, por la necesidad de aumentar su concienciación y convertirles en líderes.

Por último, corrobora que, como cómputo global, existen muchas medidas aún por adoptar y lo considera un sector con gran proyección, no solo por el desarrollo actual, sino por la labor que supone. Expone las diferencias entre las empresas más y menos tecnológicas y como cada una afronta estas situaciones

7.3 Marta Flores, CISO de Mutua

Marta Flores comenzó su andadura como CISO de Mutua en 2019, por lo que tuvo que enfrentarse a retos como la pandemia y a un departamento completamente inexistente que tuvo que construir prácticamente desde cero.

Desde su punto de vista, la labor del CISO es acompañar a los empleados y formarles por medio de la creación de cursos, medidas y campañas para concienciarles, pues reitera que el trabajador es el eslabón más débil de la cadena. Para ello, ha llevado a cabo campañas de phishing por niveles y adaptadas a los conocimientos de cada empleado, algunas de ellas, son de obligado cumplimiento, mientras que otras, son de mantención. Muchas son de carácter anual y se evalúan por desempeño y mejora respecto a los siguientes años.

La Sra. Flores, al igual que el Sr. Fernández, sitúa en un 8 el grado de eficacia de las políticas de concienciación adoptadas, pero considera que el grado de mejora es elevado y que la obligatoriedad de estas ha ayudado a aumentar esta cifra. La diferenciación en sectores hace gran merma en la puntuación global, la cual se equilibra algo más con normativas como DORA, un reglamento instaurado por La Unión Europea cuyo objetivo es reforzar la resiliencia digital y la ciberseguridad en diversos sectores (Losa, 2023).

La evaluación de todas las medidas llevadas a cabo se hace por medio de herramientas automatizadas, ayudadas y revisadas por auditoría interna y estadísticas.

"La perfección en este campo roza lo imposible", expresa la Sra. Flores, pues las campañas varían mucho, los cambios en regulaciones también, y por supuesto, el número nuevo de ataques. Pero por norma general, sitúa a la compañía en una posición elevada respecto al grado de concienciación de sus empleados y considera que esto se debe tanto al trabajo de estos, como a la infinidad de procesos de comunicación que aplica (desde campañas de comunicación apoyadas por el departamento de comunicación interna hasta certificaciones como la ISO27001).

En el caso de Mutua, las medidas son cambiantes y buscan adecuarlas al día a día para que sean más cercanas a la realidad. Para evaluar la madurez procedente del conjunto de empleados que las lleva a cabo, desarrolla evaluaciones periódicas, feedback continuo, boletines de seguridad, etc.

Entre todos los temas, la Sra. Flores hace hincapié en la labor de la Alta Dirección en apoyar y difundir la causa. Recuerda el cambio que se produjo desde su entrada hasta ahora,

con directivos bastante despreocupados e incluso reticentes, a contar con un fuerte apoyo por parte de estos y pasar a ser la seguridad un factor primordial.

Para concluir, desde su papel de CISO, observa un largo camino que recorrer y la necesidad de invertir mucho más, también refiere incrementar las acciones que ejercen los directores, e implicarlos aún más para que tengan más conciencia y la divulguen.

7.4 Carles Solé, CISO Payments Hub – PagoNxt (Santander Global)

Carles Solé es el actual CISO de PagoNxt, la empresa tecnológica de pagos del Santander, y cuenta con una larga trayectoria en el sector bancario. Entre lo más destacado de su trabajo, aparece la función de comunicar, lo que resalta a lo largo de toda la entrevista. Desde su punto de vista, los empleados deben conocer en todo momento lo que se les está permitido hacer y lo que no, y, a su vez, cuáles son los peligros del desempeño de esas malas prácticas. Por lo tanto, la labor del CISO es liderar y comunicar para que todos los empleados estén al corriente. Una de las cosas que se trata de evitar es la de hacer cualquier tipo de pruebas sobre los equipos de la compañía, para así no generar ruido que pueda ser malinterpretado.

Las medidas que lleva a cabo en la compañía van desde hackings éticos locales (de manera repentina y sin muchas consecuencias) a cuatro ejercicios oficiales, y que se realizan cada trimestre, desde los cuales se obtienen notas cuyo resultado deriva en: Un correo con copia al Manager del empleado si se falla una primera vez, un contacto directo con el empleado por parte del equipo de ciberseguridad y por último, si se falla una tercera vez, la reducción de su bonus en un 10%. Diferencia a su vez por los tipos de campaña, existiendo algunas consolidadas y otras conocidas como *"lab*" que aún se encuentran en periodo de prueba y son más laxas. A su vez, utiliza la gamificación como fórmula de educación

El Sr. Solé sitúa el nivel de eficacia de las políticas en un 7, una nota más reducida que las otras dos entidades, pues considera la estacionalidad de la calificación con respecto a la evolución de los ataques y el tiempo hasta prepare para poder enfrentarse con éxito al mismo.

El elevado nivel en concienciación entre los empleados considera que se debe, en primer lugar, a que está regulado por el consejo, debido a la aplicación de una métrica que repercute en el desempeño anual de los CISOS y que sitúa en un 2% el máximo de fallas en las que pueden incurrir los empleados. La variedad y evolución continua de las medidas, y en especial el empeño que se pone en asegurar una comunicación clara y distintiva (un ejemplo

de esta es variar las fuentes de letra que se utilizan en los correos para ver cual atrae más o menos).

Bajo su perspectiva, el apoyo de la alta dirección es fundamental a lo largo de todo el proceso, pero considera que queda un largo camino que recorrer y que se debe buscar ir a la par con las nuevas tecnologías, el desarrollo de campañas cada vez más complejas y la necesidad que aumentar el impacto emocional para realmente cerciorarse de que los empleados están verdaderamente concienciados.

7.5 Valoraciones en común

Los tres profesionales a los que se les ha realizado la entrevista comparten visiones comunes en ciertos aspectos recogidos en las preguntas de la intervención.

En primer lugar, la eficacia que tienen las políticas de concienciación en ciberseguridad, todos las sitúan como medidas de gran utilidad para mejorar la madurez de los empleados y prepararlos para ejercer sus labores de la manera más segura posible. Sin embargo, también consideran que las mismas no pueden mejorar los resultados íntegramente, pero si permitir a las compañías escalar en los niveles de salvaguarda.

La participación de la alta dirección y no solo la de los departamentos de Seguridad y de Seguridad de la Información. Los directivos y altos cargos de todos los departamentos deberían unirse y apoyar estas medidas sirviendo de ejemplo para todos los empleados. Todos aseguran que ha existido una evolución en el comportamiento de los responsables de cada departamento, pero sigue necesitándose aún más unión.

En cada una de las entidades en las que estos CISOs operan, se han desarrollado el mismo tipo de políticas, pero en mayor o menor medida. Todos comparten la realización de ciber ejercicios, la configuración de simulaciones y formaciones de carácter obligatorio.

Como tónica general, todos concluyen que la concienciación en ciberseguridad, tanto la actual sobre los incidentes conocidos, como la futura con los incidentes por conocer, está en una fase de inicio y queda mucha inversión por realizar, muchos cambios por ejecutar y muchas mejoras que desarrollar para realmente llegar a un punto en el que su efectividad a la hora de incrementar la concienciación (aunque no evite el total de los ataques que se traducen en brechas) sea completa.

PARTE 3 – Recomendaciones y Conclusión

Capítulo 8: Recomendaciones y ámbitos de mejora

Tras el estudio y conclusiones de los CISOs, parece evidente la necesidad de seguir emprendiendo el camino hacia la instauración por completo de una cultura en ciberseguridad en todas las organizaciones. Para ello, el capítulo recopila recomendaciones a llevar a cabo y ámbitos prácticos a partir de los que mejorar.

8.1 Recomendaciones prácticas

A la luz de los resultados y su relación estrecha, tanto con la literatura, como con las entrevistas realizadas a las figuras que se encargan de velar por la seguridad de la información, resulta pertinente el desarrollo de recomendaciones. Debido al largo recorrido que debe emprender aún la concienciación en ciberseguridad, estas serán de especial utilidad para cualquier tipo de empresa, pero esencialmente, para PYMES que se están iniciando en el tema y quieren invertir en el desarrollo de la concienciación en ciberseguridad.

La formación va dirigida a todos los empleados, por lo que una educación personalizada y adaptada según qué criterios, amenizará la comprensión de los elementos necesarios. Si la empresa extrapola sus medidas a todas las posibilidades, muchas posibles vulnerabilidades quedarán cubiertas impidiendo incurrir en brechas de seguridad (Mateus, 2022).

Otra recomendación muy barajada es el desarrollo de nuevos modelos de concienciación, más actualizados y que verdaderamente provoquen un cambio de hábito en el comportamiento de las personas y en su manera de desempeñar su trabajo. Por medio de cuestionarios, uso de herramientas, e incluso exposiciones a diversos retos, es posible la adquisición de conocimientos suficientes y bien asentados para hacer frente a situaciones reales (Guillén, 2018).

Las políticas de sensibilización son un fuerte aliado a la hora de mejorar la disposición de los trabajadores ante las medidas de concienciación. Dándoles a conocer la importancia de los datos con los que tratan y la necesidad de realizar buenas prácticas al manipularlos, puede disminuir un mal uso por falta de conocimiento. A esto pueden ir sumados a su vez ciertas

técnicas o estándares que aseguren el uso seguro de la información, como las políticas de modificación periódica de contraseñas (Aggity, 2023).

La importancia de amenizar el proceso de formación y concienciación parece una manera efectiva de motivar a los empleados a prestar más atención. La gamificación es de gran utilidad, pero el uso de vídeos y cuestionarios, por ejemplo, suele ser mucho más rechazado por los empleados debido a la impersonalidad. La contribución de personalidades conocedoras de las medidas y una buena comunicación destacaría en gran nivel entre las labores a desarrollar para mejorar en el ámbito.

Una propuesta a implantar supondría servirse de Inteligencia Artificial y Big Data pues, en este caso, podría ser muy beneficioso. Varias situaciones en las que es considerable que puedan ayudar podrían ser; La realización de modelos en los que se introdujeran parámetros y se estudiara como responden los empleados ante ellos, aquellos con puntuaciones más débiles serían el sujeto de revisión en siguientes ejercicios de seguridad, para mejorar esos aspectos. Esto podría individualizarse para enfocar ciertas actividades de manera más certera y obviar otras que en ese momento estén completamente controladas (uso eficiente de los recursos).

8.2 Posibilidades de mejora

Si la eficacia de las políticas fuera fructífera en todas las ocasiones, y el desempeño de aquellos que las elaboran, implementan y llevan a cabo fuera siempre correcto, el término brecha de seguridad se habría extinguido hace un tiempo.

Los ámbitos de mejora en concienciación en ciberseguridad son extensos y numerosos, pues la participación del ser humano en este proceso nunca permitirá la eliminación por completo del error. Pero se pueden introducir nuevas técnicas, modificar las actuales, o explotar las existentes para poder minimizarlo al máximo (la minimización del error es directamente proporcional a la cantidad de brechas de seguridad).

Uno de los medios que las entidades deberían cuidar más es el hecho de la sobreinformación, aturdir al empleado no resulta beneficioso de ninguna de las maneras. La implementación de un Plan de Concienciación claro suele suponer una de las mayores dificultades, ya sea tanto por la falta de comunicación, como por el uso de términos poco generalistas. Si a esto se une el propósito de distribuir la información lo más rápido posible y pretender que sea entendida por los empleados, cualquier tipo de actuación no será de utilidad en absoluto.

Las compañías deben fijar un plan organizado, definido en común y contando con la aprobación y opinión de las diferentes divisiones a las que quiere alcanzar.

Muchas otras prácticas que podrían hacer más eficaz el proceso de ser implantadas podrían ser: No centrarse exclusivamente en una empresa, sino extrapolarlo a sus proveedores y otras compañías que conforman su cadena de valor, para así, que se establezcan acuerdos de seguridad. Esto se traduciría en una comunicación mucho más clara y precisa que permitiría que la relación vertical estuviera completamente alineada y que el conjunto de compañías que apoyan al desarrollo de cierto bien o servicio, estuvieran cubiertas de la misma manera formando un muro de protección global (Egan, 2023).

8.3 El Desarrollo de un Plan de Concienciación

La manera más efectiva de comunicar la vía de actuación y mantenerla documentada es la formalización de un Plan de Concienciación, en este caso, enfocado a la seguridad informática de la organización.

Este programa recoge todos los recursos, normativas, desarrollos y planificaciones que permitirán y de los que hará uso la entidad de manera determinada, para asegurar la información contenida en sus sistemas. Los objetivos de este plan se centran en capacitar a los usuarios expuestos a los datos ante posibles amenazas, y, en dotarles de conocimientos que les permitan abordar situaciones de riesgo. Tener recogida toda la información facilita su compresión y poder consultarlo en cualquier momento por su disponibilidad constante y su naturaleza pública, ofrece una herramienta a la que acudir en cualquier circunstancia (Ciberseguridad, 2019).

Los Planes de Concienciación deben contar con los siguientes cuatro elementos para estar completos:

1. Planificación, esta debe incluir las necesidades y debilidades, un cronograma de actuación e implantación, selección de recursos y metodologías y por su puesto debe contar con el respaldo de la alta dirección.
2. Implantación, se trata de la estrategia de acción y pretende abarcar a la entidad en su conjunto.
3. Operación y mantenimiento, ejercicios y prácticas.
4. Monitorización y evaluación, conlleva todo tipo de revisión, inspección y comparación.

Como corolario, el programa debería incluir cuestiones de interés común u otro tipo de información complementaria, temas relevantes, dinámicas a seguir, etc.

8.4 Formación y actualización continua

Toda la revisión bibliográfica aportada por entidades como INCIBE, IBM, Fortinet, etc. Y respalda por los profesionales entrevistados, dejan a la vista cómo de fundamental es el mantenimiento de actualizaciones continuas e incrementales a medida que el tiempo transcurre.

Esto se traduce, principalmente, en recurrir a políticas continuamente y que se vayan adaptando a los avances propios en la ciberseguridad. Que se realicen análisis constantes respecto a la situación de madurez y que se lleven a cabo comparaciones entre épocas definidas. El seguimiento y monitorización constante que debe quedar recogida en documentos para permitir así la contrastación.

De nada sirve una política potente, con un volumen de alcance suficiente, si la misma va a quedar olvidada una vez se haya llevado a cabo en su totalidad. No se tratan de medidas transitorias a imponer en momentos determinados, sino una formación continua y no invasiva que permita al empleado continuar con su trabajo, pero siendo consciente de las buenas prácticas que debe desempeñar una vez lo lleva a cabo.

Los CISOs, expertos en la materia, como el Sr. Fernández, la Sra. Flores y el Sr. Solé reiteran en preguntas como la 7, la 9 o la 12 (*Entrevista*), la importancia que tiene la continua actualización de las medidas y como se deben ir adecuando a la evolución de las tecnologías a pesar de ir ciertos pasos por detrás y que se trata de una de las mejoras que se está intentando alcanzar.

Como conclusión para asentar la importancia del mantenimiento del conocimiento es pertinente servirse del ejemplo que acontece a la entidad estudiada en el capítulo 6. Se trata de una entidad que en 2016 estaba por encima de la media y capacitada en mayor nivel para sobrellevar cualquier tipo de incidente en el que el factor humano fuera determinante. Con la puntuación obtenida, se consideró que no era necesario continuar con medidas de concienciación o que las mismas fueran más laxas. Privándolas de la importancia que se les había otorgado hasta la fecha. El desenlace es más que evidente, si merma la atención a las políticas y estas pasan a un segundo plano, sería como retroceder hasta volver a un punto de partida en el que todo incidente de este tipo provocaría una brecha de seguridad.

Capítulo 9: Conclusión y aportaciones del estudio

9.1 Conclusión

Las organizaciones tratan de incluir en sus procesos diarios todos los medios tecnológicos pertinentes para conseguir un desarrollo más eficaz. Todos estos recursos, y la evolución de estos, llevan consigo ciertas amenazas generalmente dirigidas a la vulneración de las capas de seguridad o la incursión en equipos ajenos con finalidad maliciosa. La respuesta que cada entidad da estos ataques depende fundamentalmente de la actuación de los equipos destinados a la salvaguarda de la información cibernética y a los instrumentos que hayan utilizado para impedir o frenar este tipo de agresiones.

Mientras que estos ataques podrían considerarse más dirigidos a un área concreta de la organización y cuya contingencia no depende de todos los integrantes de la compañía, existen otro tipo de ofensivas que de perpetuarse, afectarían a todos y cada uno de los miembros de la organización con presencia en la red (la inmensa mayoría de los empleados). En estos, el factor humano es el determinante, por lo tanto, la solución para evitar este tipo de problemas no depende de la ejecución de sistemas de seguridad informáticos, sino de la educación y concienciación de los trabajadores.

Con la necesidad de proteger a la organización y la cantidad de puertas abiertas que supone cada empleado, se comenzaron a imponer medidas de concienciación a los miembros de las entidades que quedaban recogidas como Políticas de Concienciación en ciberseguridad. La función de estas disposiciones se centraba en la formación y capacitación de los trabajadores para desempeñar sus labores, atendiendo a su posición y sector de manera segura, para así evitar cualquier brecha de seguridad.

La efectividad de estas actuaciones no solo es visible en un marco global, existen ejemplos que explican como la aplicación o no aplicación de estas políticas afecta al seguro rendimiento de la organización.

Si bien es cierto que el camino por recorrer se extiende en un largo periodo de tiempo, entidades pertenecientes a los sectores conocidos como Infraestructuras Críticas, obligados por ley a implementar este tipo de medidas, han experimentado una disminución de casos cuya conclusión se tradujera en la sustracción de datos sensibles o vulneración de las barreras de seguridad.

Los principales mediadores y ejecutores, los CISOS de las corporaciones, advierten de la situación y fomentan la instauración de estas medidas globales debido al efecto que provocaría un ataque dirigido a individuos sin conocimientos en la materia. Los mismos, destacan la importancia de que, todas las organizaciones con independencia del sector al que pertenezcan, deberían adoptar Políticas de Concienciación en ciberseguridad de manera continua y actualizada para así contener o evitar incidentes con un desenlace crítico.

9.2 Aportaciones del estudio

La finalidad principal de este estudio es suplir la brecha de información que existe actualmente en internet y hacer las veces de manual de carácter introductorio para representar la situación actual y poder condensar la información que se encuentra dispersa. También, supone un análisis tanto global como focalizado de resultados y, por último, aporta valoraciones de profesionales en el ámbito, que están viviendo la evolución que se está produciendo en el entorno actual.

Esta pequeña guía informativa cuenta con objetos visuales para complementar la información y resultar más sencillo a la hora de revisarlo y poder hacerse una idea de la situación que se vive actualmente y como se podría modificar. A su vez, incluye recomendaciones, muchas de las cuales están orientadas a herramientas de Analytics, para así automatizar procesos y encontrar rutas de evolución.

Debido al tema sobre el que trata, la misma puede servir para diferentes ámbitos fuera del entorno laboral, al poder extrapolarse a diversos aspectos del día a día debido al grado de conectividad que está presente en numerosas instancias. Tanto las prácticas, como los resultados que aporta este trabajo, dejan entre ver como el factor humano es cada vez más vulnerable y eso se traduce a su vez en una necesidad de conocimiento en las tareas cotidianas que se puede obtener de esta guía.

Consideraciones finales

Como todo trabajo de investigación se ha procedido con el mayor rigor posible, nutriéndolo de fuentes fiables conectadas con concordancia y cohesión. Se ha tratado de revisar de manera cautelosa el escrito lo que ha permitido ratificar que a primera vista se trata de un trabajo soportado por literatura determinante. Sin embargo, no es posible asegurar en su totalidad que no exista alguna contingencia, propia tanto de la literatura expuesta como de los datos analizados. Se ha procurado que las ideas planteadas se expongan de manera coherente y siguiendo un metódico orden. Se ha tratado de adecuar la metodología al objeto de estudio y a la falta de información que se presenta sobre el tema. Por ello, se ha procedido a relacionar fundamentos de diferentes fuentes para obtener un resultado respaldado por la triangulación de los datos que se ha llevado a cabo. También agradecer a aquellos que han participado en este trabajo tanto aportando conocimiento y visiones actuales del problema, como dirigiendo el enfoque del proyecto general y aportando sugerencias significativas.

Muchas gracias.

Bibliografía

AEPD. (2019). *Brechas de seguridad de datos personales: qué son y cómo actuar*. Aepd.es. https://www.aepd.es/prensa-y-comunicacion/blog/brechas-de-seguridad-de-datos-personales-que-son-y-como-actuar

AEPD. (2021). *Guía para la notificación de brechas de datos personales*. Aepd.es. https://www.aepd.es/documento/guia-brechas-seguridad.pdf

Aggity. (2023). *Concienciación en Ciberseguridad*. Aggity. https://aggity.com/concienciacion-en-ciberseguridad/

Araujo, A. (2021). ISO 27001: *¿Cómo crear el plan de concientización y capacitación de tu empresa?* Hackmetrix Blog. https://blog.hackmetrix.com/plan-de-concientizacion-y-capacitacion-seguridad/

Bodnar, D. (2020). *Ingeniería social y cómo protegerse*. Avast. https://www.avast.com/es-es/c-social-engineering

Castillo, M. Á. (2022). *El factor humano como clave de éxito frente a los ciberataques*. Open3s. https://www.open3s.com/factor-humano-en-los-ciberataques-blog/

Ciberseguridad. (2019). *Plan de concienciación de seguridad informática*. Ciberseguridad. https://ciberseguridad.com/normativa/espana/medidas/plan-concienciacion/

Egan, G. (2023). *Consejos para mejorar la concienciación de ciberseguridad*. Proofpoint. https://www.proofpoint.com/es/security-awareness/post/security-awareness-training-best-practices-consider

ENISA. (2017). *Cyber Security Culture in organisations*. http://file:///C:/Users/cfvfe/Downloads/WP2017%20O-3-3-1%20Cyber%20Security%20Cultures%20in%20Organizations.pdf

FNC. (2021). *INFORME SOBRE LA CULTURA DE LA CIBERSEGURIDAD EN ESPAÑA*. https://www.seguritecnia.es/revistas/seg/documentos/informe-cultura-de-la-ciberseguridad-en-espa%C3%B1a-foro-nacional.pdf

Fortinet. (2022). 2022 *Cybersecurity Skills Gap*. Fortinet.com. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf?utm_source=pr&utm_campaign=report-2022-skills-gap-survey

Fortinet. (2023). *DoS vs. DDoS*. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/dos-vs-ddos

Fortinet. (2023). *Reporte de Brecha de Habilidades en Ciberseguridad a Nivel Mundial 2023*. Fortinet.com. https://global.fortinet.com/ai-la-lp-es-ap-reporte-ciberseguridad-mundial-2023

García, A. (2022). *Ataques cibernéticos: causas, tipos y consecuencias*. Worldsys. https://www.worldsys.co/ataques-ciberneticos-tipos-causas-y-consecuencias/

García, M. P. (2022). *Con estos ataques nos roban las contraseñas, ¡aprende a evitarlos!* Incibe.es. https://www.incibe.es/empresas/blog/estos-ataques-nos-roban-las-contrasenas-aprende-evitarlos

Garcia, Y. (2023). *Qué es un CISO: Conoce sus funciones principales*. Thinking for Innovation. https://www.iebschool.com/blog/que-es-un-ciso-tecnologia/

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). *Assessing MITRE ATT&CK risk using a cyber-security culture framework*. Sensors. https://doi.org/10.3390/s21093267

Greenlee, M. (2023). *The role of human resources in cybersecurity*. Security Intelligence. https://securityintelligence.com/articles/role-human-resources-cybersecurity/

Guillén, C. (2018). *Tres recomendaciones para reforzar la concienciación en seguridad de las organizaciones*. Entelgy.com. https://www.entelgy.com/divisiones/innotec-security/innotec-security-actualidad/en-los-medios-innotecsecurity/concienciacion-en-seguridad

IBM. (s. f.). *¿Qué es la ingeniería social?* Ibm.com. Recuperado 8 de noviembre de 2023, de https://www.ibm.com/es-es/topics/social-engineering

INCIBE. (2019). *Cinco herramientas indispensables para formar y concienciar en ciberseguridad en las empresas*. Incibe.es. https://www.incibe.es/empresas/blog/5-herramientas-indispensables-formar-y-concienciar-ciberseguridad-las

INCIBE. (2020). Gl*osario de términos de ciberseguridad, Una guía de aproximación para el empresario*. Incibe.es. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

INCIBE. (2020). *Guía de ciberataques*. Incibe.es. https://www.incibe.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

INCIBE. (2020). *Las 7 fases de un ciberataque. ¿Las conoces?* Incibe.es. https://www.incibe.es/empresas/blog/las-7-fases-ciberataque-las-conoces

INCIBE. (2020). *Luchando contra la ingeniería social: el firewall humano.* Incibe.es. https://www.incibe.es/empresas/blog/luchando-ingenieria-social-el-firewall-humano

INCIBE. (2022). *CyberEx España*. Incibe.es. https://www.incibe.es/incibe-cert/servicios-operadores/cyberex-espana

INCIBE. (2023). *Roles en ciberseguridad: desde el CEO a los usuarios finales*. Incibe.es. https://www.incibe.es/empresas/blog/roles-en-ciberseguridad-desde-el-ceo-los-usuarios-finales

Jiménez, M. M. (2022). *Ataques cibernéticos: causas, tipos y consecuencias*. Piranirisk.com. https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias

KasperskyLab. (2023). *ESTADÍSTICAS | Mapa en tiempo real de amenazas cibernéticas Kaspersky*. Kaspersky. https://cybermap.kaspersky.com/es/stats#country=129&type=OAS&period=w

Losa, L. (2023). *¿Qué es el Reglamento DORA y por qué es importante?* S2 Grupo. https://s2grupo.es/que-es-el-reglamento-dora-y-por-que-es-importante/

MacKay, J. (2018). *Cómo promover la concienciación sobre la ciberseguridad en su organización*. MetaCompliance. https://www.metacompliance.com/es/blog/cyber-security-awareness/how-to-promote-cyber-security-awareness-in-your-organisation

Malwarebytes. (2018). *¿Qué es el malware? Definición y cómo saber si está infectado*. Malwarebytes. https://es.malwarebytes.com/malware/

Mateus, F. (2022). *Los 7 elementos clave para mejorar el Programa de Concienciación en Ciberseguridad y su relación con los requisitos de Compliance*. Kymatio. https://blog.kymatio.com/es/6-razones-formas-de-mejorar-el-programa-de-concienciacion-en-ciberseguridad-y-su-relacion-con-los-requisitos-de-compliance/

MITRE ATT&CK®. (2015). Mitre.org. https://attack.mitre.org/

Muñoz, J. H. (2022). *Tipos De Ataques Informáticos: Causas, Consecuencias Y Prevenciones*. Servicios informáticos para empresas. https://salesystems.es/tipos-de-ataques-informaticos/

Orrantia, A. (2021). *¿Qué es un plan de concienciación de seguridad informática?* Com.mx. https://www.idric.com.mx/blog/post/que-es-un-plan-de-concienciacion-de-seguridad-informatica

Ortega, Á. (2021). *La importancia de la concienciación y formación en ciberseguridad*. GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/concienciacion-y-formacion-en-ciberseguridad/

Passeri, P. (2011). *DATA. HACKMAGEDDON*. https://www.hackmageddon.com/about/

Proofpoint. (2022). *¿Qué es el malware?* Proofpoint. https://www.proofpoint.com/es/threat-reference/malware

PWC. (2020). *Informe del estado de cultura de ciberseguridad en el entorno empresarial*. Pwc.es. https://www.pwc.es/es/publicaciones/digital/informe-cultura-ciberseguridad.pdf

RAE. (2001). Rae.Es. https://www.rae.es/drae2001/concienciar

Sushir, T. (2023). *¿Cómo utilizar el cortafuegos humano en su estrategia de ciberseguridad?* Geekflare. https://geekflare.com/es/human-firewall-explained/

ThriveDX. (2022). *2022 Gloabl Cibersecurity Awareness Training Study*. Thrivedx.com. https://thrivedx.com/resources/downloads/22-cybersecurity-awareness-training-report

Tuñon, R. (2023). *Los 10 mandamientos de la concienciación en ciberseguridad*. Kymatio. https://blog.kymatio.com/es/los-10-mandamientos-de-la-concienciacion-en-ciberseguridad/

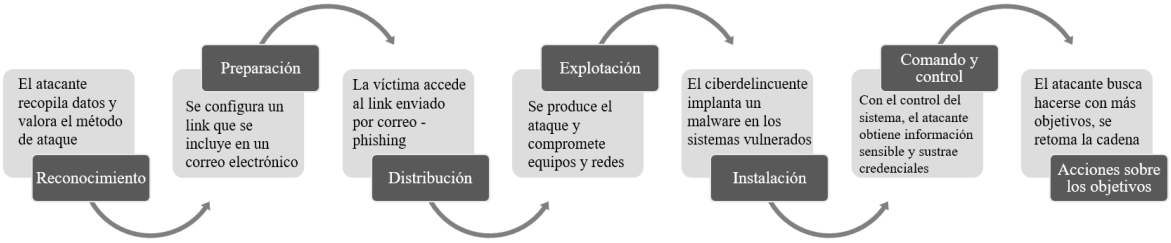
UEStudio. (2023). *Las pymes serán uno de los principales objetivos de los ciberataques en 2023*. Compartiendo Conocimiento. https://compartiendoconocimiento.elmundo.es/las-pymes-seran-uno-de-los-principales-objetivos-de-los-ciberataques-en-2023

Valenzuela, C. G. (2023). *Qué es un ataque de triple extorsión de ransomware, la nueva tendencia entre los ciberdelincuentes*. Computer Hoy. https://computerhoy.com/ciberseguridad/ataque-triple-extorsion-ransomware-nueva-tendencia-ciberdelincuentes-1200866

Anexos

Anexo 1

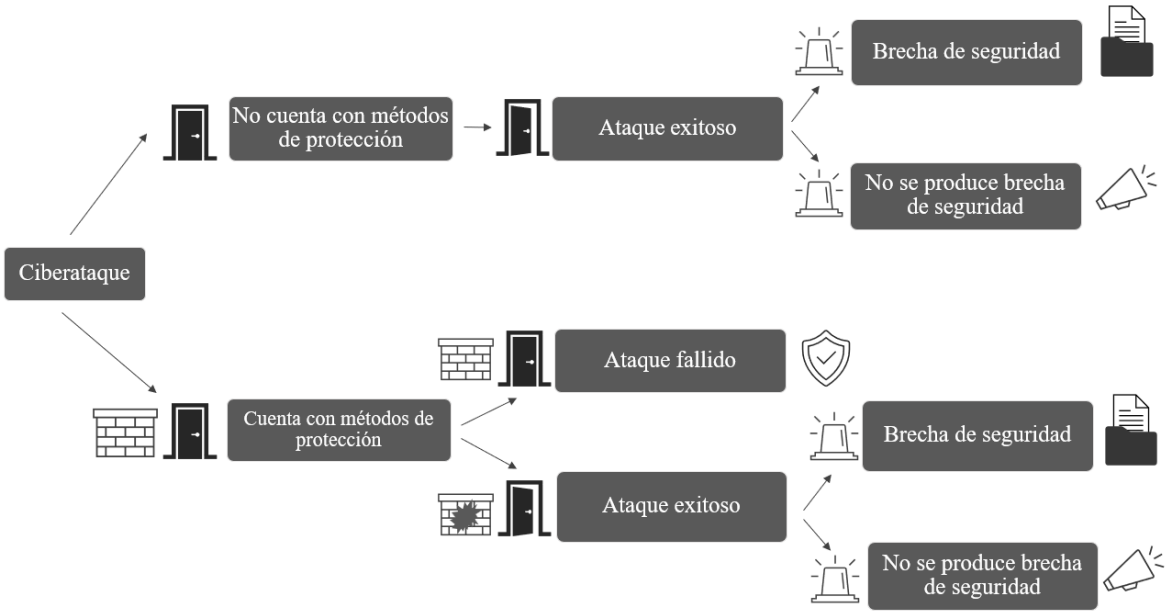
Ejemplo de la "Ciber Kill Chain" el ciclo de vida de un ciberataque



Fuente: Elaboración propia

Anexo 2

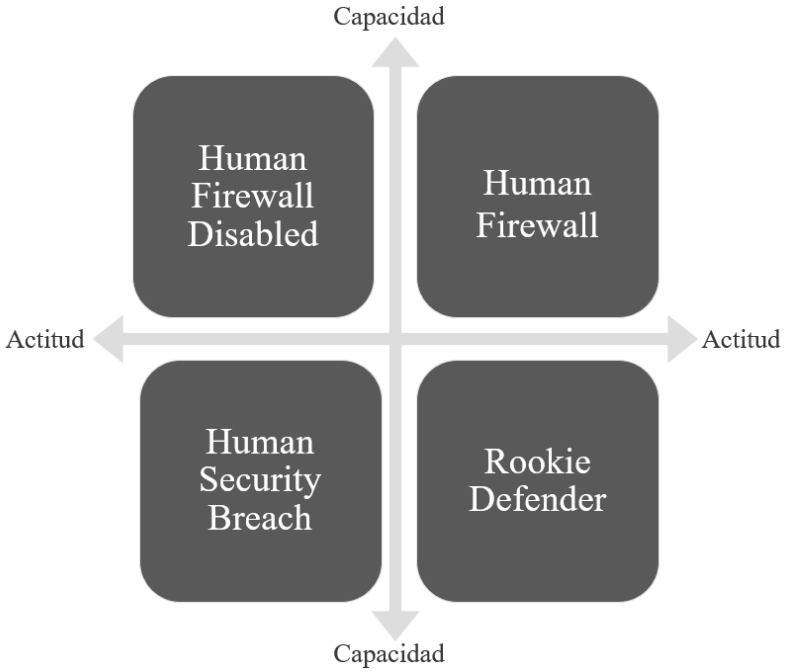
Consecución para que se produzca una brecha de seguridad



Fuente: Elaboración propia

Anexo 3

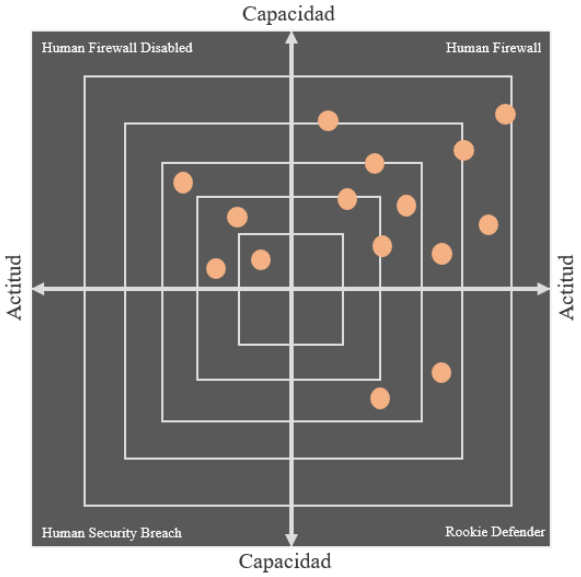
Matriz de medición de la cultura en ciberseguridad de los empleados (atendiendo a actitud y capacidad y con los perfiles)

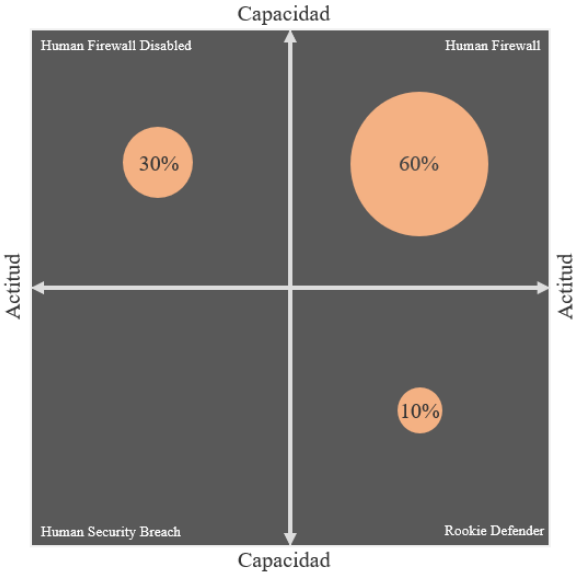


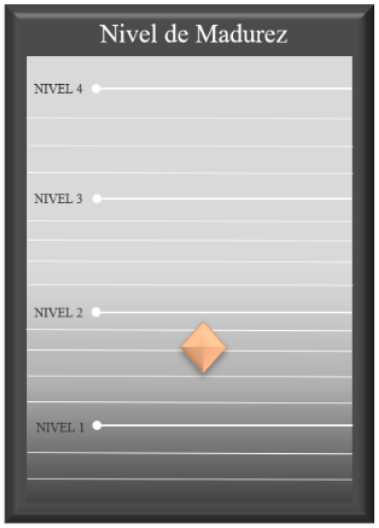
Fuente: Elaboración propia basado en el Marco de cultura en ciberseguridad MITRE (Georgiadou et al., 2021a)

Anexo 4

Ejemplo del uso de la Matriz de Medición de la madurez de la cultura en ciberseguridad y la clasificación por niveles







Fuente: Elaboración propia basado en el Marco de cultura en ciberseguridad MITRE (Georgiadou et al., 2021a)