Agencia Estatal
de Seguridad Aérea

Formación de Concienciación en Seguridad de la Información (CIBERSEGURIDAD)

F-DEA-CDO-10 4.0
AGENCIA ESTATAL DE SEGURIDAD AÉREA

ÍNDICE

1. INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

Objetivo: Introducir los conceptos básicos y algunas definiciones. Ofrecer ejemplos de ciberataques reales. Conocer los organismos que tratan los asuntos de ciberseguridad en España.

1.1. Conceptos Básicos

Seguridad de la información y seguridad informática son dos conceptos relacionados pero distintos. A continuación, se explican las diferencias más significativas:

Seguridad Informática:

La seguridad informática se enfoca en la protección de la infraestructura tecnológica, incluyendo redes, sistemas operativos, computadoras y otros componentes informáticos.

Los responsables de la seguridad informática son el equipo de seguridad del departamento de IT o ICT. Su tarea es asegurar la confidencialidad, integridad y disponibilidad de la información digitalizada.

Ejemplos de seguridad informática incluyen aislar áreas de la red con virus, poner en cuarentena computadoras infectadas y aplicar medidas técnicas para proteger los sistemas.

Seguridad de la Información (SI):

La seguridad de la información abarca toda la información, independientemente de si está en formato digital, papel o de otra naturaleza. Busca proteger la información confidencial desde una perspectiva física y del entorno, así como el control de acceso. Incluye tanto la protección de archivos físicos como bases de datos electrónicas. Es más amplia que la seguridad informática y también aborda aspectos no digitales.

Como resumen, mientras la seguridad informática o ciberseguridad se centra en la protección de sistemas digitales, la segunda, seguridad de la información. abarca todo tipo de información y su contexto.

Ciberseguridad

En muchas ocasiones se asocia o no se diferencia el término “Ciberseguridad” al concepto de “Seguridad de la Información”, se usan indistintamente. Sin embargo, esto no es correcto.

La seguridad de la información es el paraguas que abarca el resto de disciplinas, la protección de la información es el libro y la ciberseguridad es un capítulo dentro de ese libro.

La seguridad de la información abarca las medidas y actividades que intentan proteger los activos de información, es decir, la protección de la información o datos que tienen valor para una organización, a través de la reducción de riesgos y mitigando las amenazas posibles.

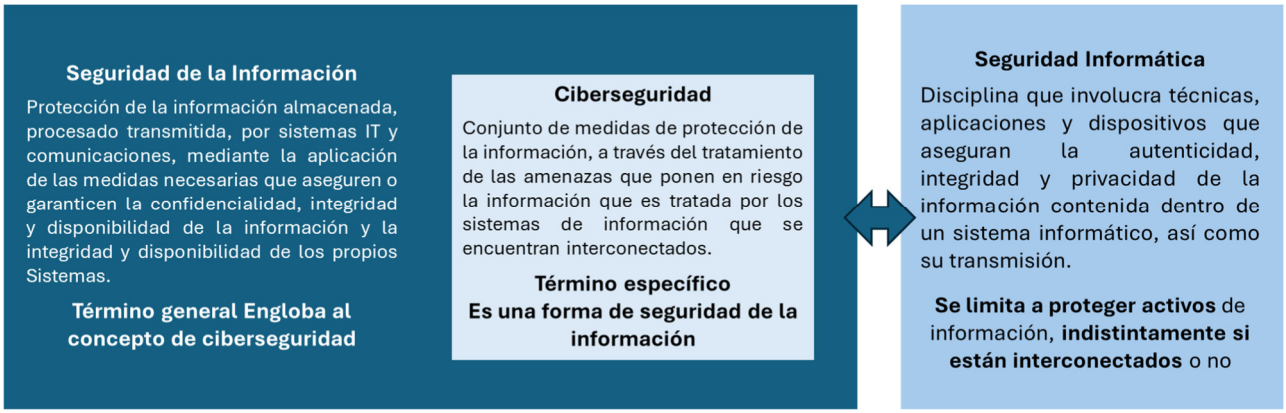
Mientras que la Ciberseguridad, tiene como foco principal la protección de la información digital de los sistemas ara ello se vale de tecnologías y prácticas de ataque contra malware y otras amenazas de los adversarios de la seguridad digital. En contraste, la seguridad de la información contempla aspectos defensivos para proteger los sistemas de información que están interconectados. Por ello, se puede considerar que la ciberseguridad está comprendida dentro de la seguridad de la información.

Como resumen, destacamos que la Seguridad de la información se refiere a la información, independientemente del formato, que abarca los documentos en papel, los documentos en formato digital o intelectual en la mente o conocimientos de las personas, y las comunicaciones verbales o visuales. Por otro lado, la Ciberseguridad, tiene que ver con la protección digital de activos, desde las redes de hardware e información que es tratada por los sistemas de información interconectados hasta software, servicios, etc.

El tercer concepto sería la seguridad informática, que se parece mucho a la ciberseguridad, la diferencia recae principalmente en que la ciberseguridad se centra en elementos interconectados. De hecho, hay quien llega a considerarlo la misma materia.

Otros aspectos a destacar sobre la Seguridad de la Información:

- Tiene un alcance mayor que la Ciberseguridad, ya que la seguridad de la información quiere proteger la información en todos los estados o formas, de los diferentes tipos de riesgos a los que se enfrentan.
- Su objetivo es proteger la información de riesgos que puedan afectar a los activos de información en formato digital y los sistemas informáticos que los procesan y almacenan, indistintamente si están interconectados o no.
- Se sustenta de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información
- Involucra la aplicación y gestión de medidas de seguridad, además de la aplicación y gestión de medidas de seguridad apropiadas para la protección de la información
- A modo de resumen, la seguridad de la información se refiere a la información, sin tener en cuenta el formato en la que esta se soporte (digital, físico o intelectual). Por otro lado, la ciberseguridad, se refiere a la salvaguarda digital de activos, bien sea hardware, software, información, sistemas interconectados, servicios, etc.



1.2. Características de la Información. Dimensiones de la SI.

Lo que se trata de preservar y/o proteger con respecto a la información son las tres características siguientes:

CONFIDENCIALIDAD: propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Debemos entender que la confidencialidad es parte principal de los activos de una empresa y como tal debe ser protegida con medios técnicos y legales contra accesos no autorizados.

Para garantizar la confidencialidad también se deben utilizar mecanismos de cifrado y de seguridad de la información. Los protocolos de cifrado garantizan dicha confidencialidad durante el tiempo necesario para descifrar el mensaje.

El establecimiento de pactos de confidencialidad con trabajadores y terceras empresas permitirá proteger la información corporativa confidencial. El incumplimiento de estos pactos puede suponer que se emprendan acciones legales y reclamaciones e indemnizaciones por daños y perjuicios.

Medios de protección de la confidencialidad:

Algunos medios de protección de la confidencialidad pueden ser:

- Limitar el acceso a la información confidencial, es decir, solo personal que por su cargo o función deba tener acceso a esos documentos. No hacerla extensiva a toda la organización y disponer de la trazabilidad de acceso oportuna en caso de producirse algún problema.
- Establecer contraseñas o permisos de accesos.
- Realizar copias de seguridad que eviten la pérdida de información.

El acuerdo de confidencialidad: Cuando se firma un pacto o acuerdo de confidencialidad debemos establecer unos puntos de obligado cumplimiento entre las partes, como, por ejemplo:

- Especificar claramente qué se entiende por información confidencial, pudiendo establecer el deber de guardar secreto respecto a una determinada información.
- Establecer claramente los recursos, medios o información que se ponen a disposición de las partes para salvaguardar la confidencialidad.
- Establecer el deber de actuar fielmente en cuanto a la conservación, almacenamiento, transporte, etc., objeto del acuerdo.
- Establecer la obligación de devolver toda la información confidencial a la que se ha tenido acceso durante la relación laboral. Esta obligación de secreto suele tener una vigencia establecida en el acuerdo.
- También se ha de informar de las consecuencias que puede derivarse por el incumplimiento del acuerdo de confidencialidad. El Código Penal, en su artículo 197, establece penas de prisión por descubrir secretos o vulnerar la intimidad.

Cifrado: El cifrado es otro mecanismo utilizado para ayudar a garantizar la confidencialidad. Tenemos varias opciones para su implementación, como pueden ser:

- Cifrar el documento.
- Estableciendo contraseña o utilizando herramientas específicas.
- Cifrando la conexión. Cuando una conexión es cifrada, se añade una “s” a los protocolos de comunicación comúnmente utilizados, como pueden ser http y ftp, que se convertirían en https y sftp.
- HTTPS: protocolo seguro de transferencia de hipertexto, es la versión segura de HTTP.
- SFTP: Secure File Transfer Protocol; Protocolo Seguro de transferencia de ficheros.

INTEGRIDAD: propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada

Mediante el cumplimiento de la integridad se pretende que la información permanezca inalterada a menos que sea modificada por una persona autorizada y dicha modificación sea registrada, asegurando así su confiabilidad.

La violación de la integridad se lleva a cabo cuando se modifican o borran datos que son parte de la información, una vez esta ha salido de su origen. Es decir, la información recibida no coincide con la información enviada en su inicio.

Para supervisar y cumplir la integridad de la información se suele utilizar la firma digital, que no es otra cosa que una secuencia de caracteres que se adjunta al final del cuerpo del mensaje.

Una firma digital permite identificar inequívocamente a la persona que emite el mensaje, teniendo la seguridad de que el mensaje se encuentra exactamente igual que cuando fue emitido, proporcionando tanto identidad como integridad.

La firma digital aumenta la seguridad de las transacciones y nos aporta, entre otras, dos importantes ventajas:

- Integridad del mensaje: Demuestra la validez de la información y nos asegura que está libre de información falsa o modificada sin autorización.
- Requerimientos legales: Supone satisfacer algunos requerimientos legales y se encarga de cualquier aspecto legal en la transacción de documentos como, por ejemplo, contratos, nóminas, facturas, etc.

Por todo lo anterior, la firma digital es uno de los pilares fundamentales de la seguridad de la información.

DISPONIBILIDAD: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Los sistemas informáticos utilizados para almacenar y procesar la información, la seguridad y los canales de comunicación deben estar funcionando correctamente cuando se realicen solicitudes de acceso.

La alta disponibilidad es un asunto de diseño y su implementación asegura un cierto grado de continuidad de los sistemas en caso de caída de algún servicio. Para asegurar un entorno de alta disponibilidad se deben utilizar servicios de comunicaciones, de seguridad y equipamiento que permitan disponer de la información continuamente replicada.

La alta disponibilidad intenta tener en cuenta todos los posibles casos que puedan llegar a afectar a los servicios críticos de la empresa para así poder planificar un sólido plan de contingencias.

No solo tiene en cuenta la caída de servidores, sino también de otros elementos hardware, como pueden ser routers, líneas de comunicaciones, conmutadores, etc. Servicios como el correo electrónico, bases de datos, presencia web, etc., utilizan mecanismos que ayudan a elevar la disponibilidad como clústeres, array de discos, equipos de alta disponibilidad, replicación de datos, redes de almacenamiento, enlaces redundantes, etc. para garantizar la disponibilidad establecida.

Array de discos: también conocido como RAID, es un conjunto de unidades de disco que aparecen lógicamente como si fueran un solo disco. Esta técnica incrementa el rendimiento y proporciona una

redundancia que protege contra el fallo de uno de los discos de la formación. Los más comunes son RAID1, RAID5 y RAID10.

Garantizar la disponibilidad implica también trabajar sobre la prevención y previsión de ataques al sistema de seguridad TI. Un ejemplo de amenaza que incide directamente sobre la disponibilidad de servicios es el conocido como ataque de denegación de servicio (DoS – Denied Of Service). Para prevenir este tipo de ataques, las empresas se pueden ayudar de sistemas de gestión que permitan conocer, administrar y minimizar posibles riesgos que atenten contra la seguridad informática.

La denegación de servicio es una amenaza, que se realiza utilizando equipos infectados (también conocidos como equipos esclavos) que son utilizados para realizar ataques predefinidos contra un mismo objetivo, normalmente sin que los propietarios de dichos equipos sepan lo que se está haciendo. Dichos equipos realizarán ataques simultáneos saturando los servicios la infraestructura objetivo, llegando a ralentizar su funcionamiento e incluso a inhabilitarla.

¿Pero cómo estas 3 propiedades dependen entre sí?

Estas tres propiedades de seguridad de la información dependen una de otra de la siguiente forma:

Si no se tiene CONFIDENCIALIDAD…

entonces la probabilidad de que se viole la integridad de la información aumenta potencialmente. Dando pie a que una persona no autorizada pueda modificar la información.

Si se modifica la INTEGRIDAD de los datos…

entonces la información o aplicaciones clave del negocio se verán afectados y no podrán dar el servicio esperado, lo que llevaría a un impacto en la disponibilidad.

Y es así como la confidencialidad, integridad y disponibilidad se convierten en un engrane importante para la seguridad de la información, en donde si alguno de estos elementos falla la consecuencia impacta a todos.

Es importante señalar que el impacto a cualquiera de las tres dimensiones no siempre es derivado de un ciberataque. Puede deberse a un fallo humano, o al desconocimiento.

En algunos textos regulatorios, incluido el **Esquema Nacional de Seguridad** se habla de otras dos características más de la información:

- **Autenticidad,** o no repudio que hace referencia a la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación
- **Trazabilidad,** propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

1.3. Conceptos relacionados con el Riesgo y la Protección de la Información

VULNERABILIDAD: Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma. *(En el Apartado 3 se desarrolla)*

AMENAZA: Evento con potencial que aprovecha una vulnerabilidad afectando negativamente a las operaciones de una organización o a sus activos. Desde el punto de vista de una organización pueden ser tanto internas como externas, intencionales como no intencionales. *(En el Apartado 4 se desarrolla)*

CIBERATAQUE: Evento con potencial que aprovecha una vulnerabilidad afectando negativamente a las operaciones de una organización o a sus activos. Desde el punto de vista de una organización pueden ser tanto internas como externas, intencionales como no intencionales.

Un ciberataque es un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u otra organización. Ahí tenéis la definición que aparece en la guía del CCN-STIC 401.

Los ataques más comunes son: malware de distintos tipos, denegaciones de servicio, ataques de día cero, inyección SQL, phishing, tunelización de DNS. También se debe hablar de las amenazas persistentes avanzadas.

- **Malware:** también llamado software o código dañino, es un término general para denominar una variedad de software hostil o intrusivo cuya función es dañar el sistema o causar un mal funcionamiento, tanto por pérdida de datos como por pérdida de productividad.

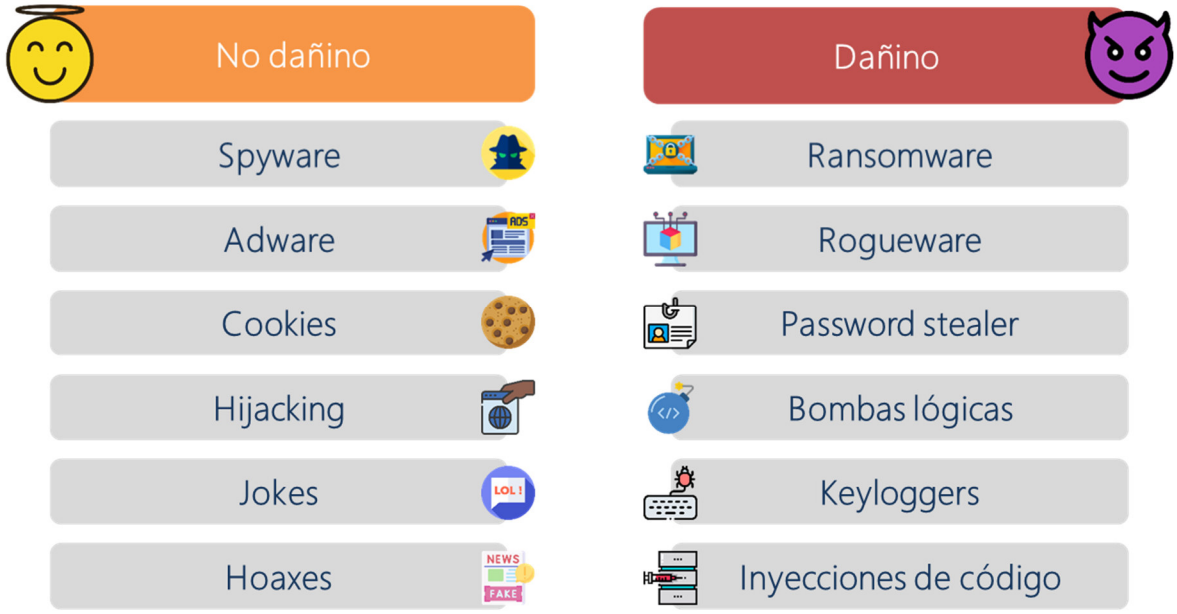


Ilustración 1. Ejemplos de Malware según sus acciones

- **DoS:** Un ataque de denegación de servicio satura los sistemas, los servidores o las redes con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede completar las solicitudes

legítimas. Los atacantes además pueden usar múltiples dispositivos comprometidos para lanzar un ataque.

- **Ataques de día cero**: es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto. Este puede impactar después del anuncio de una vulnerabilidad en la red, pero antes de que se implemente un parche o solución. Los atacantes apuntan a la vulnerabilidad divulgada durante esta ventana de tiempo. La detección de amenazas a la vulnerabilidad de día cero requiere de atención constante. El de solarwinds hace relativamente poco.

- **Inyección SQL:** Una inyección de lenguaje de consulta estructurado (SQL) ocurre cuando un atacante inserta un código malicioso en un servidor que usa el SQL y fuerza al servidor para que revele información que normalmente no revelaría. El atacante puede efectuar la inyección de SQL simplemente enviando un código malicioso a un cuadro de búsqueda de un sitio web vulnerable.

- **Phishing:** La suplantación de identidad (phishing) es la práctica de enviar comunicaciones fraudulentas que parecen provenir de fuentes confiables, habitualmente a través del correo electrónico. El objetivo es robar datos sensibles, como información de inicio de sesión y tarjetas de crédito, o instalar malware en la máquina de la víctima.

- **Tunelización DNS:** La tunelización de DNS usa el protocolo DNS para comunicar tráfico que no pertenece al DNS por el puerto 53. Envía HTTP y otro tráfico del protocolo por el DNS. Hay varias razones legítimas para usar la tunelización de DNS. Sin embargo, también existen motivos maliciosos para usar los servicios de VPN de tunelización de DNS. Pueden usarse para encubrir tráfico saliente del DNS y ocultar datos que típicamente se comparten mediante una conexión a Internet. Para el uso malicioso, se manipulan las solicitudes del DNS a fin de exfiltrar los datos de un sistema comprometido a la infraestructura del atacante. También puede usarse para las retro llamadas de comando y control de la infraestructura del atacante al sistema comprometido.

- **Amenaza persistente avanzada**: también conocida por sus siglas en inglés, APT, es un conjunto de procesos informáticos sigilosos orquestados por un tercero (organización, grupo delictivo, una empresa, un estado...) con la intención y la capacidad de atacar de forma avanzada (a través de múltiples vectores de ataque) y continuada en el tiempo, un objetivo determinado (empresa competidora, estado...). Este malware es instalado usando exploits que aprovechan vulnerabilidades de la máquina objetivo. Para realizar la infección es habitual aprovechar vulnerabilidades de día cero y/o ataques de abrevadero (watter hole attack). Las APT se caracterizan por ser orquestadas con grupos organizados con grandes recursos, y gran interés en el objetivo del ataque y su información; mantener el control de la infraestructura de la víctima de forma continuada (hasta varios años) y hacer uso de varios vectores de ataque y persistencia para mantener el acceso.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Se denomina riesgo a la posibilidad de que un sistema sufra un incidente de seguridad y que una amenaza se materialice causando una serie de daños. Para medir el riesgo de un activo o sistema se debe asumir que existe una vulnerabilidad ante una amenaza. El riesgo es, por lo tanto, la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad existente.

1.4. Ciberataques al sector del transporte aereo

La Aviación Civil tiende hacia un mayor intercambio de información entre los distintos actores (aeropuertos, aerolíneas, proveedores de servicios de navegación aérea, entidades de la cadena logística, y en general entre estos y todo tipo de proveedores externos) y hacia la implementación de procesos automatizados para el control de sistemas, comunicaciones y almacenamiento de información. En esto la aviación civil y el transporte aéreo no se diferencian mucho de otros ámbitos de la vida y los negocios.

Cuanto mayor es el nivel de compartición de información y más numerosos los procesos automatizados, en paralelo, se potencian las posibilidades de ataques cibernéticos.

La amenaza de estos ataques contra la aviación civil, y aquellos no dirigidos específicamente a ella pero que también repercuten, evolucionan de manera de rápida y continua. Los cibercriminales actúan maliciosamente para perturbar las operaciones y robar información por razones políticas, financieras y de otra índole.

Nuestra industria - que incluye a los usuarios del espacio aéreo, los proveedores de servicios de navegación aérea, los operadores aeroportuarios, las autoridades de aviación civil y los fabricantes de equipos – es el blanco de este tipo de ataques por varios motivos, pero especialmente para obtener beneficios económicos y robar propiedad intelectual.

Según el informe sobre ciberseguridad en la aviación publicado por EUROCONTROL, en 2019, el 39% de los ataques fueron dirigidos a aerolíneas, el 21% a fabricantes, el 20% a proveedores de navegación y el 16% afectaron a aeropuertos. El 4% restante a autoridades. Las entidades de la cadena logística no aparecían en las estadísticas (aún)

Sin embargo, en el informe de ENISA sobre el Sector Transporte de Marzo de 2023, la situación ha evolucionado y los porcentajes se han repartido así:

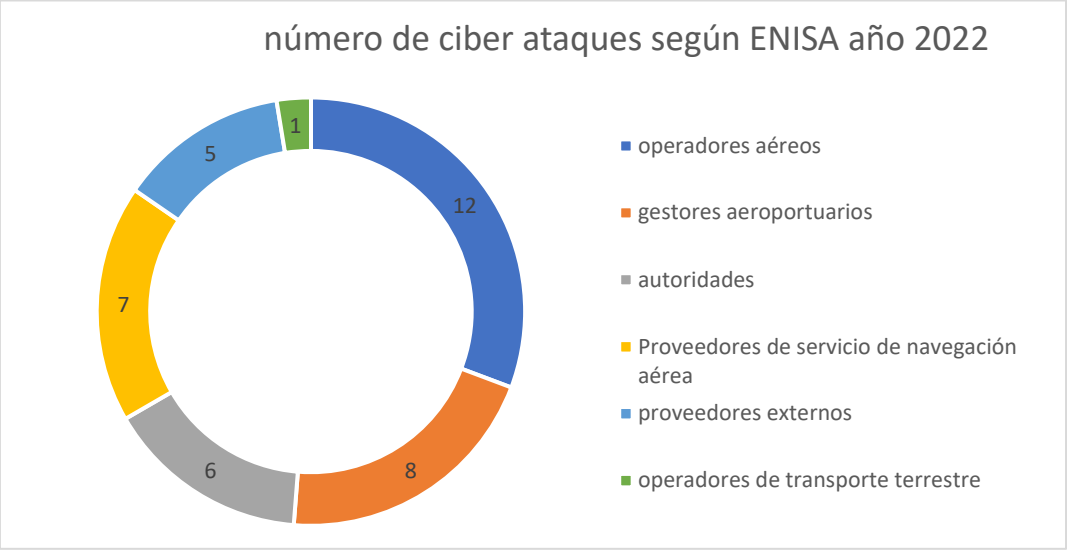


Ilustración 2. Nº de ciberataques sufridos por entidades de Aviación Civil en 2022. Fuente ENISA.

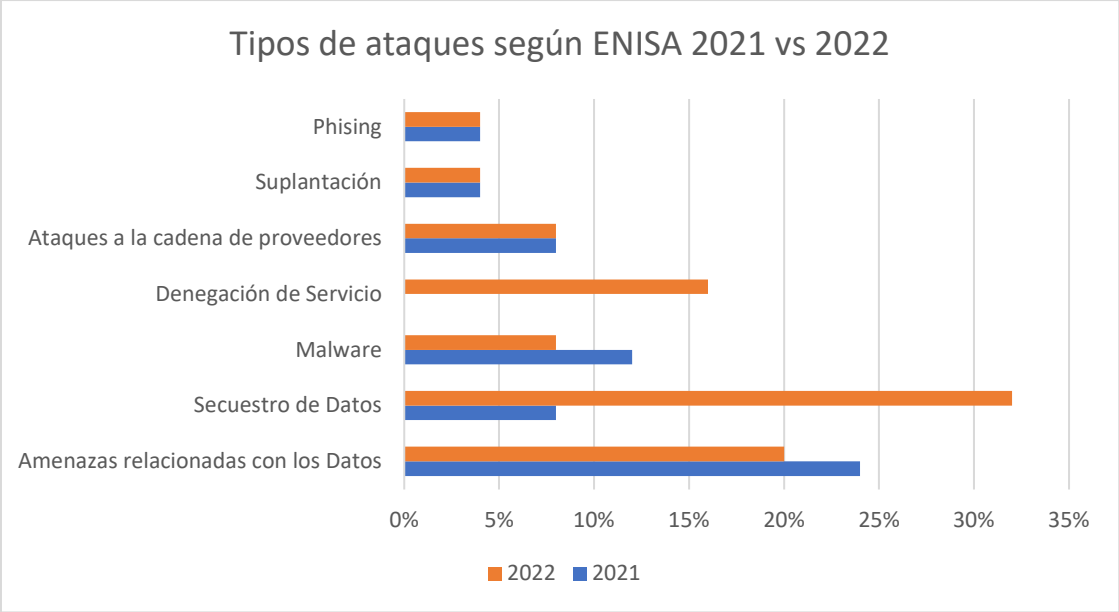


Ilustración 3. Tipos de Ataques de Ciberseguridad. Fuente ENISA.

Como curiosidad y cultura general, el famoso Grupo de DAVOS que se reúne todos los años en Suiza elabora un informe anual sobre los riesgos globales a los que se enfrente la económica mundial.

Merece la pena echar un vistazo a la posición que ocupa la ciberseguridad en este informe (cuarta posición):

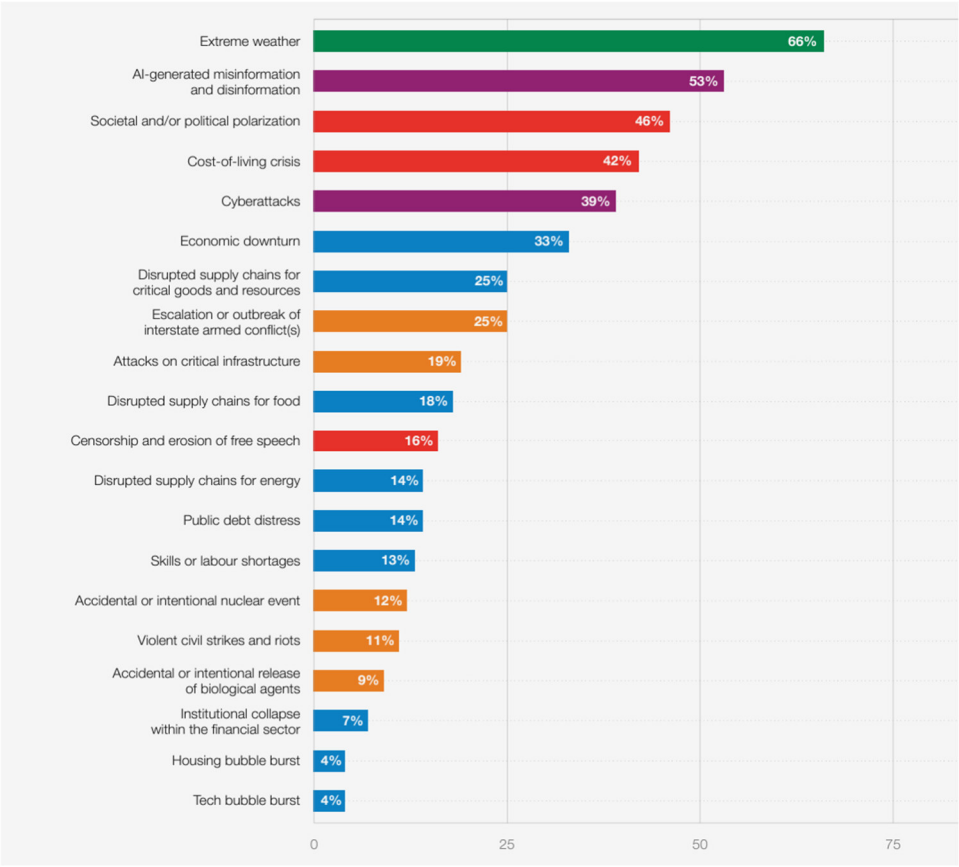


Ilustración 4. Riesgos Globales a los que se enfrenta la economía mundial. Fuente. Informe Foro Davos.

En un informe reciente de una organización líder en investigación de ciberseguridad, se informó que ha habido un aumento del 36 % en el número de ataques exitosos a la industria del transporte global en 2023 en comparación con 2022. Los métodos de ataque más populares fueron el uso de malware (35 %), explotación de vulnerabilidades (18%) y ataques a la cadena de suministro (8%). Según el informe, la industria del transporte se está volviendo cada vez más vulnerable a una variedad de amenazas cibernéticas que pueden interrumpir las operaciones de una empresa o posiblemente afectar la economía general de una nación.

Según el informe, en el 35% de los ataques exitosos al transporte, los atacantes utilizaron malware, y el ransomware encabezó la lista. En algunos ataques exitosos (8%), los atacantes pudieron dañar los sistemas comprometiendo a un tercero de confianza. Los atacantes utilizan activamente este método de ataque porque muchas organizaciones emplean contratistas, algunos de los cuales tienen defensas débiles. A menudo es más fácil piratear a estos contratistas para robar los datos de la organización objetivo u obtener acceso a la red del objetivo.

- **Febrero de 2024**: El 10 de febrero, Dark Storm Team y Anonymous Sudan lanzaron ciberataques contra aeropuertos estadounidenses, citando el apoyo de Estados Unidos a Israel en el actual conflicto de Gaza. Según se informa, los grupos llevaron a cabo ataques de denegación de servicio distribuido (DDoS) en el Aeropuerto Internacional de San Francisco (KSFO) y el Aeropuerto Internacional de Los Ángeles (KLAX). Por otra parte, el 10 de febrero, el grupo de ransomware LockBit 3.0 afirmó haber afectado a una aerolínea estadounidense. No se informaron impactos operativos en KSFO ni en KLAX. Estos ataques son comunes y tienen un impacto limitado o nulo para las víctimas previstas, pero continúan mostrando el enfoque de estos grupos de piratas informáticos en atacar la infraestructura de la aviación.

- **Febrero de 2024**, se informó que una base de datos fue exfiltrada del aeropuerto de Los Ángeles (KLAX) y anunciada en un foro público, que supuestamente contenía 2,5 millones de filas de datos adquiridos en una violación de seguridad. La información incluía datos personales de usuarios de propietarios de aviones privados y no afectó las operaciones de vuelo.

- **Febrero de 2024** la aerolínea nacional argentina Aerolíneas Argentina fue una víctima de un ataque de ransomware y se publicaron aproximadamente 50.000 registros de clientes. Finalmente, el 22 de febrero, el grupo de hackers proruso UserSec afirmó que tenía como objetivo el sector de la aviación letón, incluidos los sitios web del aeropuerto de Keipaja (EVLA), el aeropuerto de Jurmala (EVJA) y AirBaltic; no se observaron impactos operativos. Estos ataques son comunes y tienen un impacto operativo limitado o nulo, pero continúan mostrando el enfoque de estos grupos de piratas informáticos en atacar la infraestructura de la aviación.

- **Marzo de 2024**. El sitio web del aeropuerto de Copenhague fuera de línea en un ataque 'masivo' El 25 de febrero, un ciberataque tuvo como objetivo el sitio web del aeropuerto de Copenhague (EKCH) con un probable ataque de denegación de servicio (DDoS). A los pasajeros que volaban hacia o desde la capital danesa se les pidió que usaran una aplicación de teléfono inteligente para obtener actualizaciones sobre sus vuelos después de que el sitio web fuera desconectado. Un segundo ciberataque prorruso, NoName05716, tuvo como objetivo el sitio web del aeropuerto de Bornholm (EKRN) en Dinamarca el 25 de febrero; no se observaron impactos. Ese mismo mes, el grupo de hackers prorruso UserSec apuntó al sector de la aviación letón, incluidos los sitios web del aeropuerto de Keipaja (EVLA), el aeropuerto de Jurmala (EVJA) y AirBaltic; no se observaron impactos operativos. Es casi seguro que estos ataques son una respuesta a Dinamarca y otros países de la OTAN. Los países prometieron apoyo continuo y proporcionaron nuevos paquetes de ayuda letales y no letales a Ucrania. Estos ataques siguen poniendo de relieve el interés que tienen estos grupos de piratas informáticos por atacar la infraestructura de aviación de los socios de Ucrania en la OTAN.

- **Marzo 2024**: Duty Free AmericasUSPER atacado por Black Basta Ransomware Group La cadena minorista de viajes libres de impuestos Duty Free AmericasUSPER (DFA) fue recientemente atacada por el grupo Black Basta Ransomware. La banda de rescate vinculada a Rusia afirma haber robado alrededor de 1,5 terabytes de información confidencial de los sistemas de redes corporativas de DFA. La compañía tiene más de 250 tiendas dentro de aeropuertos y puertos marítimos en EE. UU. y otros países. En el presunto ataque, Black Basta informa haber robado archivos de múltiples departamentos, incluidos contabilidad, finanzas, legal y recursos humanos, incluidas grandes cantidades de datos confidenciales de los empleados. En su publicación, Black Basta muestra imágenes de pasaportes, tarjetas de seguro social, tarjetas de crédito y licencias de conducir como parte de la información que han obtenido. Black Basta ha sido vinculado a la banda de ransomware Conti, afiliada a Rusia, que ha logrado en los últimos años obtener millones de dólares en pagos de rescate. Si esta afirmación es válida y la información se vende, podría usarse para permitir futuros ataques cibernéticos dentro del sector de la aviación aprovechando los datos personales de los viajeros y empleados del aeropuerto para ataques dirigidos de ingeniería social. Estos ataques podrían tener un impacto ascendente si esas identidades se aprovechan para obtener acceso privilegiado para compromisos adicionales en organizaciones relacionadas con la aviación.
- **Marzo 2024** – Air Europa afirma que los datos de sus clientes probablemente estén comprometidos. El 22 de marzo, funcionarios de la aerolínea española Air Europa afirmaron que los datos personales de los clientes podrían haber sido comprometidos durante un incidente de seguridad detectado en octubre de 2023. En un correo electrónico a los potencialmente afectados por la violación, la compañía afirmó que una investigación reveló el nombre, el documento de identidad y los datos del pasaporte. , podrían haberse filtrado fechas de nacimiento, datos de contacto y detalles nacionales. En el momento del ciberataque, que tuvo como objetivo el sistema de pago en línea de la aerolínea y reveló algunos detalles de la tarjeta de crédito del cliente, la aerolínea afirmó que no se había expuesto ninguna otra información. La compañía recomendó a los clientes cancelar cualquier tarjeta relevante utilizada en el sitio web de Air Europa para evitar un posible uso fraudulento de la información de los clientes.
- **Abril de 2024** El grupo cibernético iraní Handala afirmó haber violado los sistemas de radar de Israel y distribuido mensajes de texto amenazantes a través de Telegram a 500.000 ciudadanos israelíes. La violación supuestamente permitió a Handala enviar mensajes advirtiendo de ataques inminentes e instando a los ciudadanos a disentir contra el gobierno israelí. Estos mensajes aconsejaban a los ciudadanos israelíes que evacuaran sus ciudades para evitar posibles daños, añadiendo urgencia al afirmar: "Sólo tienen unas pocas horas para arreglar los sistemas".
- **Abril de 2024** La FAA suspendió todos los vuelos de Alaska Airlines, incluido Horizon Air pero excluyendo SkyWest, a petición suya el 17 de abril debido a un problema informático identificado. Se reconoció que el problema se debía a una mejora en su sistema de cálculo de peso y equilibrio. Como resultado, se reportaron al menos 7 salidas retrasadas desde el Aeropuerto Internacional de San Francisco (KSFO)
- **Abril de 2024**, el sitio web del aeropuerto de Frankfurt-Hahn (EDFH) en Lautzenhausen, Alemania, experimentó problemas de conexión el 4 de abril después de que un grupo de piratas informáticos prorruso UserSec reivindicara un ataque DDoS. No se observó ningún impacto operativo. Los ataques DDoS a los aeropuertos siguen poniendo de relieve la alta prioridad que los ciberatacantes otorgan a la infraestructura y las operaciones de la aviación
- **Mayo de 2024**, Alemania acusó a Rusia de lanzar ciberataques contra sus empresas aeroespaciales y de defensa, así como contra objetivos en otros países, advirtiendo que habría consecuencias no especificadas. Específicamente, el Ministerio del Interior alemán citó la explotación previa por parte

de APT28 de una vulnerabilidad entonces desconocida en Microsoft Outlook para comprometer múltiples cuentas de correo electrónico. La OTAN dijo que la campaña también se había dirigido a organismos gubernamentales, "operadores de infraestructura crítica" y otras entidades en Lituania, Polonia, Eslovaquia y Suecia. APT28 está estrechamente vinculado al Servicio de Inteligencia Ruso, que desde el inicio del conflicto en Ucrania ha buscado formas de aprovechar sus habilidades cibernéticas para interrumpir la ayuda letal a Ucrania. Los ciberactores vinculados a Rusia han llevado a cabo ciberataques contra la OTAN, empresas aeroespaciales y aeropuertos.

1.5. Organizaciones Competentes

1.5.1. Nacionales

La **Oficina de Coordinación de Ciberseguridad (OCC)** creada en 2014 es el órgano técnico de coordinación de la Secretaría de Estado de Seguridad en materia de ciberseguridad, hasta 2020 se denominaba Oficina de Coordinación Cibernética.

La OCC proporciona las **capacidades de coordinación técnica entre el CERTSI y los órganos subordinados de la Secretaría de Estado de Seguridad y las Fuerzas y Cuerpos de Seguridad del Estado** en lo que respecta a las competencias propias del Ministerio del Interior en el campo de la ciberseguridad. La OCC mantiene personal técnico permanentemente integrado en la estructura del CERTSI.

FUNCIONES:

- Asesorar al Secretario de Estado de Seguridad en materia de ciberseguridad, aportando la información estratégica y técnica necesaria para facilitar la toma de decisiones.
- Proporcionar un canal de alerta temprana permanente en lo relativo a vulnerabilidades, ciberamenazas y ciberataques.
- Establecer cauces de intercambio de información entre otros actores, públicos y privados, nacionales e internacionales.
- Desarrollar mecanismos de respuesta ante un ciberincidente que recaiga en los ámbitos competenciales del Ministerio del Interior, teniendo capacidades para:
- Enlazar con el CERTSI para establecer la respuesta técnica apropiada.
- Enlazar con la unidad tecnológica de las FCSE para iniciar la investigación y persecución del delito.
- **Autoridad competente en materia de seguridad de las redes y sistema de información de operadores críticos** conforme a la Ley 8/2011.

COMPETENCIAS:

Esta Oficina dispondrá de las necesarias capacidades de operación 24 horas al día, 7 días a la semana, con el fin de responder a las solicitudes de ayuda.

Responsabilizarse del intercambio de información sobre ciberdelitos con terceros países, y órganos internacionales y de la Unión Europea, cuando así se requiera por las autoridades competentes.

El **Centro Criptológico Nacional (CCN)** es el Organismo responsable de **garantizar la seguridad las Tecnologías de la Información y la Comunicación (TIC) en las diferentes entidades del Sector Público**, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

COMPETENCIAS:

- Normativa: Elabora y difunde normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de Tecnologías de la Información y Comunicación (TIC)1.
- Formación: Se encarga de formar al personal del sector público especializado en el campo de la seguridad1.
- Vigilancia: Vela por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia1.
- Desarrollo: Coordina la promoción, desarrollo, obtención, adquisición y puesta en explotación y uso de tecnologías de seguridad1.
- Evaluación: Valora y acredita la capacidad de los productos de cifra y de los sistemas para manejar información de forma segura1.
- Certificación: Constituye el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad, de aplicación a productos y sistemas en su ámbito.
- Ciberseguridad: Contribuye a la mejora de la ciberseguridad española, a través del CCN-CERT, afrontando de forma activa las amenazas que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país1.
- Relaciones: Establece las necesarias relaciones y firma los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

El Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el **desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.**

COMPETENCIAS:

Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

El **CCN-CERT** es la **Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN**, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

MISION:

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo **el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas**, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT.

INCIBE-CERT es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

En el caso de la gestión de incidentes que afecten a operadores críticos del sector privado, INCIBE-CERT está operado conjuntamente por INCIBE y OCC, Oficina de Coordinación de Ciberseguridad del Ministerio del Interior.

MISIÓN:

INCIBE-CERT es uno de los equipos de respuesta de referencia ante incidentes que se coordina con el resto de los equipos nacionales e internacionales para mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, reduciendo sus efectos en la seguridad pública.

Agencia de la Unión Europea para la Ciberseguridad (ENISA). Esta agencia tiene la misión de velar por un alto nivel común de ciberseguridad en toda Europa1. Fue creada en 2004 y reforzada por el Reglamento sobre la Ciberseguridad de la UE.

MISION:

Contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de Tecnologías de la Información y Comunicación (TIC) mediante programas de certificación de la ciberseguridad1. También coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del mañana en materia de ciberseguridad.

La **Agencia Estatal de Seguridad Aérea (AESA)** tiene varios cometidos relacionados con la seguridad en general y con la ciberseguridad en particular.

MISION:

Entre sus atribuciones está la supervisión de todas las entidades que aplican el Programa Nacional de Seguridad, PNS.

El PNS tiene varios preceptos relacionados con la seguridad de la información. Se destacan aquí:

Capítulo 1.

1.8.1. La autoridad competente velará por que los gestores aeroportuarios, las compañías aéreas y las entidades definidas en el programa nacional de seguridad de la aviación civil definan y protejan sus sistemas críticos de tecnología de la información y las comunicaciones y los datos críticos frente a ciberataques que pudieran afectar a la seguridad de la aviación civil.

1.8.2. Los gestores aeroportuarios, las compañías aéreas y las entidades definirán en su programa de seguridad, o en cualquier documento pertinente a que este haga referencia, los sistemas críticos de tecnología de la información y las comunicaciones y los datos críticos descritos en el punto 1.7.1.

El programa de seguridad, o cualquier documento pertinente a que este haga referencia, detallará las medidas para garantizar la protección frente a los ciberataques mencionados en el punto 1.7.1, así como para garantizar que estos son detectados, que se responde a ellos y que se subsanan sus efectos.

1.8.3. Las medidas detalladas para proteger dichos sistemas y datos frente a actos de interferencia ilícita se definirán, desarrollarán y aplicarán de conformidad con una evaluación del riesgo efectuada por el gestor aeroportuario, la compañía aérea o la entidad, según corresponda.

Capítulo 11.

11.2.8.1. Las personas que apliquen las medidas establecidas en el punto 1.7.2 tendrán las capacidades y aptitudes necesarias para llevar a cabo sus tareas de manera efectiva. Deberán ser conscientes de los ciberriesgos pertinentes, en la medida en que sea necesario.

11.2.8.2. Las personas que tengan acceso a los datos o los sistemas recibirán una formación laboral adecuada y específica, acorde con sus funciones y sus responsabilidades, que incluirá la toma de conciencia de los riesgos

pertinentes cuando su función laboral así lo requiera. La autoridad competente, autoridad u organismo establecido en el punto 1.7.4, deberá definir o aprobar el contenido del curso.

Por tanto, los auditores de AESA comprobarán en las instalaciones de la entidad:

- Que haya un Programa de Seguridad y que estén definidos los sistemas críticos (si los hubiera).
- Que se haya acometido un Análisis de Riesgos, y se hayan identificado medidas que mitiguen los riesgos.
- Que las personas estén debidamente seleccionadas y formadas en ciberseguridad, si aplican medidas o acceden a datos críticos según corresponda.

2. CULTURA Y POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN/CIBERSEGURIDAD DE UNA ENTIDAD

Objetivo: Que el personal sea consciente de su importancia y responsabilidades para garantizar un nivel adecuado de ciberseguridad en su entidad. Tener conocimiento de la política y normas de la entidad. Conocer los activos a proteger y el sistema de clasificación de la información.

2.1. Cultura de ciberseguridad

La seguridad no es un producto, algo que se pueda conseguir y una vez terminado, se tiene inmutable. Por el contrario, la seguridad son actividades continuas realizadas dentro de un plan sistemático que debe evaluarse continuamente. Es un proceso que comienza en la Alta Dirección y que debe incluir a todos los empleados, de manera que se sientan parte de algo, ya que muchas veces el factor humano suele ser el factor más débil.

La cultura de ciberseguridad es fundamental para proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas de IT de nuestra organización. También el resto de características, pero estas son las más importantes.

La estrategia a emplear dependerá del tamaño y complejidad de las actividades de cada empresa. Sin embargo, se considera que las siguientes actividades pueden resultar efectivas para fomentar una sólida cultura de ciberseguridad entre los empleados:

- Integrar la ciberseguridad en la misión y visión de la empresa: Reconocer la ciberseguridad como un valor central que impregna todas las acciones y decisiones de la organización.
- Destinar recursos para desarrollar e implementar estrategias de ciberseguridad y asegura que cada departamento comprenda su rol en la protección de los activos digitales
- Educar y generar concienciación general. Explicar la existencia y peligros de la ingeniería social.
- Entrenar al personal, realizando sesiones regulares de formación sobre ciberseguridad.
- Abordar temas como contraseñas seguras, uso adecuado de dispositivos y redes.
- Realizar simulacros de phishing para enseñar a los empleados a identificar correos electrónicos maliciosos y otros ataques.

- Establecer un calendario de formaciones para mantener a los empleados informados sobre las últimas novedades.
- Tener políticas claras y comunicación abierta, desarrollando políticas de ciberseguridad. Los empleados deben sentirse cómodos reportando incidentes o posibles amenazas. La transparencia es clave para construir una cultura sólida.

Fomentar una cultura de ciberseguridad implica un esfuerzo continuo. Proteger la información y los sistemas es responsabilidad de todos,

2.2. Políticas y procedimientos de seguridad de la información

La Alta Dirección de la entidad debe poner escrito la política a seguir en relación con la seguridad de la información.

En función el tamaño de la empresa el número y alcance de los procedimientos que se deriven de la política general puede ir en aumento.

A continuación, se ofrece un ejemplo sencillo de política de seguridad.

- Misión
- Ámbito de Aplicación
- Marco Normativo
- Principios básicos
- Requisitos mínimos de Seguridad
- Organización de la seguridad de la información en nuestra empresa
- Explicando los roles comités, responsables, y cómo se resuelven los conflictos
- Datos de carácter personal
- Análisis y Gestión de Riesgos
- Obligaciones del Personal
- Formación y Concienciación
- Relación con terceras partes y proveedores (con los que compartimos información o sistemas)
- Revisión de la Política
- Incumplimiento de la Política de Información

En relación con los procedimientos, algunos de los más importantes serían:

- Contraseñas seguras
- Firewalls y sistemas de detección de intrusiones
- Software antivirus y antimalware
- Seguridad de los dispositivos móviles y teletrabajo
- Navegación segura por internet
- Copias de seguridad de datos
- Autenticación de dos factores (2FA)
- Comunicación y Plan de respuesta a incidentes

2.3. Activos/Sistemas Críticos

Identificar los activos críticos no es una labor de los empleados a los que va dirigido este curso de concienciación, sino de la Alta Dirección de la Entidad, así como del Responsable de Seguridad de la Información.

Sin embargo, se ofrecen aquí unas nociones sobre lo que significa que un Activo sea crítico.

- **Activo:** componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la entidad. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

- **Activo o función crítica**: conjunto de procesos, actividades, sistemas y recursos necesarios para la consecución de fines de la aviación civil.

Este es un ejemplo y una lista no exhaustiva de sistemas y datos identificados como críticos desde la perspectiva de la seguridad de la aviación:

- Bases de datos de agentes regulados, consignadores conocidos, proveedores regulados y conocidos y otras entidades aprobadas o designadas que forman parte de la cadena de suministro segura;
- control de acceso para personas distintas de pasajeros, incluidos portones electrónicos y otras puertas, y sistemas de monitoreo de alarmas;
- Lectores de tarjetas de embarque, tanto en la entrada de la zona de operaciones/SRA como en la puerta de embarque.
- Lectores de pasaportes/identificaciones electrónicas
- Sistemas de vigilancia CCTV;
- Sistema de conciliación de pasajeros y equipaje; y
- Sistemas de detección y/o sistemas de detección de explosivos, ya sea que estén conectados en red o que funcionen en una configuración independiente;
- Base de datos y archivo de tarjetas de identificación aeroportuaria, incluidos, cuando corresponda, los expedientes de contratación, preempleo y verificación de antecedentes
- Base de datos y archivo de expedientes del personal relacionados con capacitaciones y certificaciones de seguridad.
- Documentación Restringida a la que sólo deben tener acceso las personas con necesidad de conocer.

Las preguntas que debemos hacernos son…

- ¿Maneja mi entidad este tipo de activos?
- ¿Los ha identificado?
- ¿Lo ha comunicado a la plantilla?
- ¿Cómo puedo yo proteger estos activos críticos como trabajador de la entidad?

2.4. Clasificación de la Información

La clasificación de la información es la principal línea de defensa para los datos e información, permitiendo prevenir la difusión a personas no autorizadas de la información de nuestra entidad (en adelante la Organización), ya sean empleados de la Organización o usuarios de empresas externas o colaboradores. Además, es importante realizar un correcto etiquetado de la documentación para conocer la confidencialidad de la información.

Por tanto, una adecuada clasificación y etiquetado de la información, es requisito indispensable para la adecuada gestión de la Seguridad de la Información en la Organización.

Toda aquella información que existe en la Organización documentos (procesos, procedimientos, IT…), notas de voz, vídeos, imágenes, correos, etc.) tanto en formato digital como en papel debe estar clasificada y su clasificación debe ser conocida por los empleados y terceros (proveedores) cuando estos sean usuarios de los Sistemas de Información de la Organización.

El Responsable de Seguridad de la Información puede establecer unas categorías lógicas y sencillas para distinguir los distintos niveles de protección de la información. En muchas entidades se atiende a este esquema de menor a mayor protección:

- **Uso público**: Información interna o externa, que no contiene restricciones y que puede ser consultada o accedida por cualquier persona. Una divulgación no autorizada de esta información causaría un impacto nulo a la Organización.
- **Uso interno**: Información que debe mantenerse dentro de la Organización para uso de todos los empleados y colaboradores. En el caso del personal externo de la Organización, estos deberán comprometerse a no divulgar dicha información sin previa autorización del propietario de esta. Una divulgación no autorizada tendría un impacto leve.
- **Restringida**: Información propia del desempeño de tareas o actividades, cuyo conocimiento y difusión se debe limitar a los departamentos y grupos de trabajo implicados en las mismas, sin ser accesible a todos los empleados y colaboradores de la Organización. Una divulgación no autorizada tendría un impacto significativo
- **Confidencial:** Información sensible que exclusivamente puede ser conocida y utilizada por determinadas personas. Contiene datos de gran relevancia sobre decisiones estratégicas y su divulgación, o uso no autorizado, podría dañar o poner en riesgo la seguridad e intereses de la Organización de forma casi irreversible.

Podría haber otra clasificación equivalente, con más o menos escalones en función de la complejidad de la organización. Además, dicha clasificación de la información afectará a todos los soportes de esta:

- Papel.
- Documentos digitales (Office365).
- Discos duros (internos y externos).
- Almacenamientos de copias de seguridad.
- Unidades USB.
- Tarjetas de memoria.
- CD/DVD.
- Bases de datos.

Los responsables de cada unidad de negocio deben clasificar la información que les es propia. Se ofrece a continuación un ejemplo:

Nombre Información (Alineado con el inventario de activos)	Clasificación de la Información	Departamento que propone
Claves de acceso a los sistemas de protección	Confidencial	
Listado de clientes	Uso Interno	
Listado de empleados, nóminas y otros datos personales	Restringida	
Listado de empleados formación	Restringida	
Procedimientos en general	Uso Interno	

Nombre Información (Alineado con el inventario de activos)	Clasificación de la Información	Departamento que propone
Procedimiento de Security en particular	Restringido	
Apartado del PNS que son aplicables a la entidad	Restringido	

NO solo clasificarla sino también sería recomendable etiquetarla y llevar un registro donde quedará guardada.

3. CONCEPTO DE VULNERABILIDAD Y SU IMPACTO ORGANIZACIONAL

Objetivo: Comprender el concepto de vulnerabilidad en ciberseguridad y que el personal puede introducir vulnerabilidades en el sistema.

Vulnerabilidad: Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

Las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas. En términos de seguridad de la información, es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.

Las vulnerabilidades pueden clasificarse en dos tipos:

- Las **vulnerabilidades físicas** son las que van a afectar a la infraestructura de la organización de manera física y se pueden mencionar en este tipo de clasificación a los desastres naturales (por ejemplo, encontrarse en una zona de alto riesgo de terremotos), ya que estos pueden afectar a la disponibilidad de los sistemas. Otra de las opciones físicas son los controles de acceso, en muchas ocasiones no se establecen los controles de acceso a infraestructuras críticas.
- Las **vulnerabilidades lógicas** son las que van a afectar directamente la infraestructura y el desarrollo de la operación de esta. Estas a su vez se pueden clasificar en vulnerabilidades de configuración, actualización y desarrollo.

Algunas de las vulnerabilidades a destacar son:

- Error en la gestión de recursos: una aplicación permite que se consuman un exceso de recursos afectando a la disponibilidad de los mismos.
- Error de configuración: problemas de configuración de software o de servidores. Dentro de estos se pueden mencionar, por ejemplo, las contraseñas débiles, usuarios con demasiados privilegios e inclusive la utilización de protocolos de encriptación obsoleto.

- Permisos, privilegios y control de acceso: fallos en la protección y gestión de permisos que permiten el control de acceso a quién no debe a lo qué no debe.
- Validación de entrada: fallo en la validación de datos introducidos en aplicaciones puede ser una vía de acceso de un ataque
- Salto de directorio: fallo en la depuración de un programa, en la validación de caracteres especiales que permite el acceso a directorios o subdirectorios no deseados
- Factor humano: negligencias causadas generalmente por la falta de formación y concienciación. El personal es considerado el más débil de la cadena

En resumen, las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas.

Es decir, los atacantes, de forma intencionada, utilizan

- DEBILIDADES
- FALLOS del sistema

Para atacar alguna, todas o una combinación de las dimensiones de la Información

- Integridad
- Disponibilidad
- Confidencialidad

Algunas de las vulnerabilidades que pueden afectar la **INTEGRIDAD** de la información incluyen:

- Errores de software o hardware: Fallos en el diseño o configuración que permiten modificaciones no autorizadas.
- Intercepción de datos: Ataques que capturan o modifican datos durante su transmisión.
- Malware: Software malicioso diseñado para dañar o alterar datos.
- Manipulación de usuarios: Técnicas como la ingeniería social que engañan a los usuarios para que revelen información o realicen acciones que comprometan la integridad de los datos.
- Falta de controles adecuados: Ausencia de medidas de seguridad que protejan contra la alteración no autorizada.
- Descargas e instalaciones desde internet no controladas: Pueden introducir malware que comprometa la integridad

Algunas de las vulnerabilidades más comunes que permiten atacar la **DISPONIBILIDAD** de la información incluyen:

- Falta de controles de seguridad: Debilidades en los controles de seguridad pueden permitir ataques que interrumpan los servicios.
- Sistemas y aplicaciones desactualizadas: Las versiones antiguas pueden contener fallos de seguridad que afecten la disponibilidad.
- Gestión inadecuada del cambio: Cambios no controlados en el sistema pueden causar inestabilidad y caídas.
- Respaldo inapropiado o irregular: La falta de copias de seguridad puede resultar en pérdida de datos durante una interrupción.
- Protección física inapropiada: El daño físico a los equipos puede causar pérdida de acceso a la información.

- Falta de formación y conciencia sobre seguridad informática: Los usuarios no informados pueden cometer errores que afecten la disponibilidad.
- Falta de backups: Tener solo una copia de la información aumenta el riesgo de pérdida de acceso a los datos.
- Conexiones a redes públicas desprotegidas: Pueden ser explotadas para ataques que comprometan la disponibilidad.

Vulnerabilidades que permiten atacar la **CONFIDENCIALIDAD** de la Información

- Falta de controles de seguridad: Debilidades en los controles de seguridad pueden permitir accesos no autorizados.
- Sistemas y aplicaciones desactualizadas: Pueden contener fallos de seguridad que faciliten el acceso no autorizado a la información.
- Interfaz de usuario complicada: Puede llevar a errores de configuración que comprometan la confidencialidad.
- Contraseñas predeterminadas no modificadas: Son un blanco fácil para los atacantes.
- Eliminación de medios de almacenamiento sin eliminar datos previamente: Puede permitir la recuperación de datos sensibles.
- Inadecuada gestión y protección de contraseñas: La gestión insegura de contraseñas puede llevar a su compromiso.
- Falta de políticas de acceso o política de acceso remoto: Puede permitir accesos no autorizados si no se gestionan adecuadamente.
- Falta de control sobre los datos de entrada y de salida: Sin controles adecuados, los datos pueden ser interceptados o manipulados.
- Ausencia de sistemas de identificación y autenticación: Facilita el acceso no autorizado a los sistemas.
- Descargas e instalaciones desde internet no controladas: Pueden introducir malware que comprometa la confidencialidad.
- Conexiones a redes públicas desprotegidas: Pueden ser explotadas para ataques que comprometan la confidencialidad.
- Permisos, privilegios y control de acceso: fallos en la protección y gestión de permisos que permiten el control de acceso a quién no debe a lo qué no debe.

En general, el factor humano provoca negligencias causadas generalmente por la falta de formación y concienciación. El personal es considerado el más débil de la cadena.

En el sector de aviación la explotación de vulnerabilidades puede llevar a los siguientes problemas

- Interrupciones Operativas: Las vulnerabilidades pueden ser explotadas para causar interrupciones en las operaciones diarias, lo que puede llevar a retrasos o cancelaciones de vuelos.
- Costos Financieros: Los ataques cibernéticos pueden resultar en costos directos significativos debido a la necesidad de respuesta a incidentes, recuperación de datos y multas por incumplimiento de regulaciones.
- Daño a la Reputación: Un incidente de seguridad puede dañar la reputación de una aerolínea o aeropuerto, afectando la confianza del cliente y potencialmente reduciendo los ingresos futuros.
- Pérdida de Información Sensible: La exposición de datos confidenciales de pasajeros o información de propiedad intelectual puede tener consecuencias legales y de privacidad.

En resumen, las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas.

4. CONCEPTO DE AMENAZA

Objetivo: Comprender el concepto de amenaza.

4.1. Definición de Amenaza.

Se considera una amenaza a la causa potencial de un incidente no deseado, el cuál puede ocasionar daño a un sistema o a una organización.

4.2. Identificación de fuentes de amenaza.

La primera clasificación de fuentes de amenaza que se puede realizar es la procedencia de dicha fuente, es decir, si es externa o interna.

4.2.1. Amenaza Externa

Se define como amenaza externa a aquella entidad no autorizada, fuera del dominio de seguridad, que tiene el potencial de dañar un sistema de información a través de la destrucción, divulgación, modificación de datos y / o denegación de servicio.

4.2.2. Amenaza Interna

Se define amenaza interna aquella entidad con acceso autorizado (es decir, en el dominio de seguridad) que tiene el potencial de dañar un sistema de información o de la empresa a través de la destrucción, divulgación, modificación de datos y / o denegación de servicio.

4.2.3. Tipologías de Amenaza

Ingeniería Social

Las técnicas de ingeniería social son tácticas de persuasión que suelen valerse de la buena voluntad y falta de precaución de los usuarios, y cuya finalidad consiste en obtener información confidencial como contraseñas. Algunos ejemplos de este tipo de amenaza:

- **Phishing**: conjunto de técnicas que persiguen el engaño de un usuario ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de confianza), para manipularla y hacer que revele información confidencial. El phishing tradicional consiste en una emisión masiva de correos electrónicos para que las victimas hagan clic en un enlace o abra un archivo adjunto malicioso. El **spearphishing** es un tipo especial de phishing dirigido una persona o empleado especifico (i.e.: aquel con derechos de acceso) de una entidad en concreto.
- **Smishing:** similar al phishing tradicional pero el engaño se produce a través mensajes de texto (SMS, mensajería instantánea, etc.).
- **Vishing**: similar al phishing tradicional pero el engaño se produce a través de una llamada telefónica.
- **Shoulder Surfing:** Consiste en espiar físicamente a los usuarios para obtener en general claves de acceso al sistema. Por ejemplo, observando a una persona mientras escribe un código de acceso o buscando papeles dónde el personal escribe la contraseña para no olvidarla.
- **Dumpster Diving:** es el acto de acceder sin autorización a determinada información que pasa por la basura de una entidad, ya sea dentro o fuera del edificio.

- **Survey participation**: las víctimas son atraídas con la promesa de premios y otras recompensas por participar en una encuesta que parece legítima, pero en realidad sirve para obtener información confidencial

Uso de contraseñas inseguras

Debido a que una sola contraseña puede ser la puerta de acceso a una red corporativa, las buenas prácticas en la gestión y uso de contraseñas son un factor clave. En ese sentido, las contraseñas que se usen tienen que ser robustas, seguras, impersonales y a su vez fáciles de recordar; las contraseñas deberían incluir mayúsculas, números y caracteres especiales. Además, es recomendable modificar las contraseñas de manera periódica y no reutilizarlas.

Por otro lado, aunque resulte obvio, las contraseñas son confidenciales y no se deben difundir. Por tanto, no se deben apuntar en un papel y no se deben comunicar a través de un medio inseguro.

Asimismo, no se debe repetir la misma contraseña en distintos ámbitos (profesional-personal) y servicios.

Por último, no se deben utilizar las contraseñas por defecto que traen los sistemas y dispositivos electrónicos o aquellas que haya proporcionado una tercera persona o institución.

Comportamientos Sospechosos

Todo comportamiento fuera de lo normal debe ser identificado. Estos pueden ser bien acciones de otras personas, como por ejemplo *shoulder surfing;* o bien actividades o tráficos sospechosos de un sistema, por ejemplo, un navegador web que muestra contenido o re-direcciona a páginas que el usuario no solicita o equipos que muestran un rendimiento mucho menor o anormalmente lento.

Trae tu propio dispositivo *(BYOD - BRING YOUR OWN DEVICE)*

Este es un concepto que define la posibilidad de que los empleados de una organización usen los dispositivos de los que son propietarios para desarrollar sus funciones profesionales, accediendo al entorno, servicios y datos corporativos.

También se le conoce como BYOT (Bring Your Own Technology) un fenómeno mucho más amplio que incluye toda la tecnología y software propiedad de los empleados y utilizada por éstos para realizar tareas relacionadas con su trabajo, dentro o fuera de la empresa (navegador web, reproductor multimedia, antivirus, etc.).

Existen numerosas amenazas y vulnerabilidades asociadas a las políticas de BYOD que pueden poner en riesgo la seguridad, tanto del propio dispositivo, como de la información que gestiona y los sistemas a los que se accede.

- **Riesgos derivados de la movilidad**: uno de los mayores problemas que plantea la securización de los dispositivos personales deriva, precisamente, de la posibilidad de que puedan usarse en ubicaciones muy diversas (instalaciones de la organización, domicilio de los usuarios, lugares públicos, hoteles, etc.), lo que facilita el acceso físico a los dispositivos (extravío, robo o descuido temporal) por parte de un intruso, tanto para el acceso a la información que allí se almacena, como para la instalación de software de espionaje encubierto.
- **Uso de dispositivos, aplicaciones y contenidos no-confiables:** los dispositivos propiedad de los usuarios presentan importantes deficiencias en materia de seguridad derivadas tanto de su propia estructura como de un uso inseguro (procedimientos de jailbreaking o rooting). En cuanto a las aplicaciones, una de las principales amenazas es la incapacidad de detectar qué software está instalado en los dispositivos personales que se conectan a su red. Por último, en algunos casos, los dispositivos móviles pueden tener acceso a contenidos potencialmente peligrosos, que no son accesibles mediante otro tipo de equipamientos.
- **Uso de redes inseguras:** el acceso de los dispositivos personales a los servicios o a los datos corporativos puede llevarse a cabo usando redes públicas (por definición, no confiables) o redes privadas de la

organización o infraestructuras de comunicación comunes. El uso de este tipo de redes posibilita ciberataques de tipo mano-in-te-mide, que podrían interceptar e incluso modificar los datos en tránsito.

- **Interconexión con otros sistemas:** es muy frecuente que los dispositivos personales se interconecten con otros sistemas, a efectos de intercambio y almacenamiento de datos. En estos casos existe el riesgo de almacenamiento de datos en ubicaciones no confiables y fuera del control de la organización, intercambio no autorizado de datos entre dispositivos transmisión de infecciones con código dañino, de un dispositivo a otro.

Falta de protección física

Se deben aplicar medidas de protección física para impedir que los intrusos puedan acceder a los puertos, cableado y dispositivos inalámbricos. La infraestructura de redes y cableado de una entidad no debe ser accesible a personal no autorizado o ajeno a la organización. Esto implica que todo el personal debe cumplir con procedimientos de control de acceso e identificar cualquier intento de acceso de personas no autorizadas.

5. POSIBLES VECTORES DE ATAQUE Y COMO IDENTIFICARLOS

Objetivo: Comprender el concepto de ataque en ciberseguridad y conocer formas para identificarlos.

5.1. Vectores de ataque.

Los virus nos acompañan desde que los ordenadores empezaron a estar encima, o debajo, de las mesas de trabajo hace ya algunas décadas, incluso antes de que existiera Internet. En sus comienzos eran demostraciones ingeniosas de errores de los programas y se propagaban a través de disquetes. Pronto se empezaron a explotar con fines maliciosos provocando borrado de datos, intrusión, inutilización de sistemas o caída de servicios.

Los sistemas y las redes informáticas son ahora más complejas y por ello las vías de ataque se han diversificado. Los ataques llegan como adjuntos a correos, se sirven de intermediarios humanos, de dispositivos extraíbles, a través de conexiones inalámbricas, por Whatsapp, en páginas web y también vía nuestros proveedores de servicios tecnológicos, como el caso del software de Kaseya o el de SolarWinds.

Los ciberdelincuentes buscan continuamente nuevas formas de hacer llegar su "carga maliciosa" o de ganar acceso a nuestros equipos aprovechando errores humanos, fallos en la configuración o defectos de los sistemas. **A estas formas de llegar a nuestros sistemas se las conoce, en argot, como vectores de ataque.**

Vamos a ver cuáles son los más frecuentes y qué podemos hacer para impedir a los ciberdelincuentes que los utilicen en su beneficio y, casi siempre, para nuestro perjuicio.

5.2. ¿Cómo se identifican? ¿Cuáles son los vectores de ataque más frecuentes?

Teniendo en cuenta que los vectores de ataque están sujetos a cambios con los avances tecnológicos y que los ciberdelincuentes podrían utilizar varios en cada ataque, en la actualidad estos son los **10 Vectores de Ataque más frecuentes:**

1. **Correo electrónico y mensajería instantánea**, por ejemplo, los correos y SMS de phishing que suplantan a organizaciones conocidas por el receptor, como bancos, empresas de paquetería, la

Agencia Tributaria, nuestros proveedores y clientes, o nuestro soporte técnico, para engañarle con diversos señuelos, a seguir enlaces a páginas web falsas donde le pedirán introducir sus credenciales o descargar adjuntos maliciosos que instalan malware. Es muy frecuente que se trate de ransomware, es decir, el malware que bloquea los datos a cambio de un rescate. En otros casos, el malware convierte a nuestros dispositivos en zombis a su servicio para lanzar ataques a terceros o para otros fines poco éticos.

2. **Navegación web**, bien por falta de actualización de los navegadores o por instalación de plugins maliciosos, bien por visitar páginas fraudulentas. Ante navegadores no actualizados, los ciberdelincuentes podrían explotar vulnerabilidades con técnicas como:
   - drive-by download, que permite la descarga de malware sólo con visitar una página maliciosa o ver un correo html;
   - browser in the browser, que simula una ventana emergente de autenticación, donde nos pedirán las credenciales.

También puede que el usuario llegue en sus búsquedas, o por otros medios, a seguir enlaces que descargan malware o llevar a páginas de phishing. Los ciberdelincuentes suplantan webs legítimas copiándolas y poniéndoles direcciones web similares con homógrafos o enlaces que se parecen a las reales cambiando algún carácter que a la vista no es fácil distinguir.

3. **Endpoints o terminales** y otros dispositivos en los que no se han configurado las opciones de seguridad lo que los deja vulnerables. Las configuraciones de los fabricantes por defecto son, en muchos casos, poco seguras. Por ejemplo, si usan contraseñas débiles o si permiten que se conecten USB o discos extraíbles, estos podrían llevar malware. Otras veces son configuraciones incompletas o insuficientes de las redes a las que pertenecen esos dispositivos y permiten el acceso a ellos y su manipulación. Un caso particular son los dispositivos IoT.
4. **Aplicaciones web, portales corporativos, intranets y redes sociales con configuraciones defectuosas** o si están desactualizados pueden suponer una vía de entrada o bien una forma de dar información al ciberdelincuente para posteriores ataques.

Por ejemplo, si contienen o se muestra demasiada información sobre la estructura de la empresa, direcciones de correo o detalles de sus empleados podría ser utilizado en ataques de spear phishing, el phishing dirigido a una persona específica de la que antes han recopilado información para hacerlo más creíble.

Si la empresa posee una página o aplicación web, ha de tener en cuenta la ciberseguridad en su diseño y en su mantenimiento para evitar ataques como los de inyección SQL entre otros. Como veremos más adelante, se han de proteger las credenciales de acceso y los mecanismos de autenticación, tanto para usuarios como para administradores.

Un caso particular a tener en cuenta es el de las aplicaciones de videollamada y otras herramientas colaborativas, que han de actualizarse y regular su uso para evitar ataques.

El auge de las aplicaciones en la nube también hace que estén siendo utilizadas como vectores de ataque. Al contratarlas hay que analizar quién es responsable de mantener actualizados los sistemas, si el proveedor o nosotros. También debemos revisar qué aplicaciones de este tipo se permiten en la empresa y regular su uso. Por ejemplo, si se utilizan como servicios de backup, obligar a utilizar un buen cifrado. Mira estas historias reales de fraudes utilizando Google Drive y Sharepoint.

5. **Software de redes y sistemas mal configurado, desactualizado o no parcheado**, es decir, no se han seguido procedimientos adecuados en su configuración y no se han aplicado las actualizaciones o no existen por estar ya el software fuera de su vida útil. Un ejemplo de uso de esta vía de entrada por los ciberdelincuentes son los ataques contra el router, como DNS hijacking o los ataques de DoS o Denegación de servicio, como le pasó a esta empresa en esta historia real.

6. **Credenciales de usuario comprometidas** bien porque están en fugas de datos y se reutilizan en otros sistemas, bien porque han sido obtenidas por fuerza bruta o por ataques de ingeniería social. En otros casos son obtenidas mediante software o hardware que registra las pulsaciones o keyloggers o software que espía redes wifi abiertas o con configuraciones de cifrado obsoletas.
7. **Contraseñas y credenciales predecibles** o por defecto bien porque no se han cambiado, las típicas ´admin/admin´ o las que pone el fabricante y se pueden encontrar en la web; o si se han cambiado se ha hecho por otras de uso común o fácilmente predecibles por el entorno de usuario; bien porque están ´hardcodeadas´, es decir, incluidas en la electrónica de los dispositivos.
8. **Insiders o personas con acceso que pueden exfiltrar información**. Pueden ser empleados insatisfechos por despecho, exempleados que conservan por fallos de procedimiento credenciales de acceso o bien los que pudieran haberse dejado sobornar por ciberdelincuentes.
9. **Carencias del cifrado** bien por su debilidad, al usar claves simples y deducibles o protocolos obsoletos, o por no aplicarse correctamente las políticas al respecto, por ejemplo, en dispositivos móviles o portátiles o por olvido de cifrar documentos en la nube. Este vector puede llevar a fugas de información.
10. **Debilidades de la cadena de suministro**, como proveedores tecnológicos o empresas colaboradoras. Si sus sistemas sufren un incidente, nuestros datos pueden verse comprometidos. Por ello hemos de revisar las cláusulas de seguridad de los Acuerdos de Nivel de Servicio. Un caso particular son los proveedores de servicios en la nube.

6. POSIBLES MEDIDAS DE PROTECCIÓN PARA EVITAR UN ATAQUE O REDUCIR AL MÍNIMO SUS CONSECUENCIAS

Objetivo: Comprender el concepto de medidas de protección en ciberseguridad y conocer las medidas disponibles en el entorno operativo.

6.1. Contramedidas de Ciberseguridad.

6.1.1. Contramedidas para contrarrestar la Ingeniería Social.

- Impartir formación para que el personal conozca las tácticas de ingeniería social y formas de reconocerlas.
- Implementar sistema de reporte de eventos sospechosos y fomentar entre los empleados el reporte de comportamientos sospechosos tanto de personas como sistemas u ordeñadores
- Realizar simulaciones de ataque de phishing, enviando correos electrónicos ficticios al personal. En caso de que algún miembro del personal responda al correo, proporcionar instrucciones y orientación adicional para que el error no se repita.
- Instalar software de detección de malware que alerte a los remitentes de correos electrónicos de dudosa procedencia.
- Bloquear dominios y direcciones de atacantes conocidos.

6.1.2. Contramedidas para contrarrestar las Contraseñas Inseguras.

- Establecer procedimientos de administración de credenciales de acceso.

- Capacitar al personal en dichos procedimientos
- Realizar supervisiones de control interno de la aplicación de dichos procedimientos. Por ejemplo, en dispositivos de uso compartido o público, el personal cierra sesión de manera sistemática.
- Sensibilizar e informar al personal sobre la importancia de la gestión y privacidad de credenciales de acceso. Recordar la importancia de vigilar y mantener siempre a la vista los dispositivos durante viajes y zonas públicas.
- Fomentar la instalación de filtros de privacidad en los equipos informáticos, de manera que el contenido sea visto únicamente por la persona que está delante de la pantalla a escasos centímetros.
- Dependiendo de la criticidad del sistema, utilizar generadores de contraseñas seguras y sistemas de autenticación de factor múltiple

6.1.3. Contramedidas para contrarrestar el BYOD

- Establecer políticas de BYOD para proteger la información de los dispositivos propiedad del personal.
- Comprobar periódicamente el cumplimiento de la política de BYOD, solicitando a los empleados que se adhieran y renueven su compromiso con ella.
- Controlar los logs de red para determinar si los dispositivos móviles están siendo utilizados de manera adecuada.
- Establecer un sistema de gestión de las credenciales de los sistemas de la entidad que se introducen en el dispositivo propiedad del personal
- Reforzar el uso de redes privadas virtuales como punto de acceso para aquellos empleados que no puedan conectarse directamente a la red local. De manera que el acceso esté protegido, la conexión previsiblemente cifrada y el personal tiene el mismo acceso que si estuviera presencialmente.
- Concienciar al personal sobre el riesgo asociado al uso de sus dispositivos personales y hacerlo conocedor de las políticas de BYOD.

6.1.4. Contramedidas para contrarrestar la falta de protección física.

- Establecer procedimientos de control de accesos
- Comprobar periódicamente el cumplimiento de dichos procedimientos
- Concienciar a los empleados sobre los riesgos asociados con el incumplimiento de las medidas de seguridad y protección física

6.2. Medidas Disponibles en las entidades.

Las medidas de seguridad son un conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad.

Suelen diferenciarse:

• Mecanismos de mitigación técnicos (por ejemplo, un firewall) o no-técnicos (administrativos y físicos). Las medidas administrativas incluyen por ejemplo políticas y procedimientos y las físicas por ejemplo alarmas, cerraduras o detectores de fuego.

• Salvaguardas (safeguard): controles preventivos y proactivos. Contramedidas: controles correctivos (reactivos).

Atendiendo a su función en el marco de la ciberseguridad pueden clasificarse en cuatro categorías:

• Proteger: aquellas que garantizan la entrega u operación de los servicios esenciales para la actividad de la entidad, limitando o conteniendo el impacto potencial de un evento de ciberseguridad.

Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

- Detectar: aquellas que permiten identificar la ocurrencia de un evento de ciberseguridad., permitiendo el descubrimiento oportuno de los mismos.

Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

- Responder: aquellas que permiten tomar medidas respecto de un evento ciberseguridad.

Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente.

- •Recuperar: aquellas necesarias para restaurar la capacidad de los servicios que se hayan visto deteriorado debido a un ciberincidente.

Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

Además, se podría añadir una función más:

Identificar: medidas que ayudan a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus necesidades de negocio.

6.3. Acciones a evitar por parte del personal. Buenas prácticas.

El puesto de trabajo es el lugar en el que realizamos nuestras tareas diarias en la empresa.

Como parte de estas actividades cotidianas, cualquier usuario requiere acceder a diversos sistemas y manipular diferentes tipos de información. Como consecuencia directa, debemos tener en cuenta que el puesto de trabajo es clave desde un punto de vista de la seguridad de la información.

Son varios los riesgos a los que se expone el puesto de trabajo:

- información en papel al alcance de cualquiera;
- la falta de confidencialidad de los medios de comunicación tradicionales como el teléfono;
- accesos no autorizados a los dispositivos;
- infecciones por malware;
- robo de información;
- etc.

Por ello, es necesario que apliquemos un conjunto de medidas de seguridad que nos garanticen que la información, tanto en papel como en formato electrónico, está correctamente protegida.

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en la empresa, se deben seguir buenas prácticas para proteger el puesto de trabajo.

6.3.1. Mesas limpias

En el día a día de la empresa es habitual trabajar con distintos documentos en papel que se dejan encima de la mesa para mayor comodidad o porque son necesarios para las tareas diarias.

Sin embargo, al acabar la jornada se debe guardar la documentación que se encuentre a la vista (información de la empresa, clientes, proveedores, etc.). Esto es especialmente importante si se trabaja en entornos compartidos con otras empresas, o incluso públicos (atención al cliente, por ejemplo). De esta manera, se evitarán miradas indiscretas que puedan derivar en una fuga de información, además del robo de documentos que pueden contener información confidencial.

Se debe prestar especial atención a que:

- el puesto de trabajo esté limpio y ordenado;
- a documentación que no se utilice en un momento determinado debe estar guardada correctamente, especialmente cuando se abandona el puesto de trabajo o se finaliza la jornada;
- no haya usuarios ni contraseñas apuntadas en post-it o similares.

Además, también tendremos que guardar fuera del alcance de terceros, cuando no estemos en nuestro puesto, los dispositivos informáticos que se puedan desconectar, como USB o discos duros.

6.3.2. Bloqueo de sesión

Cuantas veces nos hemos levantado de nuestro puesto de trabajo y no hemos bloqueado el equipo, incluso cuando estábamos trabajando en un documento muy importante. ¿Y si alguien hubiera accedido al equipo y hubiera copiado el documento, o si hubiera enviado un correo electrónico haciéndose pasar por quien no es?

Todas esas situaciones y otras muchas se pueden evitar con un simple bloqueo de sesión.

Los dispositivos, como ordenadores, tablets o móviles, con los que se esté trabajando siempre deben estar bloqueados, a no ser que se esté en presencia de ellos.

En dispositivos de sobremesa y ordenadores portátiles, el bloqueo de pantalla se realiza por medio de los siguientes atajos de teclado:

► Windows: Win + L
► MacOS: Control + Opción + Q
► Linux: Control + Alt + L

En dispositivos móviles como smartphones o tablets se ha de establecer el bloqueo de pantalla en el menor tiempo posible y preferiblemente por contraseña o biométrico, como la huella dactilar, siempre sin interceder en la actividad laboral.

También es posible que programemos en los distintos sistemas, con ayuda del soporte informático, si fuera necesario, un bloqueo automático de sesión en caso de inactividad para que, si no se detecta actividad pasado este tiempo, se bloquee el dispositivo. Y, al terminar la jornada, dejaremos siempre los equipos apagados y si fueran portátiles o móviles, bajo llave.

6.3.3. *Software actualizado*

Todos los sistemas de la empresa deben estar actualizados a la última versión disponible, de esta manera estarán protegidos ante nuevas vulnerabilidades descubiertas y contarán con las últimas funcionalidades que haya liberado el fabricante.

Para que todos los dispositivos estén siempre actualizados es recomendable habilitar las actualizaciones automáticas, tanto en el sistema operativo como en las distintas herramientas que tengan instaladas y que dispongan de esta opción.

Un dispositivo desactualizado es un riesgo para la seguridad de la empresa, ya que un ciberdelincuente puede aprovecharse de vulnerabilidades no parcheadas para acceder a la información de la empresa.

6.3.4. *Antivirus y firewall*

Tanto el antivirus [Ref. - 3] como el firewall o cortafuegos son las herramientas de seguridad que protegen al equipo del software malicioso. Ambas herramientas siempre deben estar activadas, ya que son complementarias, es decir, las tareas que realiza el antivirus no interfieren con las del cortafuegos y viceversa.

El antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso, también conocido como malware. Actualmente, incorporan otras herramientas de seguridad como detección de webs fraudulentas o protección contra ransomware.

El firewall o cortafuegos tienen el objetivo de permitir y limitar, el flujo de tráfico que va desde y hacia Internet evitando así que el malware pueda comunicarse con el exterior y que ataques procedentes de Internet sean bloqueados.

Como con cualquier tipo de software, ambas herramientas deben estar configuradas y actualizadas a la última versión, ya que así detectarán un mayor número de amenazas.

6.3.5. *Documentación sensible*

Debido a la actividad de nuestra empresa es común que en ciertas situaciones algunos empleados hagan uso de información sensible, por ejemplo, datos de facturación, nóminas, estrategias o ideas de nuevos productos o servicios. Por ello, gestionar esta información, de manera adecuada, es imprescindible, ya que un acceso no autorizado a la misma puede suponer un grave perjuicio para la organización.

Como ya se indicó en el recurso formativo anterior, cuando este tipo de documentación se encuentra en formato físico, debe quedar guardada en un lugar seguro al finalizar la jornada laboral. Pero, ya se encuentre en formato digital o en formatos tradicionales, únicamente debe estar accesible para el personal autorizado, bien sea por medio de permisos de usuario o por cualquier otro método que evite miradas indiscretas.

En ciertas ocasiones, bien sea por descuido o por olvido esta documentación sensible puede quedar abandonada en las impresoras y escáneres de la empresa. El usuario ha de prestar especial atención cuando se utiliza este tipo de dispositivos.

El almacenamiento de documentación también puede estar externalizado en un proveedor dedicado a la custodia documental. En el caso de que exista este servicio se ha de establecer un acuerdo de confidencialidad y se comprobará que la información está correctamente custodiada.

La destrucción de la información al terminar su ciclo de vida también es un proceso crítico, que si no se realiza correctamente puede derivar en una fuga de información. Cuando se destruye información que contiene datos sensibles o confidenciales, debe hacerse de forma segura utilizando destructoras de papel o por medio de empresas especializadas que ofrezcan garantías.

6.3.6. *Contrato de confidencialidad*

En muchas ocasiones, bien sea por la necesidad de externalizar servicios o por proteger la información de la empresa, el empresario tiene que establecer acuerdos de confidencialidad. Como empresa contratada, colaborador o empleado tendremos que firmar estos acuerdos si vamos a tratar información confidencial.

Este tipo de acuerdos sentarán las bases de la relación que se establecerá entre ambas partes fijando los compromisos que se adquieren mutuamente.

Si en la empresa se trata información cuya confidencialidad debe estar garantizada, se han de incluir varias cláusulas en los contratos como:

- indicar qué información se considera confidencial y, por lo tanto, está protegida por el acuerdo;
- fijar la duración de la relación de confidencialidad, que generalmente será superior al tiempo de prestación del servicio;
- en caso de ser necesario, se indicará la jurisdicción legal a la que se acoge cada una de las partes.

6.3.7. *Uso adecuado de Internet y sistemas corporativos*

Los dispositivos y recursos que la empresa ofrece están pensados para que sean utilizados para los fines de la organización. Por tanto, no deben ser usados para cuestiones personales o en circunstancias que puedan afectar a la seguridad de la empresa.

Internet ofrece multitud de recursos que pueden ser aprovechados por los usuarios para usos no profesionales en su tiempo o lugar de trabajo o desde sus dispositivos profesionales, pero estos usos también esconden riesgos. Acceder a sitios de dudosa legitimidad como webs de descargas, juego, adultos, etc., no es un uso lícito de los recursos empresariales, pues no solo disminuye la eficiencia de estos recursos y puede ocasionar gastos innecesarios, sino que puede acarrear daños irreparables para la empresa. Muchos de esos sitios pueden no ser seguros o contar con publicidad que puede llevar a situaciones de confusión, resultando en un incidente de seguridad, como una infección por malware del dispositivo o de toda la red.

6.3.8. *Software legítimo*

Las normas de protección de la propiedad intelectual obligan a las empresas a usar en todo momento software legal. El uso de «*programas pirata*» o adquiridos de forma fraudulenta podría conllevar sanciones económicas y penales, nunca se debe instalar software sin licencia en ningún dispositivo de la empresa.

Además, por norma general, instalar software ilegal puede terminar en una infección por malware del equipo, bien sea por los anuncios de las webs de descargas, porque el programa ha sido modificado añadiendo código malicioso; o porque se requiere de un crack para que funcione, que también podrá estar infectado.

6.3.9. *Uso seguro de dispositivos de almacenamiento extraíbles*

Los dispositivos de almacenamiento extraíbles como memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc., permiten una transferencia rápida y directa de información. Hoy en día son

muy utilizados, por ello tenemos que minimizar las situaciones de riesgo como robo, manipulación, extravío e infección por virus.

En primer lugar, si su uso está permitido en la empresa, en caso de que así sea, debemos saber en qué situaciones se pueden utilizar y qué información se puede llevar en estos dispositivos. Una buena práctica cuando se necesita almacenar en estos dispositivos información sensible o confidencial consiste en cifrar la

información. También tendremos que estar atentos ante cualquier incidente como robo o pérdida de dispositivos con este tipo de información para informar de forma inmediata al responsable.

Otro aspecto importante es asegurarse de que la información que contienen los dispositivos que vamos a desechar o reutilizar, una vez es borrada, no vuelva a ser accesible, para ello se utilizarán métodos seguros de borrado y destrucción de soportes.

7. POSIBLES ACCIONES A REALIZAR EN CASO DE QUE SE SOSPECHE QUE SE HA SIDO OBJETO DE UN CIBERATAQUE

Objetivo: Conocer las medidas a realizar en caso de que se sospeche que se ha sido objeto de un ciberataque.

7.1. Medidas a tomar en caso de sospecha

La clave para detectar, detener, interrumpir y recuperarse ante un ciberataque radica en comprender cuál es su ciclo de vida y así desarrollar e implementar todas las operaciones necesarias que garanticen el mayor grado de seguridad y protección. A este ciclo de vida se le conoce como ***Cyber Kill Chain***.

¿Qué es y cómo utilizarla para evitar ataques?

Un ataque es un proceso dirigido con una intención bien definida: conseguir unos efectos sobre un objetivo; por ejemplo, robar datos que están en un servidor web o cifrar los contenidos de una máquina para hacer que el usuario pague un rescate. Pero al tratarse de una secuencia de fases (cadena), una mitigación en cualquiera de ellas romperá la cadena y, por lo tanto, frustrará el ataque.

Además, cada ataque deja una serie de huellas de las que se puede aprender y utilizar para comprender a los adversarios y estudiar cómo realizan sus acciones. Esto permitirá diseñar defensas cada vez más efectivas y comprobar si las que tenemos son las más adecuadas.

La Cyber Kill Chain está formada por una secuencia de siete pasos, cada uno de los cuales supone una etapa del ataque:

Fases de la Cyber Kill Chain. Fuente. INCIBE

Reconocimiento

Se trata de la fase en la que el ciberdelincuente recopila información sobre su objetivo. Para ello, observa los detalles que la organización publica en abierto y busca información sobre la tecnología que utiliza, así como datos en redes sociales e incluso realiza interacciones por correo electrónico.

Con esta información, el atacante valora qué métodos de ataque podrían funcionar y con qué probabilidad de éxito. Por este motivo, para evitar que el ciber atacante disponga de estos datos, resulta fundamental que los empleados estén concienciados y desarrollar una verdadera cultura en seguridad, revisando y limitando la información que se comparte en la web y en las redes sociales o imponiendo medidas que la conviertan en inaccesible (utilizando técnicas de cifrado, desechando soportes de forma segura, poniendo límites al compartir información confidencial, etc.).

Preparación

En esta fase se prepara el ataque de forma específica sobre un objetivo. Por ejemplo, un atacante podría crear un documento PDF o de Microsoft Office e incluirlo en un correo electrónico que suplante la identidad de una persona legítima con la que la empresa interactúe normalmente. Una vez más, estar concienciados con la ciberseguridad será el mejor mecanismo para frenar el ataque en esta fase.

Distribución

En esta etapa se produce la transmisión del ataque, por ejemplo, mediante la apertura del documento infectado que había sido enviado por correo electrónico, accediendo a un phishing, etc. Ser conscientes de la existencia de este tipo de ataques y aprender a identificarlos será nuestra primera línea de defensa.

Explotación

Esta fase implica la «detonación» del ataque, comprometiendo al equipo infectado y a la red que pertenezca. Esto se suele producir explotando una vulnerabilidad conocida para la cual ya existe parche de seguridad, como en el caso de una vulnerabilidad del escritorio remoto, que de no estar parcheada permitiría entrar en los equipos desde el exterior. Por este motivo, es muy importante disponer de soluciones de seguridad y mantener todos los sistemas, incluido el antivirus, actualizados a su última versión.

Instalación

Fase en la que el atacante instala el malware en la víctima. También puede darse la circunstancia de que no se requiera instalación, como en el robo de credenciales o en el fraude del CEO. En cualquier caso, la formación y concienciación en ciberseguridad será nuestra principal arma para frenar cualquier tipo de ataque en esta fase, junto con medidas técnicas como la monitorización del estado de los sistemas, ya sea mediante infraestructura propia o a través de seguridad gestionada o subcontratando personal o servicios.

Comando y control

Llegados a este punto el atacante cuenta con el control del sistema de la víctima, en el que podrá realizar o desde el que lanzar sus acciones maliciosas dirigidas desde un servidor central conocido como C&C (Command and Control), pudiendo sustraer credenciales, tomar capturas de pantalla, llevarse documentación confidencial, instalar otros programas, conocer cómo es la red del usuario, etc.

Acciones sobre los objetivos

Esta es la fase final en la que el atacante se hace con los datos e intenta expandir su acción maliciosa hacia más objetivos. Esto explica por qué la kill chain no es lineal sino cíclica, ya que se volverían a ejecutar todas y cada una de sus fases de cara a infectar a más víctimas.

Por lo tanto, para poder romper la cadena y evitar que un ataque consiga sus objetivos será necesario estar verdaderamente comprometido con la ciberseguridad.

Una organización que mantenga todos sus sistemas y equipos actualizados, utilice las soluciones de seguridad adecuadas, monitorice la actividad de sus comunicaciones y sus empleados cuenten con los conocimientos

necesarios en ciberseguridad, aumentará considerablemente su capacidad para detectar y responder ante este tipo de incidentes de seguridad, poniéndoselo mucho más difícil a los adversarios y evitando que los sistemas y la información que en ellos se almacena se vean comprometidos.

Mantenerse al día y formar y concienciar a tus empleados será la principal barrera frente a cualquier tipo de amenaza o ataque dirigido. ¡Protege tu empresa!

8. SISTEMA DE REPORTE INTERNO DE INCIDENTES EN MATERIA DE CIBERSEGURIDAD

Objetivo: Estar familiarizado con el sistema de reporte y ser consciente de la importancia del mismo.

8.1. La importancia del Sistema de Reporte de Incidentes.

La gestión de incidentes de seguridad no se basa únicamente en la respuesta cuando se produce un incidente, sino que es un proceso continuo que debe ser implantado correctamente en las Organizaciones y que presenta actividades antes, durante y después de que un incidente ocurra.

Antes de meternos con la gestión de los incidentes propiamente dicha vamos a exponer unas definiciones. Cabe señalar que estas definiciones no son únicas y que sería adecuado una estandarización a nivel nacional e internacional.

Suceso: significa una ocurrencia identificada en un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o un fallo de los controles de seguridad de la información, o una situación previamente desconocida que puede ser relevante para la seguridad de la información.

Incidente: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

La principal diferencia entre suceso e incidente es que suceso puede ser cualquier cosa que sea anómala para la seguridad de la información, aunque no haya habido tenido ningún impacto. Por su parte un incidente será un suceso o un conjunto de sucesos que hayan tenido efectos adversos.

Gestión de incidentes: todos los procedimientos seguidos para **detectar, analizar y limitar** un incidente y responder ante este.

Está definición de gestión de incidente nos introduce en el siguiente punto, en el que vamos a ver qué elementos debe contener un sistema de gestión de incidentes.

La reducción del daño causado por un ataque de ciberseguridad empieza por reconocer que se ha producido un incidente. Ser consciente del peligro inminente hace que una organización sea resistente a los impactos de la ciberseguridad.

La mitigación de los fallos de seguridad comienza con el conocimiento de un incidente de seguridad. En términos prácticos, los incidentes de seguridad deben ser registrados y esta es la labor de un sistema de notificación de incidentes que proporciona a un equipo la información necesaria para hacer frente a un evento de seguridad.

El problema de la ciberseguridad es que a menudo se oculta a plena vista. Sin embargo, está estudiado que las organizaciones que responden rápidamente a un incidente ahorran un 30% en costes y reducen el tiempo para contener una amenaza a menos de 200 días.

8.1.1. Razones para notificar incidentes de ciberseguridad

Hay buenas razones para establecer un proceso sólido de notificación de incidentes. Los resultados son beneficiosos tanto para la empresa como para el empleado e incluyen:

La notificación de incidentes fomenta una cultura de la seguridad

El espíritu que subyace en una cultura de seguridad es el de "estar todos juntos en esto". La notificación de incidentes no debe ser algo temible, sino parte de un proceso cotidiano. Haga que la notificación de incidentes forme parte de la norma de la empresa y del comportamiento esperado de los empleados cuando ocurra algo preocupante. Al proporcionar una forma fácil y rápida de informar de los incidentes, los empleados se convierten en parte de la lucha contra los ciberataques. Esto ayuda a fomentar un espíritu de comunidad en la lucha contra la ciberdelincuencia y el fraude.

Desarrolla un proceso racionalizado para evitar que los incidentes se conviertan en un ataque grave

La infraestructura de notificación debe basarse en un marco de notificación de incidentes, configurado para adaptarse a las necesidades de su organización, y utilizar flujos de trabajo automatizados. Un sistema de notificación de incidentes debe ser configurable para permitir el escalado a través de la notificación, el triaje y la mitigación, al tiempo que garantiza que se avise a la persona más adecuada una vez que se inicie el proceso de notificación de incidentes de seguridad.

Aplica las políticas de seguridad

Disponer de un proceso de incidentes de seguridad ayuda a aplicar la política de seguridad de su empresa. Un sistema de notificación que utiliza flujos de trabajo de incidentes proporciona un marco para llevar un incidente a través del triaje a la mitigación basada en los avisos de la política de seguridad.

Evita los costosos eventos de seguridad

Un incidente que se convierte en un acontecimiento, como una violación de datos, tiene como resultado costes financieros y de otro tipo. Elinforme deIBM "Cost of a Data Breach Report" (Coste de unaviolación de datos) ha visto cómo el año 2021 se llevaba el galardón de los costes más altos de violación de datos en 17 años. Si desarrolla una cultura de notificación en su organización y facilita la notificación de incidentes, su equipo estará más capacitado para evitar que un incidente se convierta en un evento de seguridad en toda regla.

Ayuda a mantener el cumplimiento de la normativa

Mantener un registro de cumplimiento es un requisito por defecto en muchas regulaciones y normas, incluyendo ISO27001, DPA2018 y GDPR. Estos registros también se extienden a los diversos requisitos de notificación de infracciones de la normativa de protección de datos. La notificación de incidentes permite a una organización demostrar que se toma en serio la seguridad y demostrar las medidas paliativas adoptadas. Un sistema de notificación debe permitir a una organización tomar los detalles de una presunta infracción y, a continuación, generar un informe si se requiere una notificación de infracción.

8.1.2. Buenas prácticas para la notificación de incidentes de seguridad

El uso de la notificación de incidentes por razones de salud y seguridad está bien establecido. Al cotejar los datos de salud y seguridad, las empresas pueden contribuir a garantizar un entorno de trabajo seguro y cumplir las expectativas normativas. La notificación de incidentes de seguridad es una extensión de esta cultura de salud y seguridad que proporciona un marco para hacer frente a una amenaza inminente. Sin embargo, la notificación requiere que se sigan ciertas prácticas básicas:

1) Facilidad de información

Un sistema de notificación de incidentes debe ser fácil de usar por todos. La introducción de incidentes debe guiar al empleado, capturando los detalles más importantes que se necesitan para iniciar el proceso de escalado. Deben evitarse las barreras de entrada, como los formularios complicados, etc.

2) Escalada adecuada

El sistema de notificación de incidentes debe ser configurable para permitir a un administrador crear flujos de trabajo que reflejen la estructura del equipo que se ocupa de los incidentes de seguridad. Al utilizar un flujo de trabajo automatizado que envíe alertas apropiadas y adaptadas a las personas adecuadas, se pueden prevenir las violaciones de datos y otros eventos de seguridad.

3) Auditoría e informe

Un sistema de notificación de incidentes debe ser capaz de auditar incidentes y acciones y generar informes. Estos informes pueden utilizarse como documentación probatoria para demostrar el cumplimiento de los reglamentos y normas. El informe de incidentes también constituye una base de pruebas para un informe de notificación de violación de datos, si se requiere.

La notificación de incidentes es importante para evitar que un incidente de seguridad se convierta en una violación de la seguridad.

8.2. Sistemas de Reporte Interno-Externo de Incidentes

Si sufrimos un incidente que pudiera afectar a la seguridad de la empresa, el primer paso que tenemos que dar es analizar qué ha pasado. De esta manera, conociendo el tipo de incidente se podrá medir más eficazmente la repercusión en la organización y cómo actuar. Una clasificación posible de los incidentes es la siguiente:

- acceso no autorizado a sistemas o información, como en el caso de robo de un dispositivo o de las credenciales de acceso;
- denegaciones de servicio, en las cuales el incidente impide el correcto funcionamiento de un recurso, como por ejemplo la página web de la empresa;
- infección por malware;
- robo de información de la empresa;

Qué tipos de incidentes de seguridad que requieren atención:

Phishing

El operador humano es donde muchos ciberatacantes centran su atención. El phishing es el método más común que utilizan los estafadores para engañar a un empleado y conseguir que facilite sus credenciales de acceso y otros datos personales. Un sistema de notificación de incidentes de seguridad debe ser capaz de capturar fácilmente los detalles de un mensaje sospechoso de phishing. El informe de incidentes debe contener detalles de cualquier interacción con el mensaje, especialmente si se ha hecho clic en un enlace de un correo electrónico/mensaje. Se deben capturar más detalles de lo que sucedió después para indicar el alcance del incidente.

Dispositivo perdido

Los dispositivos de la empresa pueden contener mucha información sensible. Además de los dispositivos de la empresa, el trabajo a distancia ha aumentado el uso de dispositivos personales para acceder a las aplicaciones corporativas en la nube. Un dispositivo perdido o robado puede acabar en las manos equivocadas, lo que puede dar lugar a la exposición de datos, ya que las empresas utilizan cada vez más la

sincronización de datos con las aplicaciones en la nube. Si se pierde o se roba un teléfono utilizado para el trabajo de la empresa, el incidente debe registrarse rápidamente para que se pueda llevar a cabo el triaje del incidente y se inicie una respuesta adecuada.

Fuga accidental de datos

Las investigaciones han revelado que el 58% de los empleados han enviado un correo electrónico a la persona equivocada. El envío erróneo de un correo electrónico puede provocar la pérdida de datos y el incumplimiento de la normativa de protección de datos. Las tendencias de incidentes de la ICO del Reino Unido muestran que la exposición de datos relacionada con el correo electrónico es la que más contribuye a los incidentes de seguridad. Si un empleado cree que ha enviado un correo electrónico con información sensible a la persona o personas equivocadas, debe informar de ello.

Otros incidentes relacionados con el correo electrónico

Uno de los mayores problemas de exposición accidental de datos es el simple hecho de olvidarse de ceder una lista de destinatarios en un intercambio de correos electrónicos. En cuanto el empleado se dé cuenta de que se ha olvidado de poner la copia oculta a los destinatarios, debe informar del incidente para que se inicie el triaje y se gestione el suceso de acuerdo con la política de la empresa.

Una vez conozcamos qué ha pasado, lo siguiente que tenemos que hacer es avisar a los miembros de la empresa que deban de estar en conocimiento de lo sucedido. Por ejemplo, si hay fuga de información de carácter personal, lo pondremos en conocimiento del responsable que deba comunicarlo a los afectados y a la Agencia Española de Protección de Datos. También tenemos que conocer que, si necesitamos apoyo en la resolución del incidente, podemos ponernos en contacto con la Línea de Ayuda en Ciberseguridad que ofrece INCIBE por medio del teléfono gratuito 900 116 117, y del correo electrónico incidencias@incibe-cert.es o el formulario de contacto.

Por último, en caso de que el incidente suponga un delito (falsificación, injurias y calumnias, daños de propiedad intelectual, sabotaje, piratería, estafa, robo de identidad, etc.) es recomendable interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado aportando toda la información que se pueda de lo sucedido.

ANEXO I – DEFINICIONES

A los efectos de la presente guía, se entenderá por:

AMENAZA: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

AMENAZA EXTERNA: Entidad no autorizada fuera del dominio de seguridad que tiene el potencial de dañar un sistema de información a través de la destrucción, divulgación, modificación de datos y / o denegación de servicio.

AMENAZA INTERNA: Entidad con acceso autorizado (es decir, en el dominio de seguridad) que tiene el potencial de dañar un sistema de información o de la empresa a través de la destrucción, divulgación, modificación de datos y / o denegación de servicio.

ANÁLISIS DE RIESGOS: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

ANTI-SPAM: Contramedida cuyo objetivo es la contención de correo electrónico no solicitado (spam).

ANTI-SPYWARE: Contramedida cuyo objetivo es evitar la infección por código malicioso de tipo spyware.

ANTIVIRUS: Aplicación informática cuya finalidad es la detección, detención y eliminación de virus y demás códigos maliciosos.

ATAQUE: Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera.

ATAQUE DE INVASIÓN: Cualquier tipo de ataque contra las autorizaciones, autenticaciones, permisos, derechos sobre los archivos o interceptación de correo electrónico.

AUTENTICACIÓN: Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.

CIBERINCIDENTE: Incidente relacionado con la seguridad de las TIC que se produce en el Ciberespacio. Este término engloba aspectos como los ataques a sistemas TIC, el fraude electrónico, el robo de identidad, el abuso del Ciberespacio, etc.

CIBERAMENAZA: Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

CIBERATAQUE: Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

CIBERESPACIO: Dominio global y dinámico compuesto por infraestructuras de tecnología de la información —incluyendo internet—, redes de telecomunicaciones y sistemas de información.

CIBERSEGURIDAD: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.

COMPROMISO DEL SISTEMA: Cualquier sistema informático, hardware o software, que está siendo o ha sido atacado con éxito. Por ejemplo: robo de información confidencial, alteración de la configuración del sistema, etc.

CONFIDENCIALIDAD: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

CONTROL DE SEGURIDAD: Medida que mantiene y/o modifica un riesgo. Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.

DENEGACIÓN DE SERVICIO: Se entiende como denegación de servicio, en términos de seguridad informática, aun con-junto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

DISPONIBILIDAD: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

HACKING: Cualquier actividad o tráfico sospechosos que puedan alterar el funcionamiento del sistema y estén relacionadas con un intento de intrusión. Por ejemplo, tentativas de acceso no autorizado al sistema o escaneo de servicios.

INFECCIÓN POR MALWARE: Incidentes provocados por malware (virus, gusanos, troyanos, bombas lógicas, spyware, rootkits, etc.). La gravedad varía según el malware, pudiendo afectar a robos de información, o a la disponibilidad de los sistemas.

INCIDENCIA: Véase suceso de seguridad de la información.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer o afectar las operaciones del negocio (seguridad de la aviación) y de amenazar la seguridad de la información.

INTEGRIDAD: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Riesgo para las operaciones de la organización, los activos, los individuos y otras organizaciones debido al potencial de una brecha de seguridad de la información

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información

SISTEMAS CRÍTICOS, COMUNICACIONES Y DATOS CRÍTICOS: Son aquellos sistemas comunicaciones y datos que en caso de sufrir deterioro en alguna de las variables (confidencialidad, integridad, disponibilidad):

- Desde el punto de vista de seguridad de la aviación civil: que pudieran afectar a un aumento de la probabilidad de que se produzca un acto de interferencia ilícita.
- Desde el punto de vista de seguridad operacional (safety): que pudieran afectar potencialmente a la seguridad operacional de aeronave o afectar al normal funcionamiento de la EATMN (Europea Air Traffic Management Network).

SUCESO O EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

VULNERABILIDAD: Debilidad de un activo o de un control que puede ser explotada por una o más amenazas o acciones inadvertidas.

➢ *En el Glosario de Términos (CCN-STIC 401) están disponibles estas y otras definiciones que pudieran ser necesarias*

ANEXO II – ENLACES DE INTERÉS

➢ INCIBE	*https://www.incibe.es/*
➢ Kit de concienciación (INCIBE)	*https://www.incibe.es/protege-tu-empresa/kit-concienciacion*
➢ CCN-CERT	*https://www.ccn-cert.cni.es/*
➢ Guías CCN-CERT	*https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html*
➢ Glosario de Términos (CCN-STIC 401)	*https://www.ccn-cert.cni.es/guias/glosario-de-terminos-ccn-stic-401.html*
➢ ENISA	*https://www.enisa.europa.eu/publications/archive/ar-quizzes-templates-es*
➢ Oficina De Seguridad del Internauta	*https://www.osi.es/es*
➢ Cyberessentials (Gov. Reino Unido)	*https://www.ncsc.gov.uk/cyberaware/home*
➢ Cyber security: advice for small businesses (Gov. Reino Unido)	*https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know*
➢ ICO (Reino Unido)	*https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf*
➢ Eleven Paths	*https://empresas.blogthinkbig.com/elevenpaths/*
➢ Noticias de Seguridad Informática	*https://noticiasseguridad.com/*