Ciberseguridad:

El objetivo es dar a conocer por qué la ciberseguridad ha alcanzado una gran importancia para todas las organizaciones de cualquier tamaño; concienciar cuáles deben ser las buenas prácticas a seguir para evitar en gran medida los riesgos y cómo responder en el caso en que nos hayamos visto afectado por alguna amenaza

1.INTRODUCCIÓN

1.1. REFLEXIÓN SOBRE DEPENDENCIA TECNOLÓGICA

La ciberseguridad nos afecta en mayor o menor medida en función de la dependencia tecnológica de nuestro organización y vida cotidiana; utilizamos mail, ordenadores conectados a Internet y otros dispositivos móviles. En algunos casos, incluso la "nube" porque tenemos un comercio electrónico, página web o hacemos uso de otros servicios en la nube (cloud computing).

Si pensamos en los activos de una empresa u organización enseguida nos vienen a la cabeza aquellos que constituyen bienes tangibles, como el mobiliario, maquinaria, servidores, etc. Sin embargo, no debemos olvidar que existen también bienes intangibles como la cartera de clientes, las tarifas, el conocimiento comercial, la propiedad intelectual o la reputación. Todos estos elementos forman parte de la información de esta que constituye uno de los activos más importantes de nuestra organización.

Se consideran activos de información, todo lo que maneja o contiene información de la organización: móviles, portátiles, memorias, USB, discos, routers, servidores, software y aplicaciones comerciales, datos en aplicaciones empresariales, página web, tienda online, bases de datos de clientes o productos, informes, documentos, contratos de trabajo, contratos de suministro, etc.

Proteger adecuadamente estos activos de información, es decir lo que tiene valor, es lo que nos ocupa en este curso.

La información que maneja nuestra organización para el desarrollo de su actividad profesional es uno de los valores que debe proteger el propietario de la organización para asegurar la buena marcha de la misma.

Esta información puede estar relacionada con:

- **Proveedores**
- **Clientes**
- **Empleados**
- **Productos y servicios**
- **Modelo de gestión**
- **Herramientas y recursos materiales**

Además, esta información se crea, transforma, almacena, transmite y elimina a través de distintos medios/entornos que también deben protegerse en función de su valor para la organización.

Estos medios y entornos son:

- **Bases de datos**
- **Aplicaciones**
- **Internet**
- **Cloud (la nube)**
- **Servidores**
- **Redes**

1.2. ¿QUÉ VALOR TIENE NUESTRA INFORMACIÓN EN INTERNET?

Gracias a la información de los usuarios se generan ingresos a través de la publicidad comportamental. Cada vez que un usuario accede a algún tipo de información, haciendo clic en un link o un anuncio, está revelando información sobre sus preferencias, intereses y gustos.

Nuestros datos se "ceden" a las empresas anunciantes, de las que viven muchos de los servicios, para que generen una publicidad extremadamente segmentada y teledirigida a nosotros que, a priori, tiene mucho más impacto lo que a su vez supone un mayor beneficio económico.

Si quieres controlar lo que alguien pueda saber sobre nosotros o lo que puedan hacer con vuestros datos, leer las condiciones de uso de todos y cada uno de los servicios que utilices antes de aceptarlas.

Por otra parte, también a través de Internet hay quien trafica con información obtenida ilegalmente y podemos encontrar información (páginas web, mensajes) relacionada con actividades o acciones ilícitas.

Además del fraude y del robo de información, otras actividades ilegales también tienen su base en la red, aunque no sean evidentes. Esto es porque utilizan los bajos fondos de internet, la Darknet a la que sólo se accede con software específico que permite el anonimato y la confidencialidad. Es donde se encuentran los mercados negros de internet.

2.SEGURIDAD DE LA INFORMACIÓN

2.1 ¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La seguridad de la información engloba un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema establecido por la empresa. Principalmente este tipo de sistemas se basan en las nuevas tecnologías, por tanto, la seguridad de la información resguardará los datos que están disponibles en dicho sistema y a los que solo tendrán accesos usuarios autorizados. Por otro lado, tampoco se podrán hacer modificaciones en la información a no ser que sea de la mano de los usuarios que tengan los permisos correspondientes.

La seguridad de la información debe responder a tres cualidades principales:

- **Crítica**
- **Valiosa**
- **Sensible**

Por un lado, debe ser crítica, ya que es una pieza fundamental para que la empresa pueda llevar a cabo sus operaciones sin asumir demasiados riesgos. También debe ser valiosa, puesto que los datos que se manejan son esenciales para el devenir del negocio y finalmente tiene que ser sensible, ya que al sistema solo podrán acceder las personas que estén debidamente autorizadas. Además, también hay que tener en cuenta que la seguridad de la información debe hacer frente a los riesgos, analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso.

2.2 EL OBJETIVO DE LA SEGURIDAD DE LA INFORMACIÓN: CARACTERÍSTICAS

La seguridad de la información tiene como objetivo principal proteger los datos de las empresas. Pero este concepto es en términos generales, puesto que el sistema lo que va a hacer es asegurar tres aspectos fundamentales: la confidencialidad, la disponibilidad y la integridad. Para llevar a cabo estas acciones se deberán establecer estrategias donde se redacten las políticas de actuación para cada uno de estos casos. También habrá que establecer el uso de las tecnologías, incluir controles de seguridad y todos los procesos que se van a llevar a cabo para detectar los riesgos a los que se puede ver expuesto el sistema. Teniendo en cuenta todas estas cosas: ¿en qué consisten esos tres aspectos fundamentales?

Confidencialidad

A través de ella la seguridad de la información garantiza que los datos que están guardados en el sistema no se divulguen a otras entidades o individuos que no están autorizados para acceder a esa información.

Disponibilidad

Toda la información que se encuentre recogida en el sistema tiene que estar siempre a disposición de los usuarios autorizados en cualquier momento que ellos necesiten acceder a ella.

Integridad

Para que el sistema sea veraz los datos no deben manipularse. Así se garantiza que la información recogida sea exacta y no haya sido modificada a no ser que algún usuario autorizado lo haya hecho por orden expresa.

2.3 Los servicios que ofrece la seguridad de la información

Ya tenemos claro que la seguridad de la información vela por el buen funcionamiento de los datos de las empresas y la transmisión de información de unos usuarios a otros siempre que estén autorizados. Pero además gracias a esta seguridad garantizamos que todos los mensajes que se lleven a cabo los enviará un emisor acreditado y que los recibirá el receptor correspondiente **sin ningún tipo de interrupciones**.

Además, se trata de un sistema que utiliza diferentes protocolos para poder realizar su función correctamente. Hablamos, por ejemplo, de la criptografía, que **utiliza un código cifrado, la identificación**, para validar el proceso e incluso una secuenciación lógica por la que se lleva a cabo todos los pasos de envío de mensajes.

También hay que tener en cuenta que dentro de la seguridad de la información otro aspecto muy importante es conocer las **técnicas para prevenir los riesgos**. Hay empresas que intentan evitarlos a toda costa, otras que los reducen al nivel más bajo e incluso aquellas que los aceptan e intentar solucionar el problema o por el contrario compartir el riesgo.

3.RIESGOS, VULNERABILIDADES Y AMENAZAS

3.1. RIESGOS

Los riesgos de tu organización son aquellos que pueden poner en peligro tu información y por ello, comprometer el desarrollo de tu actividad profesional. Sobre los riesgos habrá que calcular el impacto que dichos riesgos causen en la organización y la probabilidad de que acontezcan.

RIESGO	**IMPACTO**
Robo de información	Pérdida de ventaja competitiva
Intrusiones en mis sistemas y acceso a información sensible y confidencial.	Exponer datos e información confidencial Impacto reputacional o pérdida de imagen
No ser capaces de restaurar la situación después de un incidente	No poder restaurar la situación debidamente pone en riesgo la continuidad de nuestra actividad, con la consiguiente pérdida económica y de imagen.
Estar expuesto a ciberdelincuentes	Pérdidas económicas por robo y fraude. Impacto reputacional
Ataques a la marca (redes sociales)	Pérdidas de clientes e impacto reputacional
Estar expuestos a un ataque cibernético de denegación de servicio	Interrumpir el servicio tanto interno como a cliente (pérdida de ventas). Impacto reputacional. Incumplimiento normativo o contractual y posibles sanciones.

3.2. VULNERABILIDADES

Una vulnerabilidad es una **debilidad** que puede poner en peligro la información y comprometer el buen desarrollo de nuestra actividad profesional.

TIPOS DE VULNERABILIDADES POR SU ORIGEN:

- **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:** Problema de configuración de software o de los servidores web. Este error puede provocar la inutilización de páginas web a través de ataques de denegación de servicio (DoS)
- **Factor humano:** Negligencias causadas generalmente por la falta de formación y concienciación.
- **Validación de entrada:** Fallo en la validación de datos introducidos en aplicaciones que 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.
- **Permisos, privilegios y/o control de acceso:** Fallos en la protección y gestión de permisos que permiten el control de acceso.

3.3. AMENAZAS

Una amenaza es todo elemento que aprovecha una vulnerabilidad o debilidad de los sistemas utilizados en nuestra organización para causar un daño y ocasiona un incidente de seguridad en el sistema, comprometiendo la seguridad de la información.

Cuando hablamos de ciberseguridad, en la cabeza de la mayoría de las personas está la posibilidad de infectarse con un virus en el ámbito de su empresa.

Sin embargo, este es sólo uno de los riesgos a los que puede verse expuesto.

De hecho, los mayores problemas en materia de ciberseguridad están asociados con estos cuatro tipos de amenazas:

a) **Ataques de denegación de servicios**: El objetivo es degradar la calidad de servicio de un sistema o una red llegando a dejarlo no operativo o inaccesible.

b) **Acceso no autorizado a las bases de datos de la empresa**: Supone una amenaza muy común para las empresas en materia de ciberseguridad.

c) **Fuga de información sensible para la organización con posible publicación de la misma**: con el consiguiente daño a su imagen y reputación (ej. Se extravía un USB, móvil, notebook, etc)

d) **Robo de credenciales** de acceso a servicios y aplicaciones.

3.4. ¿Y QUÉ PUEDO HACER?

Al plantearse esta pregunta muchas personas optan por posturas bien distintas:

- "No voy a hacer nada. No creo que a mí, siendo una pequeña empresa o autónomo, vaya a atacarme nadie, yo no tengo interés para los ciberatacantes".
- "No voy a hacer nada. Porque si hasta las empresas grandes que se supone que tienen medidas de seguridad implantadas, sufren ataque, ¿qué voy a hacer yo?".
- Pero la postura más inteligente es la de la resiliencia, es decir, tu capacidad de superar situaciones adversas, ataques o incidentes no intencionados; por lo que debes implementar medidas o controles que aumenten el nivel de protección de tus activos de información.

Antes, hay que considerar las siguientes premisas:

- Primero tenemos que analizar qué medidas de seguridad tenemos ya implantadas.
- La ciberseguridad no es sólo responsabilidad de un departamento de la empresa
- La ciberseguridad es más dependiente de las personas que de la tecnología

Lo principal: FORMACIÓN Y CONCIENCIACIÓN

Medidas de seguridad informática en los establecimientos de la C.A. de Euskadi según estrato de empleo y rama de actividad (%). 2017

	Todos los establecimientos				Establecimientos de 10 y más empleados			
	Total	Rama de actividad			Total	Rama de actividad		
	% s/establ.	Industria	Construcción	Servicios	% s/establ.	Industria	Construcción	Servicios
Con alguna medida de seguridad informática	**86,4**	**91,6**	**84,5**	**86,3**	**99,2**	**99,4**	**98,0**	**99,2**
Servidores seguros	63,3	68,3	51,4	64,6	93,6	91,6	87,0	94,9
Firewalls (cortafuegos)	73,6	78,5	65,3	74,4	95,5	95,3	94,6	95,7
Encriptación de datos	37,9	31,3	25,3	40,3	61,2	51,2	43,9	65,9
Backups fuera del establecimiento	52,8	56,8	43,8	53,9	79,9	76,8	80,8	80,9
Mecanismos de autentificación:	57,3	60,7	48,6	58,3	85,0	84,4	83,8	85,3
- Firma electrónica digital	47,3	52,2	42,5	47,6	74,2	73,9	77,0	74,0
- Otros mecanismos de autentificación	44,9	46,0	36,3	46,1	71,3	69,8	72,0	71,7
Detección de virus	84,5	89,1	83,1	84,3	98,6	98,9	98,0	98,5
Suscripción a un servicio de seguridad	55,5	57,8	47,1	56,5	85,1	81,9	86,6	86,1
Utilización de protocolos seguros (SSL/TLS) para recibir pedidos por internet	27,4	22,8	15,7	29,5	48,6	36,7	27,2	54,4
Utilización de protocolos para el análisis de incidentes de seguridad	26,2	22,8	18,9	27,6	50,9	41,5	50,3	54,2

Unidad: porcentaje sobre establecimientos

Fecha 18 de julio de 2017

Fuente: Eustat. Encuesta sobre la sociedad de la información. Empresas

4.ACTORES

4.1. ACTORES MALINTENCIONADOS

CIBERACTIVISTAS O HACKTIVISTAS: Sus acciones responden a motivos ideológicos (Anonymous)

ACTORES INTERNOS (INSIDERS): Personas que han tenido algún tipo de relación con la organización (exempleados, personal temporal o proveedores) y su motivación puede ser: venganza, motivos financieros o políticos, o simplemente realizan acciones maliciosas por desconocimiento).

ORGANIZACIONES PRIVADAS: Movidas por el interés económico que supone poseer los conocimientos que tiene la competencia, desarrollan acciones de ciberespionaje industrial.

CIBERTERRORISTAS, CIBERCRIMINALES: Puede que la categoría más peligrosa de creadores de malware sean los hackers y grupos de hackers que crean programas de software malicioso con el fin de materializar sus propios objetivos criminales específicos

3.2. ACTORES AMISTOSOS

CIBERINVESTIGADORES: Personas que persiguen el descubrimiento de las vulnerabilidades que pueden afectar a los sistemas hardware o software. La publicación de los resultados de sus investigaciones (al objeto de sensibilizar sobre las necesarias medidas de seguridad) puede suponer que se use por terceros malintencionados.

HACKERS ÉTICOS: Estos agentes usan sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño. La idea es tener el conocimiento de posibles vulnerabilidades y corregirlas. Estas pruebas se llaman "pen tests" o "penetration tests" en inglés. En español se conocen como "pruebas de penetración", en donde se intenta de múltiples formas burlar la seguridad de la red para robar información sensible de una organización, para luego reportarlo a dicha organización y así mejorar su seguridad.

CSIRT: Un CSIRT es un **Equipo de Respuesta ante Incidentes de Seguridad Informática**, que estudia el estado global de la seguridad de redes y ordenadores dentro de una organización. Además, publica alertas relativas a amenazas y vulnerabilidades.

Las funciones de un CSIRT son: ayudar a prevenir incidentes de seguridad, proteger la información, guardar evidencias, apoyar a los usuarios a recuperarse, dirigir la

respuesta a incidentes y difundir la cultura de la seguridad de la información dentro de su organización.

Podemos destacar los siguientes servicios.

- **Servicio de alerta temprana**: El servicio de Alertas o Anuncios (Announcements) incluye vulnerabilidades de día cero (0-day), campañas de malware que estén teniendo un impacto significativo, fugas masivas de información sensible, ciberataques, etc. Con la publicación de las mismas se busca informar y prevenir de las amenazas o riesgos con especial relevancia con el fin de que los usuarios puedan tomar a tiempo las medidas oportunas para mitigarlas y así no verse afectados.

- **Gestión de incidents**

  Análisis de incidentes (Incident analysis): tras la recepción de un incidente realizan una valoración de la información reportada y de las evidencias relacionadas. Este análisis permite categorizar y priorizar el incidente (triage), así como determinar si se trata de un incidente aislado puede estar relacionado con algún otro que nos hayan reportado. De este modo, podemos afrontarlo de la manera más eficiente.

  Apoyo a la respuesta a incidentes (Incident response support): proporcionan apoyo y consejo a los usuarios que se ven afectados por un incidente de ciberseguridad. Les guian sobre las pautas a seguir y, en el caso de que sea necesario, les redirigen al punto de contacto más adecuado según corresponda.

5.PRINCIPALES AMENAZAS

5.1. MALWARE

EJEMPLO DE MALWARE:

Existen diferentes tipos de Malware, como por ejemplo:

- El **virus** es un código de software que puede replicarse y propagarse de un ordenador a otro.
- Los **gusanos** son una variante del virus, pero es auto-replicante, diseñado para propagarse a través de redes informáticas.
- Los **troyanos** se caracterizan en que obtienen acceso a un sistema que se suele «esconder» dentro de una aplicación real.

RAMSOMWARE:

El malware que bloquea o codifica los datos o funciones de los equipos a cambio de un pago para desbloquearlos es conocido como ransomware.

Normalmente empieza con un correo un enlace a una página web o un archivo adjunto de correo de dudosa procedencia infectado.

a. El virus malware busca archivos para cifrarlos.
b. El usuario ya no puede acceder a su propia información, es como si la secuestraran.
c. El ciberdelincuente se pone en contacto con el usuario y le solicita un «rescate».
d. El usuario debe depositar dinero en una billetera virtual para obtener la clave de los archivos cifrados, considerar que esto no siempre garantiza la devolución de los datos.
e. El ciberdelincuente le proporciona las claves para descifrar la información para poder acceder otra vez a ella.
f. El usuario restaura los datos de su última copia de seguridad.

El objetivo de este tipo de amenazas es llegar a la mayor cantidad de personas posibles, por lo que las principales vías de contagio son:

a. Anuncios en páginas web que redirigen a otra página comprometida que puede infectar tus dispositivos.

b. Dispositivos infectados (USB)

c. Sitios web fraudulentos (que suplantan a tiendas o bancos) o sitios web legítimos pero infectados.

d. Enlaces a sitios comprometidos en correos masivos o por mensajería instantánea.

e. Programas de compartición de ficheros (P2P).

f. Softwares gratuitos.

BOTNET

Una botnet es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques de denegación de servicio distribuido (DDOS) sin el conocimiento o el consentimiento de los propietarios reales de los equipos. Todo ello sin que los usuarios legítimos lo sepan.

Actúan de forma sincronizada bajo las órdenes de un C&C (ordenador de mando y control), controlado por la persona u organización que infectó esos ordenadores.

Los ciberdelincuentes o las organizaciones criminales que están detrás de estos botnets se lucran con ellos porque utilizan nuestros recursos para actividades por las que pueden obtener dinero: distribuir malware, enviar spam, alojar páginas fraudulentas, lanzar denegaciones de servicio

Las consecuencias son:

a. Conexión a internet muy lenta

b. Tu IP puede bloquearse por envío masivo de spam

c. Tus equipos pueden utilizarse en remota para la comisión de hechos delictivos.

EXPLOIT

Los exploits son pequeños trozos de código que están escritos para aprovecharse de vulnerabilidades y/o errores específicos dentro de un sistema, para lograr acceder a él de forma ilegítima o causar otro tipo de problemas. Hay que tener en cuenta siempre que el software se desarrolla por humanos, por lo tanto, es normal encontrarse con errores en los códigos. Estos errores, comúnmente llamados bugs, pueden ser del tipo desbordamiento de búfer (buffer overflow), condición de carrera (race condition), errores de validación de variables, etc.

DOS (DENEGACIÓN DE SERVICIO)

Se entiende por denegación de servicio a un conjunto de técnicas cuyo objetivo es inutilizar un servidor (por ejemplo, la web de la empresa). Un ataque de Denegación de servicio distribuido (DDoS) es más sofisticado y permite enviar peticiones coordinadas entre distintos equipos a un mismo servidor para inutilizarlo o tirarlo.

DEFACE O DEFACEMENT

Relacionado al ingreso sin autorización en un servidor web y manipular la página principal, dejando algún tipo de mensaje en texto, imagen, vídeo... Puede ser de carácter reivindicativo político, lo que sería hacktivismo, o para avergonzar a los responsables del sitio, o simplemente un graffiti al estilo "Paco estuvo aquí". Hay grupos especializados en hacer defaces, incluso quienes se lo toman como una competición.

QUÉ HACER EN CASO DE MALWARE

Descubrir los síntomas

- Lentitud al navegar por internet o durante la descarga de archivos
- Aparición de ventanas y anuncios emergentes no solicitados por el usuario
- Cambio del fondo de escritorio u otro aspecto del sistema
- Mensajes intimidatorios para el usuario o solicitud de pagos para recuperar información
- Cambio de página de inicio de internet o redirección a sitios web desconocidos
- Bajo desempeño en el procesamiento de tareas de equipo
- Aparición de programas instalados en el equipo sin el consentimiento del usuario
- Comportamiento anormal del sistema operativo como reinicio o apagado repentino

Determinar el alcance

Conocer el alcance de una infección permite calcular los recursos que serán necesarios para solucionas los inconvenientes que haya generado

Mantener la continuidad de la organización

En función del alcance de la infección, se podrán tomar decisiones para continuar correctamente con las decisiones de la compañía

Contener las acciones maliciosas

Aislamiento de los equipos informáticos. Evita que la infección se propague Erradicar la infección
Arrancar en modo seguro
Parar procesos maliciosos
Instalar antimalware

Medidas de protección

Antivirus actualizado
Revisión de las reglas de firewall
Cambio de contraseñas a otras más seguras.
Actualización de credenciales de acceso

Recuperar la normalidad de las operaciones

Aprendizaje y mejora continua

5.2. INGENIERÍA SOCIAL

Con la evolución de la tecnología y de las medidas técnicas de seguridad, si algo ha quedado patente es que **el eslabón más importante de la cadena de seguridad de la información de las organizaciones es "la persona"**. La seguridad de la información no se garantiza únicamente con la definición de procedimientos de gestión de incidencias o la implantación de mecanismos de cifrado, por poner algunos ejemplos.

Por ese motivo, es fundamental que el personal de la organización esté concienciado e implicado. No sólo en el cumplimiento de las normas que se hayan implantado, sino también manteniendo una actitud de precaución y alerta en el uso cotidiano de los sistemas de información, en las relaciones personales y laborales. Los empleados son la última barrera del sistema de defensa de la seguridad de las empresas.

EJEMPLO DE INGENIERÍA SOCIAL: PHISHING

El "phishing" consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.
Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

¿Cómo puedes protegerte del phishing?

- Usa los **filtros antispam** que facilitan los clientes de correo electrónico. También puedes ayudarte de herramientas específicas que **bloquean el correo no deseado.**

- Configura la opción antiphishing que incorporan los navegadores:

  a. El **Filtro SmartScreen** de Internet Explorer ayuda a identificar sitios web notificados como de suplantación de identidad (phishing) o de malware.
  b. **Protección contra el Malware y el Phishing** en Firefox
  c. **Protección contra phishing y software malicioso** en Google Chrome o **Evitar la suplantación de identidad** (phishing) en Safari

- **Verifica la legitimidad del sitio web.** Fíjate siempre en la URL para asegurarte que estás en la página web oficial en la que querías estar y no se trata de una web que la está suplantando.

Has detectado un caso de phishing. ¿Qué debes hacer?

- No accedas a las peticiones de solicitud de información. En caso de duda, consulta directamente a la empresa o servicio a través de los mecanismos oficiales que facilitan en su página web oficial.
- No contestes en ningún caso a estos correos.
- Bajo ningún concepto sigas posibles enlaces que se puedan facilitar en el correo fraudulento ni descargues ficheros que traiga adjuntos.
- Elimínalo y, si lo deseas, alerta a tus contactos sobre este fraude.

5.3. AMENAZAS INTERNAS

Podemos distinguir entre agentes internos **malintencionados**, **engañados** y **descuidados**.

- Los usuarios internos **malintencionados** son los menos frecuentes, pero pueden causar grandes daños al tener acceso a los recursos desde dentro. Pueden ser empleados descontentos con su situación laboral o que han salido de la empresa de forma poco amistosa y cuyas credenciales de acceso no se han eliminado. Si tenían cuentas con privilegios de administrador, pueden provocar situaciones de alto riesgo.

- Por otro lado, como hemos visto, los usuarios internos también podemos ser «**engañados**» por terceros y esto es bastante frecuente. Si "picamos" en los engaños de la ingeniería social podríamos proporcionar datos confidenciales o contraseñas de acceso, con el riesgo que eso supone.

- El tercer tipo se corresponde con un usuario interno **descuidado** que por ejemplo presiona la tecla equivocada y borra o modifica información esencial de manera no intencionada.

En este sentido podemos considerar que un empleado que por falta de formación o concienciación comete un error, supone una amenaza interna. Los usuarios internos con falta de formación son el origen de muchas brechas de seguridad que serían evitables con sesiones de concienciación.

Factores de riesgo	Consejo
Falta de conocimiento y formación.	Dotar a los empleados de formación y procedimientos para prevenir y detectar problemas de seguridad y para actuar en caso de incidente, es esencial para la supervivencia de la empresa en el mundo digital.
Administración ineficaz de usuarios con privilegios.	Los privilegios de acceso total a sistemas, aplicaciones e información clave estarán reservados para ciertos usuarios que los necesiten por su cargo o por su función.

ACCIONES PARA MITIGAR EL RIESGO

- Actividades de formación y concienciación: https://www.incibe.es/protege-tu-empresa/kit-concienciacion.
- Establecimiento de políticas de seguridad y de normativas de usos de los activos corporativos.
- Cláusulas de confidencialidad en contratos de empleados y de terceros.
- Administración adecuada de roles y permisos con privilegios.
- Gestión de permisos de exempleados.
- Establecer un sistema de clasificación de la información.
- Soluciones antifraude y antimalware
- Actualización constante de los equipos y de las credenciales (contraseñas)
- No ejecutar programas o ficheros de origen dudoso
- No conectar a tus dispositivos un USB de origen desconocido

6.ESCENARIOS DE CIBERSEGURIDAD: TU PUESTO DE TRABAJO

Al hablar de ciberseguridad en el ámbito de nuestra empresa, somos conscientes de que debemos valorar todos los riesgos que nos pueden afectar. Sin embargo, es muy frecuente que los responsables nos centremos en implantar medidas de protección en la sala de servidores o en vigilar de las amenazas que provengan de Internet. Esto es muy importante, pero no debemos olvidar que la seguridad empieza por la protección del puesto de trabajo y que gran parte de los incidentes se deben al error humano.

6.1. USO DE SOFTWARE ILEGAL

Si utilizamos un software que sobrepasa las limitaciones establecidas en la licencia o sin licencia:

- Control por el fabricante de las limitaciones establecidas en las licencias.
- Imposibilidad de acceder a las actualizaciones que mejoran la aplicación.
- Hackers: Uso de las debilidades de las aplicaciones no actualizadas para acceder a los sistemas y sustraer la información.
- Asegúrate de descargar las aplicaciones de fuentes fiables:
  - Páginas web del fabricante.
  - Leer el apartado legal de la empresa.
  - Buscar sellos oficiales de confianza y guiarnos por los organismos oficiales.

6.2. ANTIVIRUS

Un antivirus es un programa informático que permite detectar o eliminar virus informáticos, impidiendo que infecten nuestro ordenador.
Debemos tener en cuenta que, si nuestro ordenador ha sido infectado por un virus, alguien con malas intenciones podría tomar el control de nuestro ordenador, robar nuestras claves de acceso al banco, acceder a los datos de nuestros clientes o incluso cifrar nuestro disco duro impidiéndonos acceder a la información que teníamos guardada. Por todo ello, es muy recomendable que mantengamos siempre debidamente actualizado el antivirus y que no lo inhabilitemos, para mantenernos en todo momento protegidos frente a este tipo de amenazas.

6.3. CIFRADO DE DATOS

También podemos aumentar la seguridad de nuestro puesto de trabajo cifrando los datos que consideramos más importantes para nuestra organización (por ejemplo, la base de datos de clientes).
Para ello se utilizan herramientas especializadas que, aplicando unos algoritmos matemáticos, hacen ilegibles los datos si no se conoce la contraseña de cifrado. Existen en el mercado infinidad de productos para ello y hoy en día prácticamente

todos los sistemas operativos incluyen de forma nativa herramientas que nos permiten cifrar nuestros datos.

El cifrado de la información es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
Se pueden dar los siguientes casos:

- Correo electrónico, dispositivos de almacenamiento o la nube: si se va a intercambiar información confidencial, es importante cifrarla, tanto si la información es compartida por correo electrónico, como si se almacena en la nube o sale de la empresa en un portátil o dispositivo extraíble

- Proveedores que presten servicio fuera de las instalaciones de la empresa o en caso de teletrabajo: Existen soluciones de comunicación segura como el uso de la Red Privada Virtual (VPN Virtual Private Network) que permite conectar tu ordenador a una red cifrando la información que se comunica.

- Transferencias desde y hacia la empresa: A la hora de contratar un servicio con un proveedor externo hay que determinar muy bien quién corre con los gastos del servicio de acceso seguro.

6.4. COPIAS DE SEGURIDAD

Sin duda, la copia de seguridad de los datos es una de las mejores prácticas para evitar pérdidas de información por cualquier motivo, ya sea un virus, un borrado accidental o un archivo que se corrompe y al cual ya no se puede acceder, etc. Y tan importante como salvaguardar nuestra información, es comprobar que podemos recuperarla fácil y rápidamente.

6.5. CONTROL DE CONTRASEÑAS

Todos los empleados deben conocer que para que una contraseña sea realmente útil tiene que ser personal e intransferible.
Por ello son buenas prácticas de seguridad: utilizar contraseñas difíciles de adivinar, no escribir la contraseña en ningún lugar, no compartir la contraseña con nuestros compañeros y por último, cambiar la contraseña con cierta periodicidad.

https://www.youtube.com/watch?v=kvbYbsGoofo&feature=youtu.be

6.6. BLOQUEO DE ORDENADOR

Otra mala costumbre muy común en las empresas es dejar el equipo desbloqueado y sin custodia.
Un equipo desbloqueado es sinónimo de un equipo sin contraseña, por lo que cualquiera puede acceder a la información del equipo.

Para solucionar esta mala práctica, todos los empleados deben conocer y aplicar una sencilla norma: bloquear el ordenador siempre que se ausenten del puesto de trabajo.

6.7. POLÍTICA DE MESAS LIMPIAS

Igualmente, debemos marcarnos como uno de los objetivos para la protección de nuestro puesto de trabajo, que nuestra información esté siempre bajo nuestro control. En concreto, no debemos dejar nunca documentación con información sensible desatendida, estará siempre custodiada por personal responsable.

Recuerda igualmente guardar bajo llave fuera de la jornada laboral toda la documentación y soportes que contengan información para que no queden al alcance de cualquiera que pase por ahí.

Otro caso de documentación desatendida se da cuando enviamos un documento a la impresora y la recogemos más tarde, o que lo imprimimos a través de la impresora de otro departamento. Durante ese tiempo la documentación permanece a disposición de otros usuarios, que pueden recogerla accidental o intencionadamente. Para evitarlo, es recomendable retirar al momento la información impresa o que se reciba por fax.

6.8. POLÍTICA DE USO DE LOS SISTEMAS CORPORATIVOS

Para terminar, todos los empleados deben conocer que sólo han de utilizar software autorizado y legal en el ámbito de la organización.
Además, es esencial mantener actualizadas todas las herramientas y sistemas que utilicemos, para impedir el acceso no autorizado a nuestros sistemas por parte de ciberdelincuentes que aprovechan los agujeros de seguridad del software.

6.9. USO DEL CORREO CORPORATIVO

- El correo es para uso profesional exclusivamente, pudiéndose permitir el uso personal de forma excepcional.
- Está prohibida la difusión de contenidos contrarios a las leyes o que vulneren los derechos de terceros.
- No se deben enviar correos tipo spam.
- Está prohibido facilitar el acceso a tu cuenta a otra persona.
- No abrir correos o ficheros adjuntos sospechosos.

Ejemplo de cláusula para empleados (para proteger uso del correo corporativo)
"*El uso del correo electrónico debe realizarse en el ámbito profesional.*
Queda prohibido el uso del correo electrónico con contenidos inadecuados, ofensivos o no acordes con la Ley. La información que se envíe a otros destinatarios fuera de la empresa o proveedor debe estar autorizada.
Las credenciales de acceso al correo y cuenta no deben compartirse.
Se ha de poner a los destinatarios en copia oculta para preservar la privacidad de su email"

7.ESCENARIOS DE CIBERSEGURIDAD: EQUIPAMIENTOS Y MEDIDAS DE SEGURIDAD

7.1. SEGURIDAD EN LAS REDES PRIVADAS

¿QUÉ ES UNA VPN?

Una VPN es un servicio que permite el acceso remoto a la red interna de la organización y a los recursos corporativos, como pueden ser el correo electrónico, el servidor de ficheros o incluso aplicaciones de «escritorio» como el CRM, ERP o cualquier otra aplicación departamental. Este acceso a través de internet de forma segura, permite la movilidad del trabajador o incluso interconectar sedes separadas geográficamente. Una VPN crea un túnel a través de internet mediante cifrado seguro, de forma que podemos acceder desde cualquier lugar a los servicios y documentos internos de nuestra compañía.

Pero, ¿cuáles son las ventajas que nos proporciona implementar una VPN?

- **Acceso remoto seguro**.
- **Teletrabajo**
- **Control de accesos**

Sin embargo, no todos son ventajas cuando implementamos una VPN, también conlleva una serie de desventajas como las que planteamos a continuación:

- **Coste económico y temporal** que supondría instalar, configurar y poner en marcha un servicio VPN.
- **Reestructuración a nivel de red** (filtrados, rutas, etc.) que se han de llevar a cabo por parte del equipo de comunicaciones.
- **Configuración de los clientes** (móviles, PC, etc.) de los empleados para que puedan acceder a través de VPN haciendo uso de las aplicaciones correspondientes. Para ello, se ha de generar un certificado y una contraseña de acceso para cada uno de los empleados.

Es importante que los accesos remotos a los recursos internos se hagan de una forma segura y totalmente controlada. Utilizando una VPN podemos garantizar las dos cosas: seguridad; por el cifrado que se aplica a la conexión y a la información que se remite a través del túnel, y control; ya que permite conocer en todo momento quién ha accedido, cuándo, desde dónde y las acciones que ha realizado.

7.2. FIREWALL

Un cortafuego es un sistema (puede ser hardware o software o una combinación de ambos) que, mediante reglas previamente establecidas, bloquea el acceso no autorizado a nuestra red y permite la salida autorizada de información de nuestros sistemas.
Los cortafuegos son parametrizables, es decir, podemos establecer quién puede conectase con nuestra red, qué datos pueden entrar y salir, dónde pueden conectarse los usuarios.
Básicamente la función del cortafuego es analizar todo el tráfico de red que intenta entrar o salir de nuestra red y siguiendo las reglas de seguridad que hemos establecido, permitir que ese tráfico pase o no.

En general hay dos tipos de políticas de cortafuegos:

- Restrictiva: Por defecto se impide todo el tráfico de datos, siendo necesario autorizar expresamente cada una de las acciones permitidas (tráfico web, correo electrónico). Esta política, aunque es más complicada de gestionar es la que más seguridad nos aporta.

- Permisiva: Por defecto se permite todo el tráfico de datos, no siendo necesario autorizar expresamente cada una de las acciones permitidas, pero si prohibir las no autorizadas (por destino o por tipo de tráfico, por ejemplo)

7.3. SERVICIOS DE TELEFONÍA IP EN INTERNET

El servicio de telefonía IP nos permite hablar por teléfono con otra persona sin necesidad de tener una línea convencional de telefonía, usando internet para la comunicación (Skype, Hangaouts, llamadas de Whatsapp). Sus principales características:

- No es necesario que el emisor y receptor tengan un servicio de telefonía IP, pudiendo uno de los dos hablar desde la red telefónica convencional.

- Como es un servicio que se basa en la transmisión de paquetes de datos por Internet, no es necesario que los interlocutores dispongan de un terminal fijo para hablar, existiendo aplicaciones de ordenador que permiten hablar a sus usuarios (Skype)

- Las comunicaciones a través de voz IP permiten la transmisión de imágenes, permitiendo realizar videoconferencias.

Para evitar que la empresa pueda ser atacada por este servicio, hay que implantar algunas medidas de seguridad:

- Separar la red de voz IP de la red de datos
- Cifrar los paquetes de datos de voz IP
- Implantar cortafuegos y antivirus en la red de voz IP
- Monitorizar la red de voz IP para identificar comportamientos sospechosos (de los datos, no de los trabajadores)

7.4. CIBERSEGURIDAD EN LAS REDES WIFI

Para minimizar la probabilidad de ser víctima de un ataque que pueda poner en riesgo la wifi, vamos a ver los siguientes consejos:

- Cambiar la contraseña de acceso a la página de administración del router.
- Utilizar cifrado WPA
- Cambiar la contraseña por defecto para acceder a tu WIFI desde tus dispositivos móviles
- Cambiar el nombre de la WIFI o SSID
- Verificar periódicamente quién se conecta a tu red WIFI

1. Utiliza cifrado WPA2

    - Siempre que tu dispositivo lo permita, debes hacer uso de cifrado WPA2, ya que este tipo de cifrado de la comunicación en más seguro y difícil de piratear. Para configurarlo, en tu router accede a la sección "seguridad WIFI" y selecciona el método WPA2.

- Cambiar la contraseña por defecto para acceder a tu wifi desde dispositivos móviles

    - Las claves que vienen de serie no son las más adecuadas, ya que pueden ser predecibles, conocerlas el proveedor o no ser robustas, por lo que es recomendable cambiarlas.
    - Para ello, accede al apartado "seguridad WIFI" y configura que una contraseña de al menos 12 caracteres, alfanumérica y mayúsculas y minúsculas

3. Cambiar el nombre de la wifi o SSID

    - Normalmente el SSID viene definido por defecto y es el nombre que verán todos los dispositivos al buscar las redes wifi del área. Este SSID debe ser sustituido por uno que no sugiera cuál es nuestro operador y que no guarde relación con la contraseña de acceso a la red. Podrás modificar el nombre de la red en la página de configuración de tu router.

4. Verificar periódicamente quién se conecta a tu red wifi:

   - Hay varios síntomas que pueden indicar la presencia de un intruso en la red wifi de tu empresa. Selecciona uno de los iconos para conocerlo.

   - Con todos tus ordenadores y dispositivos móviles apagados, mira las luces de actividad del router. Un parpadeo rápido y continuado indica que hay dispositivos conectados y transmitiendo información o la sensación de una pérdida de velocidad significativa.

AMENAZAS CUANDO NOS CONECTAMOS A WIFIS PÚBLICAS

Estas son las amenazas a las que podemos estar expuestos cuando utilizamos las redes wifi.

Robo de información o sniffing	Una configuración deficiente de la red wifi podría permitir a un atacante robar la información transmitida a través de la red.
Conexión directa con nuestros dispositivos	Un atacante podría acceder a nuestros equipos conectados a la red y por tanto a toda nuestra información.
Vulnerabilidades conocidas	Tanto los routers, como el tipo de cifrado, o funcionalidades como WPS, podrían tener agujeros de seguridad. También es posible que utilicen contraseñas débiles o por defecto. Un atacante podría aprovecharse de ello para entrar en nuestra red y acceder a nuestra información.
Creación de redes "espejo"	Un atacante podría crear una red inalámbrica con el nombre de una res en la que el dispositivo confía para que éste se conecte. De esta manera, su comunicación y la información que contiene quedarían expuestas.
Redes Públicas	Al conectar nuestros dispositivos a redes ajenas (hoteles, aeropuertos) los exponemos a posibles deficiencias de seguridad que éstas puedan tener.

Por otra parte, también la wifi de nuestra oficina puede ser vulnerable. Acceder de forma no autorizada a una red cableada es complicado, ya que hay que tener acceso físico a los equipos de la red para conectar un cable. Sin embargo, acceder a una red inalámbrica, donde la comunicación se realiza mediante ondas de radio, es más sencillo.

Debido a esto, debemos poner especial cuidado en **blindar** la red wifi de nuestra organización para evitar cualquier intento de acceso no autorizado a la misma.

Estas son las recomendaciones para configurar la seguridad de nuestras redes wifi.

Cambiar contraseña por defecto del router	Debemos establecer una contraseña robusta y cambiarla con frecuencia
Cambiar nombre de la red (SSID/ESSID) por defecto y coultarlo	Ocultar el nombre de la red hace que no se muestre a otros dispositivos. Así evitaremos que alguien externo pueda intentar conectarse. Los nombres por defecto pueden dar información sobre nuestra tecnología, nuestro Proveedo, etc Si no lo ocultamos al menos debemos cambiarlo
Actualizar firmware del router	Las actualizaciones suelen incluir mejoras de seguridad
Desactivar WPS	WPS es un mecanismo que facilita la conexión de dispositivos a la red. Desactívalo pues es vulnerable y puede facilitar también la conexión de terceros a la red
Cambiar la contraseña de acceso al panel de configuración del router	Las contraseñas que traen por defecto los routers para acceder al panel de configuración se encuentran fácilmente buscando en Google el modelo y fabricante. Si no la cambias, cualquier podrá acceder a este panel y cambiar la configuración del router sin restricciones
Elige un protocolo de cifrado seguro	Utiliza en todo momento el protocolo más seguro de cifrado de las comunicaciones. WPA2 es actualmente el más seguro

8.ESCENARIOS DE CIBERSEGURIDAD: LOS DISPOSITIVOS MÓVILES

La movilidad conlleva riesgos de acceso no permitido a información de nuestra organización, ya sea por pérdida o robo. Para minimizar este riesgo, se deben establecer unas mejores prácticas para proteger estos dispositivos con independencia del sistema operativo que esté utilizando.

Podemos tener dos tipos de ataques: In situ (con el fin de vender el dispositivo en el mercado negro) o ciberataques (para robar la información o controlar el dispositivo)

¿Cómo nos protegemos de los ciberataques?

Los ciberataques pueden ser:

- Infección del dispositivo a través de malware
- Ataques de phishing a través de mensajes o web
- Aprovechamiento de vulnerabilidades de nuestro dispositivo
- Acceso a un falso punto de acceso wifi (rogueAP) al que nos atrae un atacante para robarnos la información
- Abuso de permisos de aplicaciones

¿De qué manera nos afectan estos ataques?

- Pérdida de confidencialidad: Robo de información contenida en el dispositivo
- Pérdida de integridad: Modificación de los archivos o documentos almacenados en nuestro dispositivo
- Pérdida de disponibilidad: Nuestro dispositivo no funciona correctamente

¿Cuáles son las intenciones de los atacantes?

- Robo de información empresarial en beneficio suyo o de terceros: daños económicos o pérdida de clientes
- Robo de información personal y posterior extorsión para recuperar los datos
- Seguimiento del propietario del dispositivo móvil a través de GPS o WIFI: obtener información de los lugares que frecuentamos o nuestras rutinas
- Utilizar nuestro dispositivo para sus propios fines: Realizar ataques desde él.

8.1. RECOMENDACIONES BÁSICAS

- Configura tu dispositivo para que se **bloquee automáticamente** pasado cierto tiempo de inactividad.
- Bloqueando el acceso al dispositivo por **contraseña**, únicamente su titular podrá acceder a los datos que contiene.
- Para evitar que la información que hay en tu dispositivo pueda ser leída por una persona ajena, existen programas que permiten **cifrar la información**, de forma que sólo pueda ser visualizada por ti mediante la introducción de un código secreto.
- Si pierdes o te roban el teléfono móvil, deberás **denunciar** este hecho. Con la denuncia podrás ponerte en contacto con tu operador y **solicitar el bloqueo tanto de la tarjeta SIM como del teléfono**.
- En estos casos, también te recomendamos contar con un **servicio o aplicación de borrado remoto de la información**, para evitar que personas no autorizadas puedan acceder a ella.
- Realiza **copias periódicas** de la información que tienes almacenada en el dispositivo.
- Es imprescindible la instalación de un **antivirus** para prevenir la infección por malware del dispositivo y su posible transferencia al resto de sistemas.
- Recuerda que la **instalación de aplicaciones** dentro de tu dispositivo móvil debe proceder **sólo de fuentes fiables**.
- Igualmente, la **actualización del software instalado** es importante para corregir los fallos de seguridad que pudieran detectar los fabricantes.
- **Evita siempre que sea posible el uso de redes wifi públicas**. Cualquiera podría capturar nuestro tráfico, recopilando información confidencial y contraseñas almacenadas en tu dispositivo.
- Si lo haces, aplica medidas de seguridad como usar una VPN.

8.2. COPIAS DE SEGURIDAD Y CIFRADO

Las **copias de seguridad o backups** son copias de respaldo de la información almacenada en el teléfono (lista de contactos, fotos, información guardada de correos corporativos o personales) Los backups nos garantizan poder recuperar la información importante en caso de que surja un imprevisto. Se puede realizar en local o en la nube. Permite sincronizar los contactos, el correo, el calendario o las fotografías de manera instantánea.

8.3. ACTUALIZACIÓN DEL SISTEMA Y DE LAS APLICACIONES

Las actualizaciones además de mejorar las capacidades del sistema y de las aplicaciones, solucionan fallos de seguridad y vulnerabilidades que, de no corregirse, pueden poner en peligro el dispositivo y la información almacenada en él.

8.4. LOCALIZACIÓN DE DISPOSITIVOS EN CASO DE PÉRDIDA

- **PREY:** Disponible para iPhone y Android. Tiene la funcionalidad de hacer fotos a distancia con la que podemos capturar la imagen del ladrón

- **ADMINISTRACIÓN DE DISPOSITIVOS**: Opción dentro de las opciones de seguridad en los teléfonos Android. Permite localizarlo, hacerlo sonar o borrar los datos, desde una página web

- **LOOKOUT MOBILE SECURITY:** Disponible para iPhone y Android. Guarda la posición GPS antes de que el móvil se quede sin batería. También detecta versiones inseguras o antiguas de iOS

8.5. CONEXIONES INALÁMBRICAS EN DISPOSITIVOS MÓVILES

POSIBLES ATAQUES A TRAVÉS DE LAS CONEXIONES INALÁMBRICAS:

WIFI

- **Man in the Middle (MITM):** Un usuario malintencionado se pone a escuchar entre el dispositivo e internet y obtiene información de las acciones que realizamos con él y la información que enviamos (datos bancarios, redes sociales, información confidencial de la empresa)
- **Robo de información pasivo:** Pueden obtener datos de nuestra ubicación a través de las señales que el dispositivo envía para buscar redes wifi cuando no está conectado.

BLUETOOTH

- **Bluejacking:** Envían spam a la víctima mediante notas, contactos o imágenes. Puede resultar peligroso y convertirse en una denegación de servicio dirigida a un objetivo o a un espacio (por ejemplo, un bar).

- **Bluesnarfing:** Aprovecha vulnerabilidades conocidas para obtener información del dispositivo atacado.

- **Bluebugging:** Aprovecha bugs (fallos de programación) para ejecutar comandos en el terminal y controlarlos.

NFC

- Ejecución de programas maliciosos: ejecuta código en terminales Android simplemente acercando una etiqueta NFC al dispositivo.

- Pagos sin autorización: Realiza compras por proximidad sin consentimiento**.**

- Transmisión de datos sin cifrar: Lee datos como el nombre, apellidos, número de tarjeta o transacciones realizadas.

8.6. DESCARGA DE APLICACIONES SEGURAS

Las aplicaciones móviles aprovechan la funcionalidad de los dispositivos para ofrecernos todo tipo de utilidades: juegos, redes sociales, envío de correos, información
Para poder funcionar, las aplicaciones necesitan una serie de permisos específicos del dispositivo (uso de geolocalización, acceso a cuentas, contactos, teléfono, grabar audio o video) pero a veces piden permisos que no tienen nada que ver con la funcionalidad de la aplicación.
Cuando descargues aplicaciones revisa la información sobre permisos (a qué le vamos a dar acceso) y comprueba que es coherente con la funcionalidad que ofrecen.

Si quieres comprobar los permisos de tus aplicaciones instaladas utiliza
esta herramienta: CONAN Mobile

https://www.osi.es/es/conan-mobile

¿CÓMO IDENTIFICAR APLICACIONES FRAUDULENTAS?

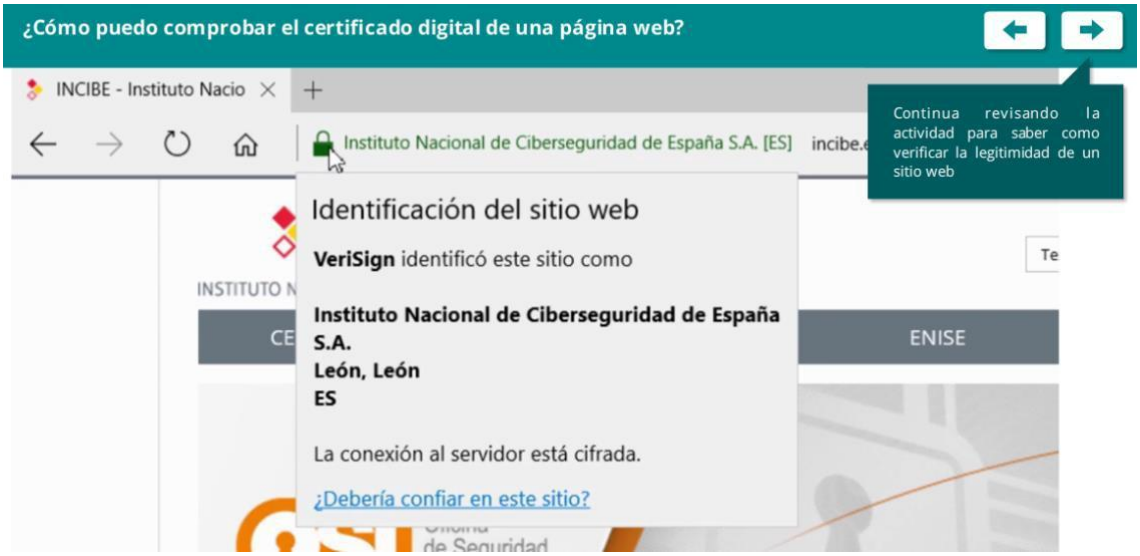
- Comprobar el nombre de los desarrolladores para comprobar la legitimidad de la aplicación y visitar su página para ver si son de fiar.
- Comprobar el rating para ver cómo está posicionada.
- Revisar los comentarios de otros usuarios.
- Leer la descripción de la aplicación y sus permisos: para detectar engaños, faltas de ortografía que nos puedan hacer dudar.
- Comprobar capturas de pantalla por si vemos algo raro.
- Ver aplicaciones alternativas que ofrecen lo mismo.

9.ESCENARIOS DE CIBERSEGURIDAD: NAVEGACIÓN SEGURA

¿CÓMO PUEDO SABER SI UNA PÁGINA WEB ES LEGÍTIMA?

Debemos comprobar su certificado digital: El certificado digital es un elemento de seguridad emitido por una entidad certificadora autorizada que garantiza que la página es realmente de la entidad que dice ser. Así se puede preguntar a una página qué certificado digital tiene y quién se lo ha otorgado.

- Verificar HTTPS importante: colores y candado



- Otra opción es comprobar si la empresa posee sede física y número de teléfono
- Otra recomendación, leer la política de privacidad del sitio web e informarse de las condiciones de la contratación de la página
- Otra sería conservar toda la información relativa a la transacción hasta que termine el periodo de garantía del producto

10.ESCENARIOS DE CIBERSEGURIDAD: CLOUD COMPUTING

10.1. CONTRATACIÓN DE APLICACIONES EN LA NUBE

Cuando nuestra organización va a contratar un servicio, es necesario reflexionar sobre qué solicitamos al proveedor, a qué le daremos acceso, qué datos se compartirán y qué forma de prestación es la más adecuada. Así podremos elegir al proveedor que mejor se adapte a nuestras necesidades.
En concreto, a la hora de elegir un proveedor, debemos valorar y comparar diferentes cuestiones de seguridad:

- Qué tratamiento necesitamos que realicen con los datos.
- Dónde, en qué país, se van a ubicar los datos, sobre todo si son datos personales.
- Cuáles serán las opciones de portabilidad de los datos cuando termine el servicio.
- Las características de los Servicios que nos ofrecen (horario, capacidad, rapidez de acceso, resolución de incidentes).

Por último, qué contienen los acuerdos de nivel de servicio con el proveedor. Es decir, qué compromisos adquieren y cuales quedan bajo nuestra responsabilidad. Los podemos encontrar con uno de estos 3 tipos:

- Acuerdo Unilateral, es decir que es impuesto y no se puede negociar. Este tipo de acuerdo es propio de los servicios en nubes públicas.
- En segundo lugar, se encuentra el acuerdo parcialmente definido, en el cual se pueden negociar algunas cláusulas y otras no. Esta modalidad es frecuente que nos la ofrezcan para servicios en nubes híbridas y privadas.
- Por último, el acuerdo negociable, que es ajustable en todos sus términos y es el utilizado por los servicios de proveedores de nubes privadas.

CÓMO SABER QUE LAS MEDIDAS SE ESTÁN CUMPLIENDO CORRECTAMENTE

- El cliente tiene derecho a acceder a los registros que permiten saber quién o quiénes han accedido a los datos.
- El cliente de cloud puede requerir que un tercero audite la seguridad según los estándares establecidos.
- El proveedor puede acreditar haber superado una certificación de seguridad adecuada.
- El proveedor del servicio debe notificar al cliente sobre cualquier incidente de seguridad.

CÓMO RECUPERAR LOS DATOS UNA VEZ QUE SE EXTINGUE LA RELACIÓN CON EL PROVEEDOR

El proveedor debe entregar toda la información de forma segura al cliente para que éste la guarde en sus propios sistemas o la transfiera a otro proveedor.

CÓMO SABER SI SE HAN BORRADO LOS DATOS CUANDO SE CESA LA RELACIÓN CON EL PROVEEDOR

Antes de extinguir el contrato deben establecerse las medidas adecuadas que aseguren el borrado seguro de datos cuando el cliente lo desee o cuando el contrato finalice. Esto se puede hacer a través de una certificación de destrucción que emite el proveedor.

10.2. AMENAZAS DEL CLOUD COMPUTING

ACCESO NO AUTORIZADO

Si no se toman las medidas de seguridad adecuadas con el proveedor de cloud no habrá posibilidad de controlar los accesos de los empleados a la información de la organización, lo que puede provocar robo de datos, inyección de código malicioso

AMENAZAS INTERNAS

Cuando los trabajadores salen de la organización (fin de contrato o despido) se debe notificar al proveedor de servicios cloud su baja para evitar que siga teniendo acceso a la información

INTERFACES SEGURAS: PROBLEMAS DERIVADOS DEL USO DE TECNOLOGÍAS COMPARTIDAS

El problema aparece cuando las interfaces que proporciona el proveedor para acceder a la plataforma en la nube no son del todo seguras y presentan fallos de seguridad que pueden ser explotados por terceros.

FUGA DE INFORMACIÓN

Si nuestra organización lleva a cabo muchas operaciones con cliente al cabo del día y éstas no están cifradas, puede producirse una fuga de información

SUPLANTACIÓN DE IDENTIDAD

Esto sucede cuando a una persona le roban las credenciales de usuario y aceden a la plataforma en su nombre, pudiendo manipular la información.

DESCONOCIMIENTO DEL ENTORNO

Si el personal encargado de implantar las políticas se seguridad no conoce el entorno cloud, estás no serán eficientes.

ATAQUES DE HACKING

Sucede cuando una persona maliciosa intenta robar o acceder a la información que maneja alguno de los empleados de nuestra organización o el administrador de la plataforma.

11.ESCENARIOS DE CIBERSEGURIDAD: TU PÁGINA WEB

Si tienes una página web o una tienda online también puedes sufrir incidentes de seguridad que pueden afectar de forma muy negativa a la imagen de tu empresa o a los propios clientes.

¿POR QUÉ QUERRÁN ATACAR NUESTRA TIENDA o WEB?

- Para robar nuestros datos de clientes, sus contraseñas, datos de pago, correos electrónicos y utilizarlos, publicarlos o venderlos.
- Utilizar nuestro servidor web para simular ser otra organización fraudulenta o instalar publicidad engañosa.
- Dejar fuera de servicio nuestra web para desprestigiarnos.
- Utilizar nuestro servidor web para reivindicar ideas políticas o sociales.
- Robar nuestras contraseñas de acceso a otros sistemas, acceder y utilizarlos para fines maliciosos (spam, distribución de malware, lanzar ataques de denegación de servicio)

10.1. POSIBLES ATAQUES A NUESTRA PÁGINA WEB

Las amenazas a nuestra tienda online utilizan bien el factor humano bien el fallo tecnológico o una combinación de ambos.

Los ciberdelincuentes tienen en sus manos muchas herramientas para aprovecharse de estos fallos y lo hacen. Unos para ganar dinero, otros por prestigio o por diversión/reto.

INGENIERÍA SOCIAL: MENSAJES DE PHISHING Y SPEAR PHISHING

Algunos ejemplos serían: recibir y abrir un mail personalizado que nos infecta porque nos convence para descargar un documento infectado o recibir un mensaje de phishing que suplanta al administrador de un servicio y nos dirige a una web donde supuestamente desbloquearemos la cuenta introduciendo nuestras credenciales de acceso, pero en realidad se las habremos dado al ciberdelincuente.

FALLO TECNOLÓGICO: PHISHING A NUESTRA WEB

También se llama phishing al ataque a nuestro servidor web para que muestre una página falsa de un banco, por ejemplo, con la que pescar credenciales de usuarios. En este caso suplantan la web de otra entidad aprovechándose de un fallo en nuestro servidor web. Nos infectan con un troyano para robar las contraseñas de acceso al panel de control de la web y la sustituyen por la web falsa de un conocido banco.

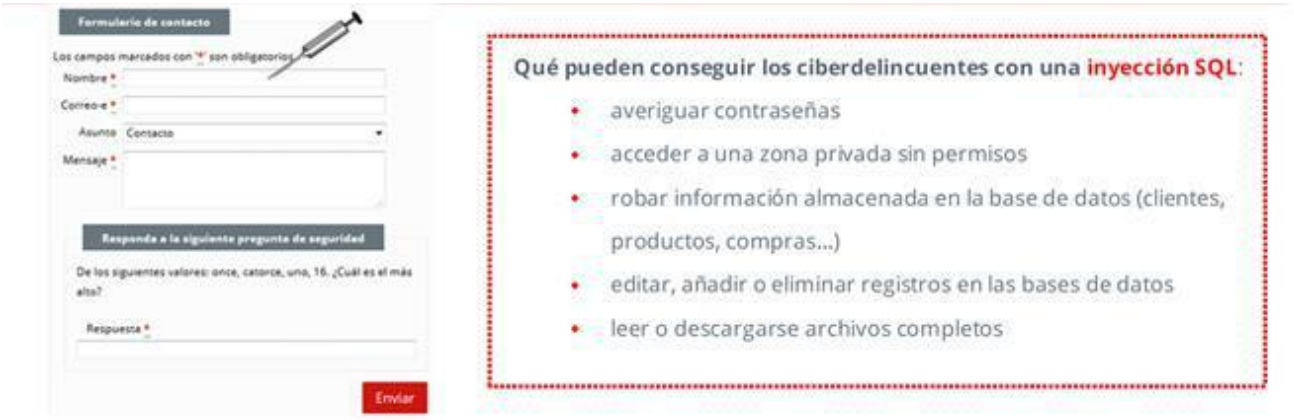
Con un correo de phishing con cualquier pretexto falso invitan a los usuarios a ir a esta dirección y capturan sus claves de acceso o de pago

FALLO TECNOLÓGICO: INYECCIÓN SQL

Los ataques de inyección SQL se aprovechan de fallos en la programación de las consultas a la base **de datos de nuestra web**, como formularios o los sistemas de acceso de usuarios (login).

Existen vulnerabilidades y fallos de diseño conocidos, y que se pueden evitar, en la forma de tratar los datos que introduce el usuario.

Los desarrolladores deben extremar las precauciones cuando diseñan la web para evitar que los delincuentes puedan aprovecharse de estos fallos.



FALLO TECNOLÓGICO: CROSS SITE SCRIPTING (XSS)

Este tipo de ataques se aprovechan de que los navegadores de los visitantes de nuestra web comparten datos entre aplicaciones y con el servidor.

Mediante técnicas de forgery o falsificación suplantan una aplicación o servicio real, para engañar a la víctima y hacer que se ejecute algún tipo de código malicioso en el contexto de su navegador.

Qué permiten:

- Robo de **cookies de sesión** (las del carrito de la compra en tiendas online p. ej.) para capturar la sesión del usuario y:
  - cambiar su contraseña
  - realizar compras en su nombre
  - fisgar sus datos financieros y transacciones
- Ejecución de **código** malicioso.
- Dirigir al usuario hacia **páginas fraudulentas** para robarles las credenciales de acceso a su banco o pasarelas de pago.

FALLO TECNOLÓGICO O INGENIERÍA SOCIAL: DEFACEMENT

De esta forma, los hackers se aprovechan de nuestros recursos para su beneficio político o publicitario además de dañar nuestra imagen. En este caso su motivo es reivindicativo más que el robo de datos. (Caso Anonymous)

10.2. ATAQUES A NUESTRA IDENTIDAD Y REPUTACIÓN ON LINE

En estos casos utilizan nuestra marca para engañar a los usuarios para que se suscriban a servicios Premium, etc. Son ataques contra nuestra identidad digital y nuestra reputación.

La identidad digital corporativa puede ser definida como el conjunto de información sobre una empresa expuesta en Internet (Datos, imágenes, registros, noticias, comentarios.) que conforma una descripción de dicha organización en el plano digital.

La reputación corporativa es el concepto que mide cuál es la valoración que hace el público de una compañía. La reputación online puede definirse como la valoración alcanzada por una empresa a través del uso, o mal uso, de las posibilidades que ofrece internet.

¿Cómo gestionar nuestra identidad y reputación online?

Para gestionar adecuadamente nuestra identidad y monitorizar nuestra reputación online, debemos tener en cuenta estas situaciones que pueden influir negativamente:

- La utilización no consentida de nuestra marca
- Publicaciones por terceros de informaciones negativas
- Fuga de información con repercusiones legales
- Suplantación de identidad con phishing y pharming (redireccionan a páginas que suplantan al original)
- Ataques de denegación de servicio.

10.4. QUÉ HACER EN CASO DE DESASTRE

Es importante saber detectar los incidentes potencialmente peligrosos, tener un plan de prevención ante este tipo de incidentes y tener los medios y capacidad adecuados para responder a ellos.

Veamos a continuación algunas **medidas** que nos ayudarán a **detectar** este tipo de ataques:

- Comprobar la **apariencia** y **funcionalidad** de la web;
- Revisar los **sistemas de monitorización** y el log de conexiones http y ftp;
- Comprobar desde que **IP** se han conectado vía **FTP**;
- Comprobar el **listado de ficheros** en busca de **cambios**: directorios y subdirectorios, permisos, bases de datos, nuevos archivos, etc.
- Comparar el **código fuente de la tienda** contra copias de seguridad y
- Comprobar si hemos recibido alguna **notificación** de proveedores de servicios de alojamiento, de clientes o de terceros.

En cuanto a la respuesta ante incidentes, el método más fiable contra la pérdida de datos es hacer copias de seguridad con frecuencia. Recuerda, "un backup a buen recaudo será siempre nuestro mejor amigo en caso de desastre".

En caso de sufrir un incidente de ciberseguridad que afecte a nuestra tienda online o a nuestra web, ¿cómo debemos **reaccionar**?

Debemos adoptar las siguientes **medidas**:

- Poner off-line la tienda o la web y contactar con el proveedor;
- Obtener una copia de la web comprometida (evidencia forense del ataque) y guardar la cadena de custodia para hacer una denuncia;
- Denunciar, aportando las evidencias;
- Pasar el antivirus, cambiar las contraseñas y restaurar el servicio con una copia de seguridad y
- Comprobar si nuestra página web o dirección IP está en alguna lista negra y, si es así, notificarlo al proveedor.

También tomaremos las siguientes medidas:

- Exigir seguridad cuando contratemos servicios tecnológicos como el alojamiento o el desarrollo web.
- Proteger nuestra tienda o nuestra web como si fuera nuestro castillo.
- Asegurarnos de que las comunicaciones tanto con clientes como con proveedores están cifradas y autenticadas.
- Concienciar a nuestros empleados.
- Auditar la seguridad de nuestra tienda o nuestra web con frecuencia.
- Tener un Plan B.

Recuerda también que:

- la selección de proveedores TIC ha de hacerse siempre además de con criterios económicos, de calidad y de funcionalidad, con criterios de seguridad;
- el desarrollador o el proveedor deben ser conscientes de ello y demostrarnos su compromiso con la seguridad y nosotros debemos exigirlo.

11. GESTIÓN DE LOS INCIDENTES DE SEGURIDAD

11.1. ¿CÓMO RESPONDER ANTE UN INCIDENTE DE SEGURIDAD?

FASE 1: PREPARACIÓN

En esta fase hay que estimar las necesidades para la gestión de incidentes:

- Personal que va a realizar la gestión de incidentes.

- Documentación de los sistemas y redes que se usan en la empresa: Definir cuál es la actividad "normal" para permitir detectar actividades sospechosas que sean indicios de incidentes. Otra cosa sería: registrar los contactos de terceras partes. Por ejemplo, si tenemos una web que la mantiene un proveedor, en caso de incidencia hay que tener identificado el responsable en el proveedor.

- Centros de respuesta ante incidentes de organismos externos en los que apoyarnos para la gestión de incidentes: CERT/CSIRT.

También hay que establecer procedimientos de gestión:

- Definir una política de gestión de incidentes, así como el procedimiento a seguir en caso de que ocurran.

- Monitorización o catálogo de las incidencias que tengan mayor probabilidad de ocurrir o mayor impacto previsible en la empresa, de forma que podamos predefinir pautas de actuación en caso de materializarse.

FASE 2: DETECCIÓN Y ANÁLISIS

Es evidente que no se podrá gestionar un incidente si éste no se ha detectado.
Los signos de un incidente pueden ser de dos tipos:

- Signos indicadores: Son aquellos que ponen de manifiesto que un incidente ha ocurrido o puede estar ocurriendo, por ejemplo:

    - Alertas de sensores de un servidor.
    - Una alerta del antivirus
    - La caída de un servidor o sistema
    - Accesos lentos

- Signos precursores: son los que nos pueden indicar que un incidente tiene posibilidades de ocurrir en el futuro, por ejemplo:

    - La detección de un escáner de puertos
    - El resultado del análisis de vulnerabilidades
    - Las amenazas de ataque por parte de hackers

FASE 3: IDENTIFICACIÓN DEL INCIDENTE

El primer paso consiste en identificar el tipo de incidente ocurrido y si ha ocurrido más de uno, priorizarlos dependiendo de su gravedad. Una de las clasificaciones más comunes se basa en el origen del incidente:

- Un usuario no autorizado accede al sistema o a información interna.
- Se impide el correcto funcionamiento de servicios tales como DNS, correo electrónico, navegación web.
- El sistema ha sido comprometido por una infección de virus, troyanos, spyware.
- Extraer información personal de una persona o empresa con la finalidad de obtener un beneficio económico.

FASE 4: NOTIFICACIÓN DEL INCIDENTE

El proceso de notificación de incidentes de seguridad pasa por las siguientes acciones: reportar, notificar y registrar el incidente e iniciar el seguimiento en un evento de gestión. En función del tipo de incidente, éste se asignará y escalará a las personas que procedan para asegurar, en la medida de lo posible, su análisis, resolución y cierre.

FASE 5: CLASIFICACIÓN Y PRIORIZACIÓN DE INCIDENTES

Una vez detectado un incidente, hay que clasificarlo. Se pueden usar para la clasificación los siguientes atributos:

- Tipo de amenaza: código dañino, intrusiones, fraude
- Origen de la amenaza: interna o externa
- Categoría de seguridad o criticidad de los sistemas afectados
- El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en consecuencia, sus privilegios de acceso a la información sensible o confidencial.
- El número y tipología de los sistemas afectados.

Las características del incidente, tipo de recursos afectados y criticidad de los mismos determinará el impacto potencial sobre la organización de la empresa, además del orden de prioridad en el tratamiento, en caso de detectarse más de un incidente de forma simultánea.

Priorizar el incidente según su criticidad

Estas tablas muestran un modelo para **tipificar y priorizar los incidentes**:

Clase de incidente	Tipo de incidente
Ataque	Ataque dirigido
	Modificación del sitio web
Código dañino	Infección extendida
	Infección única
Denegación de servicio (DoS)	Exitosa
	No exitosa
Acceso no autorizado, robo o pérdida de datos	Acceso no autorizado
	Robo o perdida de equipos
	Pérdida de datos
Pruebas y reconocimientos	Pruebas no autorizadas
	Alarmas de sistemas monitorización
Daños físicos	Daños o cambios físicos no autorizados a los sistemas
	Fuego
	Inundación
Abuso de privilegios y usos inadecuados	Abuso de privilegios o de políticas de seguridad de la información
	Infracciones de derechos de autor o piratería
	Uso indebido de la marca

Nivel de criticidad	Tiempo para registro interno
BAJO	Lo antes posible, pero no más de un mes desde la detección
MEDIO	Lo antes posible, pero no más de una semana desde la detección
ALTO	En las 48 horas siguientes a la detección
MUY ALTO	En las 12 horas siguientes a la detección
CRÍTICO	En la hora siguientes a la detección

Fuente: **cnn-cert.cni.es** [2]

Una vez determinado el tipo de incidente acontecido, es fundamental determinar las implicaciones jurídicas que puede tener para nuestra empresa. De esta manera se pueden poner en marcha medidas para mitigar los daños y las responsabilidades legales o judiciales que el incidente pueda tener en la empresa o en los servicios que ofrece.

Los incidentes de seguridad pueden ser constitutivos de delito. Estos son algunos de los incidentes de seguridad que son más relevantes desde el punto de vista legal por sus consecuencias:

- Casos de robo o fugas de información de la organización relacionada con mis clientes, proveedores, etc., que pueden incluir datos de carácter personal.

- Casos de suplantación de identidad a través de técnicas de ingeniería social como el phishing para obtener información sensible o inducir a engaño y conseguir algún beneficio económico.

- Uso de herramientas o aplicaciones sin las oportunas licencias (software pirata)

FASE 6: CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

Las estrategias de contención de incidentes varían dependiendo del tipo de incidente, así como del posible impacto sobre la empresa.

En función de la gravedad de los incidentes, puede que sea necesario aplicar medidas como deshabilitar servicios, apagar sistemas o desconectarlos de la red, para intentar evitar que el incidente se extienda por la empresa.

Estas decisiones pueden facilitarse y agilizarse si se han definido previamente estrategias y procedimientos para contener los distintos tipos de incidentes posibles.

Una vez contenido el incidente, hay que verificar si es necesario eliminar o limpiar componentes asociados al incidente, además de proceder a la recuperación de todos los sistemas afectados, para devolverlos a la situación de operación normal de la empresa.

En las actividades de recuperación se realiza la eliminación de los componentes asociados al incidente y otras actividades que se consideren adecuadas de cada a resolver el incidente o prevenir que vuelva a ocurrir en el futuro.

Actividades de resolución:

- Instalación de parches de seguridad
- Cambios en el cortafuego y equipamiento de seguridad

Cambios en las listas de acceso Actividades de recuperación:

- Restaurar información desde las copias de seguridad (backups)
- Reemplazar componentes afectados con otros limpios de infección
- Instalar actualizaciones de software
- Cambiar contraseñas
- Reforzar la seguridad actualizando reglas de cortafuegos.

FASE 7: ACCIONES POSTERIORES AL CIERRE

El cierre de un incidente de seguridad y el fin de su gestión debe incluir un conjunto de evidencias que acrediten las acciones que se han llevado a cabo, los procesos que se han realizado y todas las personas que han estado involucradas o han sido consultadas para su gestión.

Es recomendable disponer de un **registro común** para todos los incidentes, donde se describan los datos mencionados anteriormente, incluyendo el origen y la persona que detecta el incidente, así como los servicios y sistemas infectados, fechas/horas más relevantes, responsables de la gestión y acciones tomadas.

Periódicamente se deben analizar las actividades a realizar, estudiando posibles mejoras o cambios ante futuros incidentes.

Además, es recomendable **recoger y analizar métricas** sobre los tipos y frecuencia de incidentes, impactos (financieros, obligaciones legales, imagen frente a terceros, operativos), métodos de resolución, coste de la resolución de incidentes y acciones correctivas o preventivas.

De esta forma, si es necesario, se pueden detectar mejoras en los procedimientos de gestión, escalamiento, etc. y podemos detectar posibles patrones que te ayuden a identificar dónde está el foco de riesgo de tu organización.

CONSEJOS BÁSICOS:

- Mantener un registro de incidentes sufridos en tu organización
- Hacer un seguimiento de las acciones realizadas y las personas que hayan intervenido en la gestión del incidente.
- Mantener un registro de los documentos que sirvan como evidencia de las acciones realizadas para solucionar o cerrar el incidente de seguridad.
- Mantener esta información como inventario de incidentes de seguridad sufridos por mi organización para intentar mejorar la gestión sobre mis activos implementando medidas que contribuyan a impedir que los incidentes de seguridad se repitan.