CEC
CONFEDERACIÓN
EMPRESAS
PROVINCIA DE CÁDIZ

GUÍA PARA PYMES Y AUTÓNOMOS SOBRE CÓMO PROCEDER ANTE UN CIBERATAQUE A SU NEGOCIO

Con la colaboración de:

Diputación de Cádiz
COORDINACIÓN
Y DESARROLLO ESTRATÉGICO,
PRODUCTIVO Y SOCIAL

INDICE

0. CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

La **ciberseguridad** se podría definir como la parte de informática que **protege** a los sistemas, redes y programas informáticos de los **ataques digitales**. Estos ciberataques normalmente están diseñados para acceder, cambiar o destruir información sensible, solicitar dinero a cambio o interrumpir los procesos normales de una empresa.

Implementar medidas efectivas de ciberseguridad es realmente un reto a dia de hoy, ya que hay más dispositivos que personas y los atacantes cada vez son más creativos.

En ciberseguridad no existe un manual, hardware o software que nos proteja al 100% de los ataques. Solo un conocimiento de nuestros sistemas y una práctica continua pueden mejorar nuestra capacidad de respuesta ante tales ataques.

Por tanto para ser un **experto** solo hacen falta dos cualidades: **experiencia** y **sentido común**.

Un entorno seguro tiene múltiples capas de protección distribuidas por ordenadores, redes, programas o datos que queramos mantener a salvo. En una empresa, las personas, los procesos y la tecnología se deben complementar entre ellos para crear una defensa efectiva contra los ciberataques. Un sistema unificado de gestión de amenazas puede automatizar las integraciones entre todos estos participantes y acelerar las operaciones clave de la seguridad, que son: detección, análisis y solución.

Personas

Los usuarios deben comprender y cumplir con los principios básicos de seguridad, como usar contraseñas seguras, tener cuidado con los adjuntos de los correos electrónicos y hacer copias de seguridad.

Procesos

Las empresas deben tener un protocolo en caso de que tengan que enfrentarse a un ciberataque. Este protocolo debe servir de guía y explicar cómo se pueden identificar los ataques, proteger los sistemas, detectar y responder a amenazas y recuperarse de ataques con éxito.

Tecnología

La tecnología es esencial para proveer a las empresas y usuarios las herramientas informáticas necesarias para protegerse de los ciberataques. Se deben proteger tres activos principales: los dispositivos como ordenadores, dispositivos inteligentes, enrutadores, redes y la nube.

Las tecnologías mas usadas para protegerlos incluyen *cortafuegos, filtros DNS, protección antimalware, protección antivirus y soluciones de seguridad para correo electrónico*.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

En el mundo conectado de hoy en día, cualquiera se puede beneficiar de programas avanzados de ciberseguridad.

A nivel de usuario, un ciberataque puede provocar desde suplantación o robo de identidad, extorsión, o perdida de datos personales como pueden ser fotos familiares.

Todo el mundo confía en las **infraestructuras críticas** como *plantas de energía, hospitales y entidades financieras*. Proteger estas y otras organizaciones es esencial para mantener el correcto funcionamiento de nuestra sociedad.

Los avances tecnológicos están transformando la forma de hacer negocios. Casi sin darnos cuenta dependemos de Internet, la wifi, los móviles, las tabletas y hasta de la computación en la nube. El e-commerce, la administración electrónica, los blogs, las redes sociales y las herramientas de colaboración han llegado para quedarse.

Las empresas **interaccionan** con clientes, con proveedores y con la administración a través de **correo electrónico e Internet**. Muchas empresas también se relacionan a través de redes sociales, comparten documentos en la nube, disponen de *página web* o venden desde su *tienda online*. La generación y el intercambio de documentos en formato digital son imprescindibles.

La información ya sea en el disco del equipo, en USB, en dispositivos externos, en servidores (de correo, de almacenamiento,…) o en servicios en la nube es un activo para la empresa, es decir, tiene mucho valor y ha de protegerse.

En su día a día las empresas manejan información de clientes, de marketing, de recursos humanos, de productos, de facturación, contable, financiera, estratégica, etc. Entre ellas información crítica que si se altera, destruye, divulga o por alguna causa resulta inaccesible puede causar graves pérdidas a la empresa.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Tradicionalmente el soporte de la información era el papel, más adelante fueron los soportes magnéticos y hoy en día los **soportes electrónicos**. Los soportes y el software que maneja la información son también activos a proteger, como lo son las redes de comunicaciones por las que transita y las personas que las manejan.

El establecimiento de procedimientos, planes y políticas de almacenamiento, conservación, recuperación y borrado es esencial para garantizar la seguridad de un activo tan importante para la empresa como es la información. Estos van a hacer posible:

- el **acceso de los recursos de información** por los usuarios o programas autorizados
- evitar la **fuga de información**
- evitar el **deterioro de la información** almacenada o que deba ser conservada
- evitar el uso de **dispositivos no autorizados**
- proveer **métodos de recuperación de la información** y la actividad en caso de fallos técnicos, accidentes o desastres
- conocer cómo tratar las **incidencias, las fugas de información y los desastres** u otras contingencias

Las empresas manejan a diario **gran cantidad de información** y parte de esta información es más sensible, ya que es estratégica para el negocio, contiene datos

personales de clientes, proveedores o empleados, tiene valor como propiedad intelectual, etc. Por este motivo, es imprescindible una adecuada **gestión de la información** que se maneja, tanto para asegurar la actividad del negocio como para cumplir con los requisitos legales que apliquen.

En el contexto de las normativas de gestión se entiende por activo aquello que tiene algún valor para la organización y por tanto debe protegerse. Los activos de información son, además de los soportes de la misma, todo tipo de información que posea **valor para la empresa**, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Algunos ejemplos son: *ficheros, bases de datos, contratos y acuerdos, facturas, documentación, manuales, aplicaciones, software, estadísticas, tráfico del sitio web, interacción en redes sociales*, etc.

En este mismo contexto se define la seguridad de la información como la preservación de la *confidencialidad, la integridad y la disponibilidad* de los activos de información.

Por tanto a la hora de confirmar que el modo en que se trata la información es seguro hay que considerar tres dimensiones: el grado de confidencialidad, la integridad y el nivel de disponibilidad.

- **Confidencialidad**: por la cual la información no debe ponerse a disposición o revelarse a individuos, entidades o procesos no autorizados
- **Integridad**: por la cual la información debe poder conservar su exactitud y completitud

- **Disponibilidad**: por la cual la información debe estar accesible y utilizable por las entidades (usuarios, procesos…) autorizadas

En algunos contextos, se pueden tener en cuenta por su importancia otras propiedades de la seguridad de la información como son la **responsabilidad y el no repudio**. Por ejemplo en el caso de las transacciones (apuntes en una cuenta bancaria, entradas y salidas de almacén…) es importante considerar la responsabilidad o rendición de cuentas, es decir, la capacidad de justificar qué ha ocurrido, quién lo ha hecho y cuándo.

Si se trata de la transmisión de mensajes, por ejemplo por correo electrónico, es importante también el «no repudio», es decir poder certificar el origen, dónde se generó el mensaje, o el destino, a dónde ha llegado.

Dada la trascendencia de la información como base para la toma de decisiones estratégicas y su relevancia a la hora de establecer ventajas competitivas, es necesario contar con una eficiente gestión de la seguridad que preste especial atención a este recurso, a lo largo de todo su ciclo de vida desde que se crea hasta que se destruye de forma definitiva.

Estas son algunas de las situaciones que una correcta gestión de la seguridad de la información quiere evitar:

- Los **equipos y soportes** que utilizamos para almacenar la información (*móviles, portátiles, discos externos, pendrives*…) pueden ser extraviados o robados, con la consecuente pérdida o robo de información que contienen.
- Las **comunicaciones**, tanto por correo electrónico como por otros medios como redes sociales, pueden ser el origen de la difusión indebida de información confidencial, incluidas contraseñas y credenciales de acceso por desconocimiento, error o con intención.

- El **acceso por personas no autorizadas** a la información puede dar lugar a la consiguiente destrucción, manipulación o difusión no autorizadas. Por ejemplo los datos que registran transacciones, de ser accedidos por personas no autorizadas, pueden ser alterados o destruidos y resultar inservibles para justificar acciones realizadas.
- El **tratamiento de la información personal** está regulado por la ley y su no cumplimiento puede acarrear sanciones legales.
- **Empleados o usuarios sin mala intención**, por descuido o por caer en los engaños de la ingeniería social, pueden divulgar o destruir información sensible o de carácter personal, incluso credenciales de acceso que pueden llevar a intrusión en sistemas, daños de imagen o tener consecuencias legales.
- Los **soportes y equipos** que han **dejado de utilizarse** contienen información que debe borrarse o destruirse pues puede llegar a terceros y acarrear, si se divulgan, daños de imagen, consecuencias legales, etc.
- También puede ocasionar daños de imagen la **manipulación de contenidos** en nuestra web o de nuestra tienda online (precios, productos…) por personas no autorizadas que puedan acceder al gestor de contenidos. Esto puede ocurrir si llegan a sus manos las credenciales de acceso al mismo por ejemplo por descuido o por estar infectado con malware.
- La **información almacenada** en sistemas de almacenamiento compartido o en la nube puede ser **manipulada, destruida o divulgada** si no se toman las mismas medidas para garantizar su seguridad (control de acceso, cifrado…) que para el almacenamiento en local.
- En caso de **desastre natural**, si las copias de seguridad se almacenan en la misma oficina, pueden resultar destruidas como el resto de los equipos y hacer imposible su recuperación. Si no se hacen copias de seguridad tampoco podremos recuperar los sistemas en caso de incidentes o desastres.
- Los **soportes se deterioran con el tiempo**, las partes mecánicas pueden fallar pudiendo dejar inaccesible la información que contienen.

- El **software** que trata la información puede tener **vulnerabilidades** y, si no se actualiza con frecuencia, podría ser objeto de todo tipo de ataques, accesos no autorizados, infecciones con malware, etc.
- Los **dispositivos** personales, móviles y tabletas con sus apps, que se usan para acceder a recursos de la empresa, de no estar **correctamente configurados**, pueden dar lugar a fugas de información.

HACKERS

Un **hacker** es una persona que usa un ordenador, una red de ordenadores u otras habilidades para superar un problema técnico. El término hacker se puede usar para referirse a alguien con habilidades especiales, pero a menudo se refiere a una persona que usa sus habilidades para obtener acceso no autorizado a sistemas o redes para cometer delitos.

Un hacker puede, por ejemplo, robar información para hacer daño a otras personas a través de la suplantación de identidad, dañar o inutilizar sistemas y a menudo, secuestrar esos sistemas para pedir un rescate.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

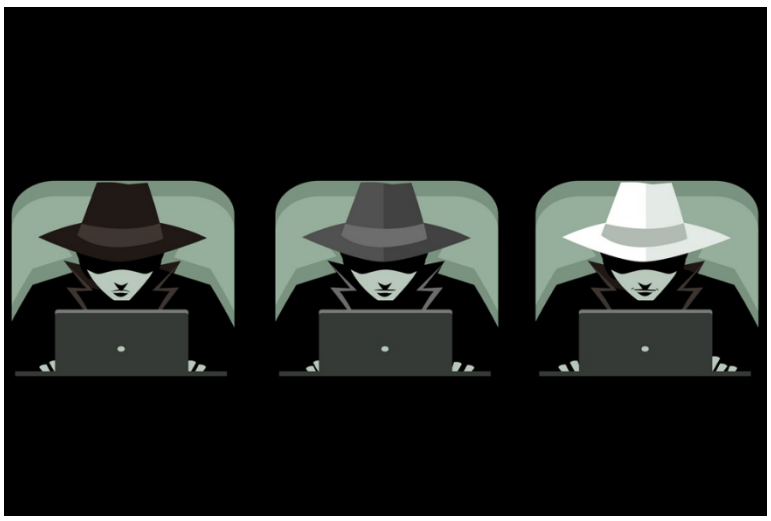
El término hacker siempre ha estado en discusión, algunas veces se usa como admiración a una persona que muestra unas habilidades sorprendentes, así como su creatividad para superar problemas técnicos. Sin embargo, muchas veces se usa comúnmente a una persona que usas estas habilidades para propósitos ilegales o fuera de cualquier ética.

Tipos de hackers

La comunidad de usuarios de seguridad ha usado informalmente referencias al color del sombrero como forma de identificar a los tipos de hackers. Se dividen normalmente en tres: sombrero blanco, sombrero negro y sombrero gris.

- Los hackers de **sombrero blanco**, también conocidos como hackers éticos, se esfuerzan en operar en bien del interés público en vez de crear confusión. Muchos de estos hackers trabajan haciendo tests de penetración (pentesting). Son contratados para intentar entrar en las redes de las empresas para encontrar e informar de las vulnerabilidades de seguridad. Las empresas de seguridad ayudan a sus clientes a reducir los problemas antes de que los ciberdelincuentes puedan aprovecharse de ellos.
- Los hackers de **sombrero negro** acceden intencionalmente a redes y sistemas sin autorización con intenciones delictivas. Sus objetivos pueden ser robar información, propagar malware, obtener beneficios pidiendo un rescate, destruir o dañar sistemas o incluso hacerse famosos. Este tipo de hackers son por definición criminales, ya que incumplen la ley al acceder a sistemas sin autorización, e incluso pueden llegar a hacer otro tipo de actividades ilegales, como suplantación de identidad y ataques distribuidos de denegación de servicio (DDoS).
- Los hackers de **sombrero gris** están en un punto intermedio entre los de sombrero blanco y los de sombrero negro. Mientras que sus motivos pueden

ser similares a los de sombrero blanco, los de sombrero gris se parecen mas a los de sombrero negro al acceder a sistemas sin autorización, pero al mismo tiempo, también se parecen mas a los de sombrero blanco al evitar hacer daños innecesarios a los sistemas que entran. Aunque no están típicamente o únicamente motivados por el factor económico, los de sombrero gris pueden ofrecer soluciones a vulnerabilidades que han descubierto ellos mismos a través de actividades no autorizadas. Vulnerabilidades que podrían usar en su propio beneficio.



Toda clase de hackers participan en foros para intercambiar información acerca de técnicas de *hackeo*. Hay numerosos foros y congresos donde los hackers de sombrero blanco pueden discutir y preguntar acerca de este tema. Otros foros ofrecen guías técnicas o manuales con instrucciones paso-a-paso.

En la *web profunda* podemos encontrar foros destinados a hackers de sombrero negro. Éstos a menudo ofrecen un espacio para anunciar los servicios ilegales de un hacker de este tipo.

Los ciberdelincuentes, que a veces carecen de habilidades técnicas suficientes, a menudo usan scripts u otros programas específicamente diseñados para entrar en

redes corporativas. Este software puede manipular las conexiones de datos para obtener información privilegiada de los sistemas atacados.

Estos scripts se encuentran publicados a disposición de cualquiera en internet, normalmente los usan los que están comenzando en el mundo del hacking. Este tipo de hackers se llaman a menudo *script kiddies o skiddies*, haciendo referencia a su necesidad de usar scripts maliciosos en vez de crear los suyos propios. Los avanzados lo que hacen es estudiar estos scripts y modificarlos para desarrollar nuevas funcionalidades.

Hacker vs. Cracker

El término hacker se usó por primera vez en los años 60 para describir a un programador o a una persona que gracias a sus habilidades en informáticas, podía aumentar la eficiencia del código fuente de un programa que eliminaba o "hackeaba" las instrucciones innecesarias de ese código. Ha evolucionado a lo largo de los años para referirse a una persona con conocimientos avanzados de ordenadores, redes, programación o sistemas.

Para muchos en el mundo de la tecnología, el término hacker se aplica mejor a aquellos que usan sus habilidades sin intención de provocar ningún daño. Pero después, se aplicó a personas que usan estas destrezas de forma malintencionada.

Para contrarrestar la tendencia de etiquetar a estas personas tecnológicamente avanzadas como delincuentes, se propuso el término *cracker* para los ciberdelincuentes, con la intención de suavizar el término hacker y distinguirlos de los verdaderamente peligrosos.

Dentro de la arquitectura *hacker-cracker*, los *hackers* son los que buscan e identifican fallos en los sistemas de seguridad y trabajan para mejorarlos. Entre ellos se encuentran los expertos en seguridad, cuya tarea no es otra que localizar e identificar fallos en sistemas y arreglar estas vulnerabilidades.

Por otro lado están los *crackers*, que lo que intentan es penetrar en ordenadores y redes para aprovecharse de las vulnerabilidades en su propio beneficio.

Mientras que los expertos en tecnología han motivado el uso del término cracker durante años, para diferenciar a los distintos tipos de hacker por el color del sombrero: blanco, negro o gris. En general el término cracker apenas se usa.

Hackers famosos

Mientras que muchos expertos en tecnología se han considerado como si fueran hackers, como Donald Knuth, Ken Thompson, Vinton Cerf, Steve Jobs y Bill Gates, los hackers de sombrero negro son más propensos a ganar notoriedad como hackers de la manera tradicional. Aunque a Bill Gates lo atraparon entrando en una red corporativa cuando era un adolescente, antes de fundar Microsoft.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Algunos hackers de sombrero negro famosos son:

- **Anonymous**. Son un grupo de hackers a nivel mundial que se reúnen en foros y redes sociales en internet. Se centran principalmente en la desobediencia civil, en provocar intranquilidad a través de ataques de denegación de servicio, publicando información personal de sus víctimas en internet o suplantando y difamando sitios webs.
- **Jonathan James** se convirtió en famoso al hackear varios sitios webs, entre los que se encuentra el Departamento de Defensa de los Estados Unidos o la NASA, así como de robar código cuando era adolescente. En el año 2000, al cumplir los 16 años, fue condenado a prisión por hacker. Se suicidó en el año 2008 a la edad de 25 años.
- **Adrian Lamo** consiguió entrar en sistemas de muchas empresas, incluyendo el New York Times, Microsoft y Yahoo al aprovecharse de fallos de seguridad. Fue detenido en 2003, condenado en 2004 y sentenciado a seis meses de arresto domiciliario en casa de sus padres. Estuvo 2 años en libertad condicional y tuvo que pagar una multa de 65.000$.

- **Kevin Mitnick** fue condenado por multiples delitos informáticos después de estar más de 2 años esquivando a las autoridades. Despúes de ser unos de los mas buscados por el FBI al entrar sin autorización en mas de 40 redes de las empresas mas importantes del país, fue arrestado en 1993 y condenado a 5 años en una prisión federal. Una vez liberado, Mitnick creó una empresa de ciberseguridad para ayudar a las organizaciones a mantener sus redes seguras.

Glosario

CIBERACOSO

Este tipo de delitos es materia de estudio obligada en la Informática Forense no solo por la dificultad muchas veces de descubrir al acosador, sino porque detrás de muchos perfiles de este tipo se esconde un criminal o futuro criminal.

La persona o personas que realizan el Ciberacoso utilizan los medios tecnológicos para perseguir a una persona, pueden acosar a través de llamadas, sms, mensajes de Whatsapp, publicaciones anónimas en internet nombrando a la persona acosada y multitud de técnicas empleadas bajo un mal uso de la tecnología.

En EEUU se conoce también como Stalking que viene a significar cazar algo de alguien, estar al acecho o seguir los pasos a alguien.

ADWARE

Componente de un programa que instalamos, en el cual puede ir escondido o no, y que nos muestra anuncios publicitarios de una forma más o menos molesta y que en ocasiones puede también recabar datos acerca de nuestras actividades.

ANONIMIZADOR

Servicio proxy que permite navegar sin que se sepa la IP del cliente

CIBERBULO

Es un mensaje de correo electrónico que alerta sobre un virus inexistente. También se conocen como hoaxes o falsas alarmas, y no son más que bromas y/o intentos de causar pánico entre usuarios inexpertos.

CIBERBULLYING

Acción mediante la cual un menor atormenta, hostiga, amenaza, humilla o molesta a otro/a menor mediante el uso de Internet, teléfonos móviles, videoconsolas online u otras a través de las nuevas tecnologías. No reviste carácter sexual.

CIBERDELITO

Delitos cometidos a través de cualquier medio tecnológico.

CRAWLER

Programa que recorre Internet a la caza de direcciones de correo electrónico, normalmente para luego convertirlas en objetivo del spam.

ENGAÑO O CEBO

Señuelo para atraer, tentar, seducir, persuadir con mañas, hacer caer en una trampa… Se usa en el entorno de los pederastas en Internet para hablar de su forma de convencer a los niños de que se encuentren con ellos fuera de la Red.

FISGÓN DE PAQUETES O SNIFFER

Programa que espía las comunicaciones de Internet, por ejemplo, para encontrar números de tarjetas de crédito. Las agencias de seguridad también los utilizan con fines de espionaje, contraterrorismo, etc.

FLAME O FLAMING

Mensaje incendiario enviado a un foro, lista de correo o tablón de mensajes para provocar y obtener una respuesta indignada de cualquiera de los participantes o de alguno/a en particular. En general, mensaje insultante u ofensivo. Muy empleado por los TROLLS de internet.

GROOMING

Acciones deliberadas por parte de un/a adulto/a de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos.

GUERRAS DE AVISOS

Batallas entre usuarios de Internet a base de provocaciones que dan lugar a advertencias de los proveedores de acceso por violar las condiciones de utilización, normalmente utilizado por gente que busca reventar un espacio ya sea un foro, como un diario de noticias, etc… hay de muchos tipos de perfiles detrás de cada persona desde los simples TROLLS, hasta grupos organizados para sabotear a la competencia previo pago del servicio, como por ejemplo Debunkers, que cobran por desinformar o cambiar opiniones políticas o de otro ámbito a través de internet.

GUSANO

Es un programa que se trasmite a sí mismo activamente por una red (se dice que es "autorreplicante"). No requiere ninguna intervención del usuario para extenderse ni "esconderse" en ningún programa. Tienen en común con los virus que su principal función es reproducirse, pero los gusanos en lugar de meterse dentro de otros archivos, crean copias de sí mismos. Pueden realizar acciones adicionales malignas.

MALWARE

Cualquier tipo de software dañino o con malas intenciones.

PHISING

Prácticas utilizadas para obtener información confidencial (como números de cuentas, de tarjetas de crédito, contraseñas, etc.).

PIRATEO

Aunque no es del todo correcto utilizar esta palabra pues los piratas son los que van en embarcaciones marítimas para saquear los bienes ajenos, se viene empleando para denominar a las entradas ilegales en un sistema informático o ruptura de las protecciones anticopia de un programa. El término pirateo o piratear, también se aplica a quien produce copias ilegales de programas, discos de música, DVDs, o cualquier otro producto. En inglés la diferencia entre los términos consiste en que hacking, originalmente, es simplemente una habilidad que no implica nada ilegal (hacker), mientras que cracking implica ruptura de protecciones o entradas ilegales en sistemas (cracker).

1. BUENAS PRACTICAS EN REDES SOCIALES.

Las redes sociales cada vez son más importantes en la estrategia corporativa en una empresa: son un gran canal de comunicación para las empresas y una herramienta de marketing muy potente.

Es por esto que las compañías hacen uso de ellas con diferentes objetivos. Por ejemplo, un 90% lo hace para mejorar la imagen de marca; un 77% para manejar la reputación; un 60% para proporcionar atención al cliente y un 60% para incrementar las ventas.

Por el contrario, solo un 15% recurre a ellas como herramienta para mejorar la comunicación interna, según datos del Barómetro de Hootsuite 2018. Actualmente estamos más conectados e informados que nunca. Según el estudio realizado por Hootsuite y We Are Social, el uso de las redes sociales ha aumentado un 13% en el último año, alcanzando los 3.196 millones de usuarios, por lo que se convierten en un buen medio de comunicación para contactar con el público objetivo.

Sin embargo, debido a la gran cantidad de información que se comparte diariamente, estamos también expuestos a muchas amenazas externas que debemos combatir.

Algunos de los riesgos más comunes relacionados con el ámbito de la seguridad son, por ejemplo, dejar los perfiles sociales desatendidos, utilizar aplicaciones de terceros que se integran en las redes sociales, el phishing o estafas de suplantación de identidad, o errores que pueden cometer los empleados de una empresa, entre otros.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Por todo esto, podemos aplicar estas 8 claves para disminuir el riesgo al que nos exponemos cuando hacemos uso de las redes sociales:

1. **Crear una política sobre el uso de las redes sociales**: es conveniente que las empresas que utilizan diariamente sus redes sociales establezcan una política para que todos los empleados conozcan cómo usarlas de la forma más responsable posible.
2. **Enseñar a tus empleados las mejores prácticas de identidad**: así aprenderán qué hacer en cada momento y será una gran oportunidad para que sepan cuáles son las últimas amenazas en las redes. Se sentirán más seguros al utilizarlas, ya sea de forma personal o comercial.
3. **Limitar el acceso a las redes sociales**: la mayor parte de las amenazas externas llegan a través de incidentes provocados por los propios empleados, por lo que es aconsejable limitar la cantidad de usuarios que pueden publicar contenido en las cuentas y elegir quién estará a cargo de cada publicación.
4. **Desarrollar un sistema de aprobación para las publicaciones**: han sido muchos los perfiles profesionales que han publicado tweets erróneos que no han sido detectados a tiempo. Por ello, conviene crear un borrador de las publicaciones de tal modo que puedan revisarse antes de ser publicadas y evitar así errores graves.

5. **Seleccionar a una persona responsable de los perfiles sociales**: si hay un responsable que revise todas las publicaciones se reducirá el riesgo. Esta persona deberá conocer a la perfección la política de redes sociales, controlar la presencia de la marca en las mismas y decidir quién puede publicar contenido.
6. **Monitorizar tus cuentas y hacer una escucha social**: es importante no desatender los perfiles sociales ya que se trata de cuentas muy vulnerables. Es importante contar con un responsable que verifique todos los contenidos y esté atento a cualquier sospecha de que la cuenta haya podido ser robada.
7. **Invertir en soluciones de seguridad**: vigilar 24 horas un canal social es muy difícil, por lo que existen softwares que pueden hacerlo por nosotros. Estos programas pueden ayudarte a prevenir cualquier amenaza a tu cuenta.
8. **Hacer inspecciones regulares**: las amenazas en redes sociales evolucionan constantemente por lo que no solo conviene estar al tanto de las mismas, sino también revisar periódicamente la política de privacidad de estas redes, así como la configuración de privacidad de los perfiles. También se deben revisar los permisos de publicación para saber quién tiene acceso a ellos.

Existen varios aspectos a tener en cuenta para mantener e incluso recuperar la reputación online.

Vamos a ver cinco claves para mantener por el buen camino la identidad digital de una empresa:

1. **Cuida todo lo que publiques.** Todos los soportes pueden originar una crisis de identidad digital. Un error muy común es prestar excesiva atención a la página web, y descuidar otros soportes como las Redes Sociales o los blogs. Ten en cuenta detalles como la ortografía (las faltas desprestigian a tu marca), la

orientación de esos contenidos y la gestión de los comentarios negativos, intenta neutralizarlos con respuestas cordiales.

2. **Controla lo que se dice de tu empresa.** Mantente al día sobre lo que se dice de tu negocio en la red para ver si es positivo o negativo y, en el último caso, tratar de solucionarlo. En este artículo te explicamos los principales canales alternativos donde se habla de tu marca para que puedas monitorizarlos y cuidar tu reputación online. En el mismo descubrirás por qué es esencial revisar lo que se dice de tu empresa en:

    - Foros de opinión
    - Agregadores de noticias
    - Medios de comunicación
    - Influencers
    - Marketplaces
    - Comparadores de productos
    - Tus propios perfiles sociales
    - La información que tu entono offline te proporciona

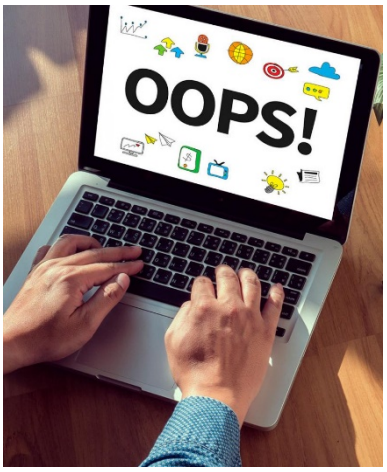
3. **Vigila a tu competencia.** Es vital controlar aquello que se dice de tu competencia directa, puede darte pistas sobre si lo estás haciendo bien o mal e incluso conocer algunos errores que debes evitar. Los aciertos y errores de tus principales competidores siempre son una fuente de información e inspiración ideal.

4. **Monitoriza las Redes Sociales.** Son el principal foco generador de crisis de identidad digital. Trata de responder con asiduidad a los comentarios, y haz especial hincapié en los negativos a través de respuestas amables y cordiales. Lograrás una reputación positiva.

5. **Cuidado con los perfiles personales de los directivos e inversores.** Pese a que un perfil personal a priori no debería afectar a nivel de empresa, la realidad es que si tienes un negocio con inversores o socios, toda la información que circula sobre ti en Internet también es importante. Cuídala al máximo. Para ello, trata de monitorizar de manera periódica aquello que dicen y se dice de tus directivos, inversores y socios más representativos.

Como hemos podido comprobar, gestionar la reputación online es muy importante para mejorar tu presencia en Internet y crecer con tu estrategia digital. La clave está en elaborar un plan de acción para conseguir avanzar en la transformación digital y aumentar positivamente la reputación online de tu marca o empresa.

Cuando un usuario accede a Internet, no tiene por qué tener la más mínima experiencia en la red y por supuesto, tampoco ha recibido ninguna formación para ello. Por lo tanto, el usuario medio no tiene ningún sentido común digital pero necesariamente accede a Internet para uso profesional y personal. Se toman decisiones porque están de moda, pero sin criterio y sin conocimiento del peligro o problemas que puedan acarrear dichas decisiones.



Por otro lado, el mundo Internet está dominado por delincuentes muy preparados y organizados en mafias con el objetivo de robarnos, chantajearnos y estafarnos. Con lo cual, la situación está muy desequilibrada, en un lado el ciberdelincuente y en el otro lado el usuario sin experiencia, sin conocimiento y con una inocencia digital que jamás tendría en el mundo real.

En relación a la seguridad de la información, todas las medidas técnicas que apliquemos y productos que instalemos no nos sirven para casi nada si no concienciamos y formamos a los usuarios, ya que muchas de las fugas de información y vulnerabilidades van asociadas a la mala actuación, generalmente por desconocimiento, de los propios usuarios.

La seguridad de la información es un área poco conocida incluso por técnicos informáticos, pero es evidente que en este momento es clave ya que tenemos Internet presente en todas nuestras actividades profesionales y personales.

Antes de comenzar, deberíamos hacernos algunas preguntas en cuanto a la seguridad de la información de nuestra empresa:

- ¿Trabajan todos los ordenadores SIN permiso de administrador?
- ¿Están todos los ordenadores securizados?
- ¿Tenemos instalado un UTM (cortafuegos hardware) como seguridad perimetral?
- ¿Hemos realizado una Revisión de Seguridad de todos los ordenadores en el último año?

Si las respuestas a todas estas preguntas no han sido afirmativas, tendremos que realizar una actualización urgente de las medidas de seguridad para minimizar su nivel de riesgo.

Mundo digital vs mundo real

La primera regla cuando navegamos por Internet es mantener, al menos, el mismo sentido común que en el mundo real y no bloquearnos por la inocencia digital.

Algunos ejemplos de inocencia digital son los siguientes:

- Si dando un paseo, alguien se acerca a nosotros y nos pide el carnet de identidad o el número de su cuenta bancaria, ¿Se lo da?. Evidentemente no se lo da, y entonces, ¿por qué lo da en Internet cuando se lo piden?
- Si en el mundo real todo tiene un precio, ¿por qué cree que en Internet hay sitios web que le permiten descargarse programas, juegos o películas gratis?. Muy sencillo, porque no es gratis, incluido en lo que se descarga van virus que permitirá a los delincuentes robarle, chantajearle, estafarle o poder controlar su ordenador para cometer delitos, y así pagará a precio de oro lo que se ha descargado. Las descargas no cuestan dinero pero no son gratis.
- Si cuando sale de casa cierra la puerta, ¿por qué cuando navega por Internet deja la puerta abierta, que es lo mismo que utilizar un usuario con permiso de administrador?. La primera regla de seguridad es usar un ordenador siempre con un usuario sin permiso de administrador y solo elevar a permiso de administrador cuando tenga que instalar un nuevo programa o configurar algo del sistema operativo. Si trabaja con permiso de administrador, cualquier virus puede instalarse y tomar el control del ordenador. El permiso de administrador es la llave de su ordenador y es la única forma de que controle qué se está instalando en el mismo. Si es incómodo tener que abrir la llave de su ordenador cada vez que tiene que instalar un programa, pruebe por comodidad a no cerrar la puerta de su casa durante una temporada.
- Si recibe un correo diciendo que le ha tocado una herencia de mil millones de euros de un familiar en África y lleva adjunto un fichero. ¿Por qué abre el fichero adjunto si no tiene ningún familiar en África?. Si le hubiera tocado dicha herencia ¿a quién se le ocurre que se lo van a comunicar por un correo electrónico?. Las estafas son muy habituales en Internet, y debemos desconfiar de los correos que recibimos de remitentes desconocidos e incluso aunque sean conocidos si el contenido del correo le resulta extraño, bórrelo, ya que puede haberse cometido una suplantación de identidad y que por lo tanto, no haya sido enviado por su

conocido. Y jamás debe abrir un fichero adjunto sospechoso. La curiosidad en Internet es muy peligrosa.

- A pesar del peligro de utilizar programas descargados de Internet los necesito usar, ¿qué puedo hacer?. Muy sencillo, el ordenador que va a utilizar dichos programas no debe estar en la misma red local que el resto de los ordenadores de la empresa y no debe contener archivos con datos de la empresa ni personales; y, sobre todo, jamás acceder en dicho ordenador a bancos ni sitios web en los que teclees contraseñas.
- Ya hemos implantado en nuestra empresa todas las medidas de seguridad necesarias, pero en casa cuando navego por Internet, ¿me tengo que preocupar?. Por supuesto, el peligro es el mismo y debemos utilizar Internet siempre con sentido común digital. Lo más importante es no utilizar el mismo equipo para navegar por divertimiento y descarga de juegos y películas, del que voy a usar para acceso a bancos o que contenga datos personales de la familia. Si el ordenador que uso para divertimiento y ocio, contiene fotos familiares y datos personales no me debe extrañar que en cualquier momento salgan publicadas en Internet.
- Se puede dar el caso de algunas empresas que pierden últimamente muchas operaciones en donde la competencia ofrecen los mismos productos a un precio algo inferior, ¿es un problema de fuga de datos?. En algunos casos son los propios clientes los que entregan a la competencia las ofertas para convertir cada operación en una subasta, pero también es cierto que desgraciadamente se están dando muchos casos, más de los que nos podemos imaginar, de fuga de información y de ataque remoto a través de troyanos contratados que permiten acceder fácilmente al ordenador de alguien en particular. Una vez que accede al ordenador atacado se tiene acceso a toda la información, correos electrónicos y por supuesto, a las ofertas enviadas.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

REFLEXIÓN

En unos años el uso de Internet ha cambiado por completo. Antes, el uso principal era de búsqueda de información y ahora publicamos nuestra intimidad, ¿supone este cambio una pérdida voluntaria de nuestra privacidad?. Exactamente. Nadie se podía imaginar que renunciaríamos tan fácilmente a nuestra privacidad, que dejaríamos a la vista de cualquiera los datos de dónde estamos en cada momento, qué pensamos, quiénes son nuestros amigos, qué nos gusta, a dónde hemos ido y con quién, qué ignoramos e incluso qué consumimos.

La realidad ha superado a la ficción. Además toda nuestra información íntima se almacena en servidores de terceros y por el uso de programas y servicios "gratuitos" hemos voluntariamente perdido nuestra privacidad. En este punto es muy importante una reflexión personal de cómo una falta de sentido común digital ha llevado a una pérdida voluntaria de la privacidad de imposible marcha atrás.

BYOD

La nueva moda en el tema de los móviles es BYOD (Bring Your Own Device), en castellano "trae tu propio dispositivo", ¿qué ventajas proporciona?. Esta moda parte de la premisa que los empleados estarían deseosos de aportar sus dispositivos personales para el uso de la empresa y la ventaja sería una mejora de la productividad ya que el empleado conoce mejor el uso de su dispositivo. Esta moda tiene muchos inconvenientes siendo el más importante el de la seguridad.

¿Cómo se garantiza la seguridad de los datos si el empleado instala en su móvil programas contrarios a la seguridad de la empresa?.

El argumento de la productividad es débil ya que cualquier empleado aprende rápidamente el uso de cualquier dispositivo que la empresa le facilite para su trabajo. Por otro lado, el coste del dispositivo por parte de la empresa es insignificante frente a los costes de mejora de la seguridad al usar cada empleado un dispositivo diferente.

Un tema importante a tener en cuenta, olvidando la inocencia digital, es que el uso del móvil personal se puede legalmente prohibir en horario laboral, simplemente indicándolo en el documento de uso de los medios tecnológicos.

Cualquier llamada urgente que tenga que recibir un empleado en horario laboral se realizaría llamando a los teléfonos de la empresa. Las llamadas urgentes son las únicas que tiene que recibir y realizar un empleado durante la jornada laboral.

No tiene ningún sentido común digital que un empleado utilice su móvil personal recibiendo durante el día cientos de whatsapps que le están interrumpiendo en vez de estar concentrado en el desarrollo de su trabajo. Este es un ejemplo más de inocencia digital en el que no se aplica sentido común digital y el empleado en horario laboral usa su móvil como si no estuviera en el trabajo. ¿Cuánto le cuesta a una empresa esta inocencia digital?

Mitos o falsas creencias de la seguridad

La mayoría de los usuarios no tienen conciencia real de los peligros de Internet y todavía persisten mitos o leyendas urbanas de la seguridad que pueden llegar a poner en peligro los sistemas informáticos, siendo los principales mitos los siguientes:

- **En Internet todo es gratis**. Al contrario, en Internet nada es gratis, salvo determinadas páginas institucionales y de la Administración y determinados fabricantes en todas las demás páginas de descargas el fichero descargado incluye troyanos, cuyos delitos pagan con creces la descarga realizada. Nos creemos que es gratis porque en el momento de la descarga no pagamos por ello, pero nos cuesta por los datos personales que nos roban los troyanos y el uso que hacen de ellos, por el uso remoto de nuestro ordenador por las redes mafiosas y por la publicidad que nos bombardea. Todo software descargado de Internet ha sido manipulado para crear agujeros de seguridad e instalar virus, troyanos o malware, y por lo tanto, están comprometiendo seriamente la seguridad de la información del ordenador.
- **Es una tontería comprar un programa si me lo puedo descargar de Internet gratis**. Lo más grave es que todo programa descargado de Internet ha sido manipulado e incluye virus y troyanos con el objetivo de robarnos datos o usar nuestro ordenador para cometer delitos. Una inocencia digital es pensar que alguien financia un sitio web con programas ilegales "gratis" para que cualquiera se lo pueda descargar. Lamentablemente estos sitios web son financiados por las mafias de delincuentes para la infección masiva de ordenadores. Por lo tanto, debemos ser conscientes que al descargar un programa lo pagamos con nuestros datos y delitos cometidos con nuestro ordenador. Por otro lado, incumplimos la Ley de Propiedad Intelectual, la Ley de Protección de Datos y el Código Penal. En el Código Penal la responsabilidad penal se extiende a la propia empresa del delito cometido por sus empleados por su falta de control ante el delito y por el beneficio o provecho productivo asociado al uso de programas sin licencia.
- **Tengo un antivirus instalado así que no puedo ser infectado. Esto es totalmente falso.** El antivirus en un sistema de seguridad es lo último que debe entrar en juego, ya que si debe intervenir es porque el virus ya ha entrado en el ordenador y se tiene que encomendar que sea detectado y

eliminado. Pero puede ocurrir que el antivirus actualice la detección de ese virus después de que ya se haya infectado. Por lo tanto, de lo que se trata es de no jugársela e implementar una serie de soluciones que impidan que el virus pueda llegar al ordenador. Un antivirus es totalmente necesario. Diariamente se generan 150.000 nuevas amenazas y los antivirus se actualizan, entre otras, con la información obtenida de ordenadores infectados con nuevos virus. Esta falsa creencia conduce a una falsa sensación de seguridad de verse protegido y la seguridad no son solo controles técnicos siendo fundamental aplicar un sentido común digital que evite situaciones de alto riesgo.

- **Tengo un Mac, no puedo ser infectado**. Lamentablemente, los productos Apple son un objetivo de los piratas informáticos y tienen virus al igual que cualquier sistema operativo. El riesgo adicional con Apple es que no son ágiles lanzando nuevas actualizaciones y pueden estar los equipos en situación vulnerable durante muchos meses. Android es el sistema operativo con mayor número de virus, y la situación va camino de convertirse en epidemia, cada dos minutos se libera un nuevo malware para Android.
- **No navego por webs peligrosas, así que no hay riesgo**. Una leyenda urbana considera a las páginas pornográficas y de juegos como las más peligrosas y a las web legítimas sin ningún peligro, lo cual es totalmente falso. La industria del porno y de los juegos generan mucho dinero y sus propietarios dedican un buen presupuesto a garantizar que no les infecten sus páginas. En cambio, la mayoría de las web legítimas no se han revisado desde que las programaron y los ciberdelincuentes aprovechan sus vulnerabilidades para infectarlas a un ritmo alarmante (una página web infectada cada tres segundos). El gravísimo problema de estas infecciones de páginas web es que cualquier ordenador se infecta de virus simplemente visitando dichas páginas. Con lo cual, nos encontramos que cualquier cliente, proveedor o curioso que visite una página web infectada infecta su

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

ordenador de virus con los consiguientes problemas de llamadas de quejas y disgustos. Una página web diseñada para dar a conocer una empresa con sus productos y servicios y ser generadora de negocio, se puede convertir en una fuente de infección de ordenadores y generadora de reclamaciones y problemas. Es muy importante recalcar que un ordenador se puede infectar con solo visitar una página legítima y el número de páginas legítimas que han sido infectadas por virus va creciendo exponencialmente.

- **No soy nadie importante, ¿quién querría mis datos?.** Cualquier ordenador puede ser víctima de un pirata informático y controlado remotamente por mafias de ciberdelincuentes para cometer delitos desde nuestro ordenador y con nuestra responsabilidad legal. El objetivo de los delincuentes no solo es robar datos de un ordenador, sino utilizarlo para cometer delitos.
- **El correo electrónico es la principal vía de entrada de virus.** Esta creencia ha quedado obsoleta. Actualmente, las principales vías de infección son las redes sociales, las páginas web previamente infectadas y la descarga de programas o archivos que incluyen virus. La inmensa mayoría de las infecciones de Android viene por la instalación consciente de aplicaciones "gratuitas" con troyanos. Cada semana los hackers crean 57.000 nuevas direcciones web que posicionan e indexan en los principales buscadores con la esperanza de que usuarios despistados pinchen por error en ellas y, al visitarlas, se infecten o bien introduzcan sus datos creyendo que corresponden a sitios lícitos. Hace unos años la infección por correo electrónico era la tónica general, en cambio desde el año pasado los hackers han optado por la técnica de crear falsas direcciones web con el atractivo de marcas conocidas y la infección de páginas legítimas, incluso gubernamentales, con código malicioso.
- **No se ve nada raro en mi equipo, así que no tiene virus.** Esta idea está muy extendida, aunque lo normal que puede ocurrir es que el usuario no sea consciente de que ya está infectado. Los virus se diseñan para que cumplan

con su objetivo de robar información o realizar ataques sin que el usuario sea consciente de ello y no lo detecte.

Situación actual de inseguridad en Internet

Algunos datos de la situación actual de inseguridad de Internet son los siguientes:

- Más del 80% de los ordenadores del mundo están infectados y controlados remotamente por mafias de ciberdelincuentes para cometer delitos desde nuestro ordenador y con nuestra responsabilidad legal.
- Muchísimas páginas web legítimas han sido infectadas y un ordenador se infecta simplemente visitando dichas páginas.
- Los ciberdelincuentes han creado infinidad de páginas atractivas de descargas con el objetivo de infectar los ordenadores.

En la prensa nos invaden titulares catastrofistas como: "La OTAN refuerza su ciberdefensa. La principal amenaza es que un software maligno puede ser capaz de paralizar instalaciones como las centrales nucleares" u "Obama reconoce ciberataques respaldados por gobiernos".

Todos estos datos y titulares de prensa sobre la inseguridad de Internet nos pueden sonar a algo lejano, aunque la realidad es que las estafas, acosos y chantajes se están realizando en nuestro entorno:

- Andalucía registra medio centenar de delitos cibernéticos a la semana. Estafas, acoso y pornografía infantil son los más frecuentes.
- Detienen en Zaragoza a uno que grababa a cientos de sus vecinos pirateando sus ordenadores.
- Los ciberdelitos le cuestan a España 19.000 millones de euros al año.

- El 13% de los adolescentes españoles han sido víctimas de ciberbulling (acoso entre menores en Internet) alguna vez y el 9,4% confiesa haber ciberacosado a algún compañero, lo cual equivale a decenas de miles de jóvenes y familias sufriendo esta situación.
- Más de 1,5 millones de españoles han sido víctimas de estafas en Internet en el último año, aunque es presumible que la cifra sea aún mayor ya que muchos casos no son denunciados.

Según la Policía Nacional, las cinco ciberestafas más frecuentes de este año son:

- **Páginas falsas de compraventa** de artículos baratos y que piden el dinero por adelantado.
- **Engaño de cursos de formación** falsos y petición de dinero para la gestión o compra de libros.
- **Virus de la policía** que bloqueaba el ordenador hasta que se abonase 100 euros por una supuesta multa.
- Delitos de **phishing** o robo de identidad en supuestas ofertas de trabajo.
- **Robos de cuentas** en redes sociales y delitos asociados a la recepción de SMS de pago.

En el mundo de la empresa dos graves situaciones que se están produciendo frecuentemente son: la **fuga de datos y los ataques dirigidos** a empresas por ex-empleados, competencia o desequilibrados.

Cuando hablamos sobre ciberdelincuencia, la visión de la gran mayoría de usuarios gira en torno a complejos códigos maliciosos creados exprofeso para atacar una organización en concreto.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Pero en realidad, la ciberdelincuencia no opera generalmente de esta manera. El principal motivo es que ese tipo de ataques requieren una inversión de tiempo, recursos humanos y económicos muy elevados.

La mayoría de ciberataques se centran en atacar al mayor número de víctimas, con la menor inversión posible. Para conseguirlo, se utiliza una de las técnicas preferidas por los ciberdelincuentes: la ingeniería social.

¿Qué es la ingeniería social?

La ingeniería social basa su comportamiento en una premisa básica: es más fácil manejar a las personas que a las máquinas. Para llevar a cabo este tipo de ataque se utilizan técnicas de manipulación psicológica con el objetivo de conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente.

Los ataques de ingeniería social usan como canal principal para su propagación el correo electrónico gracias a su uso masivo tanto por empresas, como por particulares. Pero no es la única vía de la que hacen uso los ciberdelincuentes, ya que pueden utilizar otros canales de comunicación como llamadas telefónicas, aplicaciones de mensajería, redes sociales, etc.

Los ataques de ingeniería social se pueden dividir en dos tipos distintos dependiendo del número de interacciones que requieran por parte del ciberdelincuente.

- **Hunting**. Este tipo de ataques buscan afectar al mayor número de usuarios realizando, únicamente, una comunicación. Son comunes en campañas de phishing, como los realizados contra entidades energéticas o bancarias. Algunos ejemplos son:

- Si te llega un reembolso de Endesa, guarda precaución, es un phishing
- ¡Cuidado no piques! Detectada campaña de phishing que suplanta a Bankia
- Campaña de phishing suplantando a la entidad bancaria BBVA

También son utilizados en ataques cuyo objetivo es realizar una campaña de infección por malware, como las que se llevaron a cabo para realizar ataques de ransomware:

- Envío de falsos presupuestos en Excel como adjuntos maliciosos
- Detectada oleada de correos con facturas que infectarán tu equipo
- Nueva oleada de ransomware afectando a múltiples equipos

- **Farming**. En los ataques de farming los ciberdelincuentes realizan varias comunicaciones con las víctimas hasta conseguir su objetivo u obtener la mayor cantidad de información posible. Algunos ejemplos de este tipo de ataques son los que buscan infundir miedo en las víctimas por medio de supuestos videos privados o futuros ataques contra su empresa:
  - Campaña de correos extorsionan con supuestos vídeos privado
  - Oleada de correos electrónicos que amenazan con atacar tu empresa

  En otros casos, como sucede en el **fraude del CEO** o más recientemente el de RRHH, los ciberdelincuentes suplantan a un miembro de la empresa y utilizan diferentes técnicas de ingeniería social para conseguir su objetivo:
  - Fraude del CEO
  - Fraude de RRHH

¿Qué técnicas utilizan los ciberdelincuentes en los ataques de ingeniería social?

A pesar de ser múltiples y varias las técnicas utilizadas por los ciberdelincuentes para manipular a sus víctimas, suelen seguir una serie de principios básicos:

- **Respeto a la autoridad**. Por norma general, nosotros como trabajadores y ciudadanos en general, respetamos la autoridad de nuestros superiores, bien sea dentro de la organización o en la vida cotidiana. Este tipo de ataques se basa en ese respeto que tenemos a nuestros responsables y a autoridades como las Fuerzas y Cuerpos de Seguridad del Estado.
- **Voluntad de ayudar**. Sobre todo en los entornos laborales, los trabajadores, generalmente, cuentan con esta voluntad de ayudar a los compañeros en todo lo posible. Por este motivo, los ciberdelincuentes pueden hacerse pasar por un falso empleado de la empresa. Otra variante utilizada, es hacerse pasar por un técnico de informática para instalar herramientas de acceso remoto no autorizado.
- **Temor a perder un servicio**. Esta técnica es habitualmente utilizada en campañas de phishing. Bajo el pretexto de existir repetidos accesos no autorizados, cambio en las políticas o cualquier otro engaño, los ciberdelincuentes fuerzan a la víctima acceder a una web fraudulenta donde roban información confidencial.
- **Respeto social**. En algunos casos, los ciberdelincuentes basan su estrategia en el miedo que tienen los usuarios a no ser socialmente aceptados o a perder su reputación. Esto es habitual en los correos de sextorsión, donde los ciberdelincuentes amenazan con difundir un supuesto video privado que en realidad no existe.
- **Gratis**. Este tipo de engaño se basa en ofrecer un producto o servicio gratis a cambio de información privada. Este tipo de fraude suele llevarse a cabo por medio de páginas web emergentes que suelen aparecer cuando se navega por sitios poco legítimos. También es común en mensajes de redes sociales o aplicaciones de mensajería.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

¿Cómo protegerse contra los ataques de ingeniería social?

La mejor manera de protegerse contra los ataques de ingeniería social es formar y concienciar a los empleados. Un sistema con las medidas de seguridad y tecnologías más modernas no servirá de nada si por medio de un simple correo electrónico el ciberdelincuente consigue información confidencial muy valiosa para la empresa.

Para evitar ataques de ingeniería social no existe una fórmula mágica que permita su identificación, ya que estos pueden ser muy variados y utilizar diferentes técnicas.

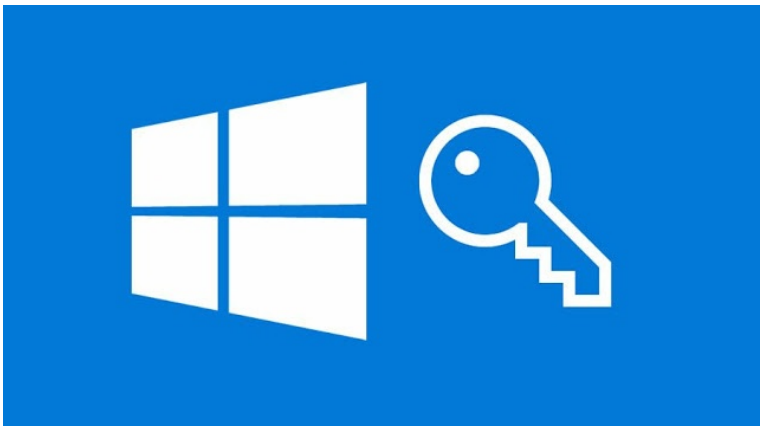
La ingeniería social es una de las técnicas más utilizadas por los ciberdelincuentes para conseguir sus objetivos delictivos. Para minimizar los riesgos de este tipo de fraude, la mejor vía es formar y concienciar a tus empleados.

PASSWORDS EN WINDOWS

A partir de Windows 8/10, tenemos cuentas locales y cuentas de Microsoft. Las cuentas de Microsoft están obligadas a usar una contraseña que no esté en blanco debido a que una cuenta de Microsoft nos da acceso a los servicios de Microsoft. Usar una contraseña en blanco significaría exponernos a muchos problemas. Sin embargo, las cuentas locales en Windows 8.1 pueden usar una contraseña en blanco.

Además de las contraseñas tradicionales, cualquier cuenta de usuario puede crear y usar un PIN de 4 dígitos o una contraseña de imagen. Microsoft introdujo estos

conceptos para acelerar el proceso de inicio de sesión desde el sistema operativo Windows 8.



Sin embargo, no reemplazan el uso de una contraseña tradicional y solo se pueden usar junto con una contraseña de cuenta de usuario tradicional.

Otro tipo de contraseña que encuentra en los sistemas operativos Windows es la contraseña del grupo en el hogar. En una red doméstica típica, los usuarios pueden usar el grupo en el hogar para compartir recursos fácilmente. Un dispositivo Windows puede unirse solo usando la contraseña del grupo en el hogar.

¿Qué debemos tener en cuenta al crear contraseñas, PIN y contraseñas con imágenes?

Al crear contraseñas, un PIN o una contraseña de imagen para la cuenta de usuario, deberíamos tener en cuenta las siguientes recomendaciones:

- **No usar contraseñas en blanco**, incluso en los equipos de escritorio del hogar. Nunca se sabe quién puede obtener acceso no deseado a ellos. Además, el malware puede ejecutarse más fácilmente como administrador porque no tiene

una contraseña. Anteponer la seguridad por comodidad al iniciar sesión nunca es una buena idea.

- Al crear una contraseña, debe tener **al menos ocho caracteres de longitud**, pero idealmente 12 o incluso 20 si es posible. Tendremos que asegurarnos de que incluye una **combinación aleatoria de letras mayúsculas y minúsculas, números y símbolos**. Idealmente, no debería estar relacionado de ninguna manera con nuestro nombre, nombre de usuario o nombre de la empresa. Nos aseguraremos de que las contraseñas no incluyan palabras completas de ningún diccionario. Los diccionarios son lo primero que usan los crackers para hackear contraseñas.
- **No usar la misma contraseña para más de una cuenta**. Todas las contraseñas deben ser únicas y deberemos usar un sistema como LastPass, KeePass, Roboform o algo similar para realizar un seguimiento de ellas.
- **Al crear un PIN, usaremos cuatro dígitos diferentes** para hacer que las cosas sean un poco más difíciles de descifrar.
- **Al crear una contraseña de imagen, escogeremos una foto que tenga al menos 10 "puntos de interés".** Los puntos de interés son áreas que sirven como punto de referencia para los gestos. Usaremos una mezcla aleatoria de tipos de gestos y secuencia y nos aseguraremos de no repetir el mismo gesto dos veces. Hay que tener en cuenta que las manchas en la pantalla podrían revelar los gestos a los demás.

La seguridad de la contraseña frente al PIN y la contraseña de la imagen

Cualquier tipo de contraseña se puede descifrar con suficiente esfuerzo y las herramientas adecuadas. No existe una contraseña completamente segura.

Sin embargo, las contraseñas creadas usando solo unos pocos principios de seguridad son mucho más difíciles de descifrar que otras. Si respeta las recomendaciones

compartidas en la sección anterior de esta unidad, terminará teniendo contraseñas razonablemente seguras.

De todos los métodos de inicio de sesión en Windows, el PIN es la fuerza bruta más fácil porque los PIN están restringidos a cuatro dígitos y solo hay 10,000 combinaciones únicas posibles disponibles. La contraseña de la imagen es más segura que el PIN porque brinda muchas más oportunidades para crear combinaciones únicas de gestos.

Con el fin de desalentar los ataques de fuerza bruta contra las contraseñas y los PIN de las imágenes, después de cinco intentos fallidos, Windows establece de manera predeterminada la contraseña de texto tradicional.

El PIN y la contraseña de la imagen funcionan solo como métodos de inicio de sesión alternativos a Windows. Por lo tanto, si alguien las descifra, no tendrá acceso a la contraseña de su cuenta de usuario. Sin embargo, esa persona puede usar todas las aplicaciones instaladas en el dispositivo, acceder a sus archivos, datos, etc.

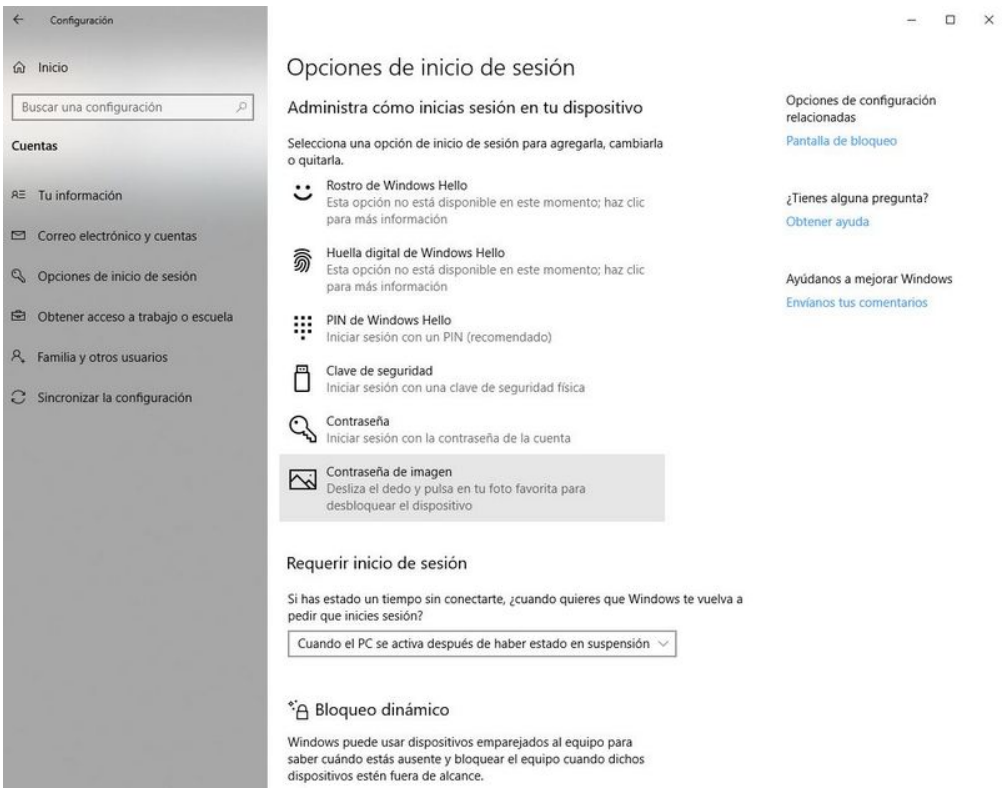
Cómo crear un PIN en Windows

Si iniciamos sesión en un dispositivo Windows con una cuenta de usuario que tiene una contraseña que no está en blanco, podemos crear un PIN de 4 dígitos para usarlo como método de inicio de sesión complementario.

Para crear uno, debemos ir a "Configuración". Si no sabemos cómo, presionamos la tecla Windows en el teclado o haremos click en el boton inicio del lado izquierdo de la pantalla, y luego presionamos "Configuración".

En la ventana de configuración, iremos a Cuentas y luego a “Opciones de inicio de sesión”. Aquí encontraremos todas las opciones necesarias para cambiar la contraseña existente, crear un PIN o una contraseña de imagen.

Para crear un PIN, presionamos el botón "Agregar" en la sección PIN. Se iniciará el asistente "Crear un PIN" y se nos solicitará que introduzcamos la contraseña de la cuenta de usuario. Lo escribimos y presionamos "Aceptar". Ahora nos pedirá que introduzcamos un pin de 4 dígitos en los campos "Introducir PIN" y "Confirmar PIN". El PIN se ha creado y ahora podremos usarlo para iniciar sesión en Windows.



Cómo crear una contraseña de imagen en Windows

Si iniciamos sesión en un dispositivo Windows con una cuenta de usuario que tiene una contraseña que no está en blanco, también podemos crear una contraseña de imagen

y usarla como un método de inicio de sesión complementario. Para crear uno, debemos ir a "Configuración de PC".

En Configuración de PC, iremos a Cuentas y luego a “Opciones de inicio de sesión”. Aquí encontraremos todas las opciones necesarias para cambiar la contraseña existente, crear un PIN o una contraseña de imagen. Para crear una contraseña de imagen, presione el botón "Agregar" en la sección "Contraseña de imagen".

El asistente "Crear una contraseña de imagen" se inicia y nos solicita que ingresemos la contraseña de la cuenta de usuario. Nos muestra una guía sobre cómo funciona la contraseña de la imagen. Podemos aprovechar para verlo y aprender los gestos que se pueden usar para la contraseña de imagen. Veremos que se puede crear una combinación de círculos, líneas rectas y toques. Cuando estemos preparados, presionaremos "Elegir imagen". Exploramos las carpetas y seleccionaremos la imagen que deseamos usar para la contraseña y presionamos “Abrir”.

Ahora podemos arrastrar la imagen para colocarla de la manera que deseemos. Cuando nos guste cómo se posiciona la imagen, presionaremos “Usar esta imagen” a la izquierda. Si no estamos satisfechos con la imagen, presionamos “Elegir nueva imagen” y seleccionamos una nueva, como se muestra en el paso anterior.

Una vez que hayamos confirmado que deseamos utilizar esta imagen, se nos pedirá que configuremos los gestos para la contraseña de la imagen. Dibujamos tres gestos en la imagen, cualquier combinación que deseemos. Hay que recordar que solo pueden usar tres gestos: círculos, líneas rectas y toques. Una vez que hayamos dibujado esos tres gestos, se nos pedirá que confirmemos. Dibujaremos los mismos gestos una vez más.

Si todo va bien, nos informa que se ha creado la contraseña de imagen y que podemos usarla la próxima vez que iniciemos sesión en Windows. Si no confirmamos los gestos correctamente, se nos pedirá que lo intentemos nuevamente, hasta que dibujemos los mismos gestos dos veces. Para cerrar el asistente de contraseña de imagen, presionamos "Finalizar".

¿Dónde almacena Windows sus contraseñas? ¿Es seguro?

Todas las contraseñas que usamos en Windows y guardamos para uso futuro se almacenan en el Administrador de credenciales. Esta herramienta es una caja fuerte con los nombres de usuario y las contraseñas que usa para iniciar sesión en el equipo, en otros equipos de la red, en aplicaciones de la Tienda Windows o en sitios web que usan Internet Explorer.

Al almacenar estas credenciales, Windows puede iniciar sesión automáticamente la próxima vez que acceda a la misma aplicación, recurso compartido de red o sitio web. Todo lo que está almacenado en el Administrador de credenciales está encriptado para su protección.

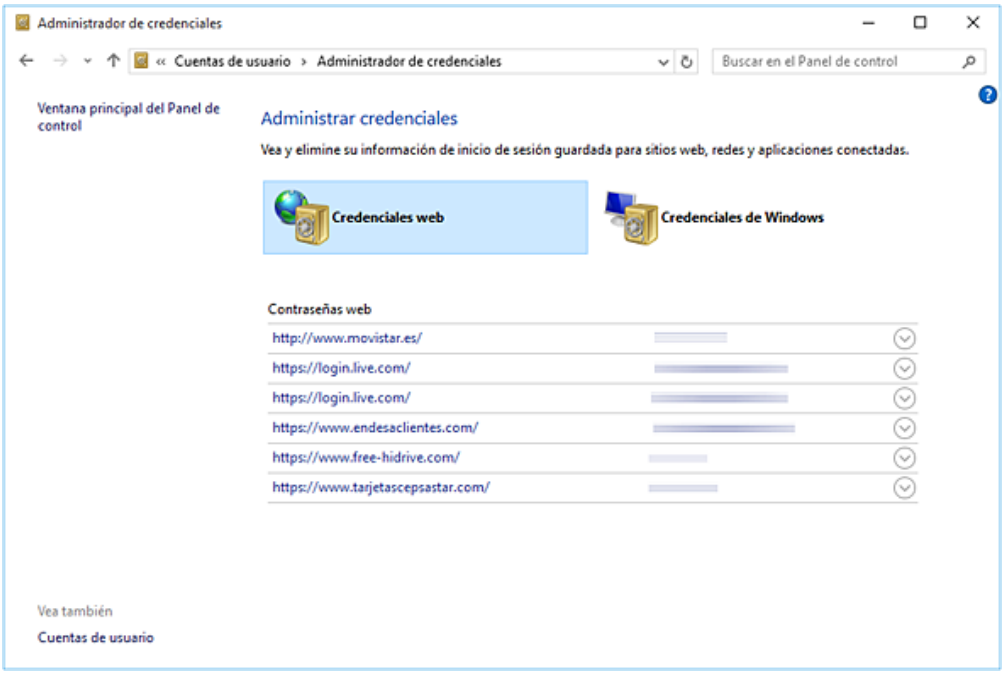
Para acceder al Administrador de credenciales, debemos abrir el *Panel de control* e ir a "*Cuentas de usuario -> Administrador de credenciales*". A partir de los sistemas operativos Windows 8, el Administrador de credenciales tiene dos almacenes principales: *"Credenciales web"* y "*Credenciales de Windows"*.

El almacén de credenciales web almacena los nombres de usuario y las contraseñas que usamos en las aplicaciones de la Tienda Windows, y cuando iniciamos sesión en sitios web en Internet Explorer. Los navegadores de terceros tienen sus propias funciones de almacenamiento de contraseñas y no almacenan sus nombres de usuario y contraseñas en el almacén de Windows.

Cuando naveguemos a través de estas credenciales, veremos que se muestran de forma cifrada y no se puede saber para qué aplicaciones o sitios web se utilizan, ni se pueden conocer las credenciales de inicio de sesión reales.

En el almacén de credenciales de Windows, se almacenan los detalles de inicio de sesión para nuestro ordenador, para el grupo en el hogar y para acceder a otros dispositivos en la red. Estas credenciales también están encriptadas y no se pueden averiguar las contraseñas que se almacenan al observar cada entrada en el almacén.

En Windows 7, el Administrador de credenciales solo tiene un almacén: el de Windows. Windows 7 no utiliza un almacén de credenciales web para almacenar los nombres de usuario y las contraseñas utilizadas al navegar por la web en Internet Explorer.



Cómo agregar credenciales para acceder a otro equipo en la red

Podemos agregar manualmente las credenciales de inicio de sesión para acceder a una dirección de Internet o de red u otro equipo en la red. Veremos un ejemplo de cómo funciona todo el proceso. En este caso, agregaremos las credenciales para un ordenador en red a cuyos recursos compartidos deseamos acceder.

1. En el Administrador de credenciales, haremos clic en el enlace que dice "*Agregar una credencial de Windows"* en la sección de Windows.
2. En la ventana "*Agregar una credencial de Windows*", escribiremos la dirección IP o el nombre del equipo de red al que deseamos acceder.
3. En el campo "*Nombre de usuario*", escribiremos primero el nombre de ese equipo, seguido de \ y luego la cuenta de usuario que utilizaremos para iniciar sesión.
4. En el campo "*Contraseña*", escribiremos la contraseña para esa cuenta de usuario. Cuando terminemos, presionamos "*Aceptar*" y las credenciales se

almacenarán y usarán automáticamente la próxima vez que accedamos a ese equipo de red.

Cómo quitar credenciales del administrador de credenciales

Hay situaciones en las que un equipo de la red ha cambiado la contraseña de la cuenta de usuario que utiliza para acceder. En este caso, ya no querremos que Windows use esas credenciales antiguas para acceder a ese equipo. Para eso podemos eliminarlos fácilmente del Administrador de credenciales:

1. Iremos a la sección Credenciales de Windows y seleccionaremos las credenciales para ese equipo en concreto, luego haremos clic en el botón "*Eliminar*".
2. Se nos pide que confirmemos la eliminación de las credenciales, presionamos "*Sí*" y se eliminarán.
3. Ahora podemos ingresar las nuevas credenciales en el Administrador de credenciales o podemos acceder a ese equipo de red como lo haríamos normalmente, y nos pedirá que ingresemos las nuevas.
   Obviamente, terminarán siendo almacenadas en el Administrador de credenciales.

El proceso para eliminar credenciales para sitios web y aplicaciones es el mismo. La única diferencia es que debemos ir a la sección Credenciales web.

Cómo hacer una copia de seguridad de los nombres de usuario y contraseñas almacenados en Windows

Una característica poco conocida de Windows es que se puede hacer una copia de seguridad manual de los nombres de usuario y contraseñas almacenados en un archivo cifrado y bloqueado con una contraseña. Este archivo tiene la extensión ".crd"

(Credential Backup Files) y se puede almacenar en un disco duro externo, una tarjeta de memoria o cualquier carpeta del ordenador.

Para hacer una copia de seguridad, seguiremos los siguientes pasos:

1. Hacer clic en el enlace que dice "*Copia de seguridad de credenciales*" en la sección Credenciales de Windows.
2. Se muestra la ventana "*Nombres de usuario y contraseñas almacenados*". En este apartado, hacemos clic en "*Examinar*", seleccionamos la ubicación donde deseamos guardar el archivo, le ponemos un nombre y presionamos "*Guardar*".
3. Para ir al siguiente paso, presione "*Siguiente*". Presionamos "*Ctrl + Alt + Supr*" para continuar la copia de seguridad en un escritorio seguro, que no puede ser interceptado tomando capturas de pantalla remotas o cualquier tipo de herramientas de monitoreo remoto.
4. La pantalla se volverá negra y solo veremos la ventana "*Nombres de usuario y contraseñas almacenados*". Aquí nos pide que escribamos una contraseña para proteger el archivo que vamos a crear. Escribiremos una contraseña larga, utilizando las recomendaciones que hicimos anteriormente en esta lección, y luego presionamos "*Siguiente*".
5. Ahora nos informa que la copia de seguridad se realizó correctamente. Las credenciales ahora se almacenan en el archivo que hemos creado, en la ubicación que seleccionamos anteriormente. Presionamos "*Finalizar*" para cerrar el asistente.

Ahora podemos usar este archivo de respaldo para restaurar los nombres de usuario y contraseñas en otro equipo o en el mismo equipo en el caso que tuviéramos que reinstalar el sistema operativo.

Cómo restaurar los nombres de usuario y contraseñas almacenados por Windows

Si disponemos de un archivo de respaldo con todos los nombres de usuario y contraseñas que hemos utilizado en un ordenador con Windows, podemos usarlo en cualquier momento para restaurarlo en el mismo equipo, en caso de que hayamos reinstalado el sistema operativo u en otro equipo que estemos usando.

Para restaurar los nombres de usuario y contraseñas:

1. Tendremos que acceder al Administrador de credenciales y luego a la sección Credenciales de Windows. Buscamos el enlace que dice "*Restaurar credenciales"* y hacemos clic en él.
2. Nos mostrará la ventana "*Nombres de usuario y contraseñas almacenados*". Hacemos clic en "*Examinar*" y seleccionamos el archivo de respaldo que deseamos usar, luego presionamos "*Siguiente*".
3. Presionamos "*Ctrl + Alt + Supr*" para continuar la copia de seguridad en un escritorio seguro, que no puede ser interceptado tomando capturas de pantalla remotas o cualquier tipo de herramientas de monitoreo remoto.
4. La pantalla se volverá negra y solo veremos la ventana "*Nombres de usuario y contraseñas almacenados*". Aquí nos pide que escribamos la contraseña utilizada para proteger el archivo. Lo escribimos y presionamos "*Siguiente*".
5. Nos informa que las credenciales han sido almacenadas.
6. Presionamos "*Finalizar*" para cerrar el asistente. Windows usará automáticamente los nombres de usuario y las contraseñas que hayamos restaurado cuando sea necesario.

ATAQUES POR EMAIL

El *phishing* es una técnica utilizada por ciberdelincuentes para obtener información personal y bancaria de los usuarios. Les envían mensajes suplantando a una entidad legítima como puede ser un banco, una red social, un servicio, una entidad pública, etc. El objetivo es engañarles y manipularles a fin de que acaben realizando alguna acción que ponga en peligro sus datos.

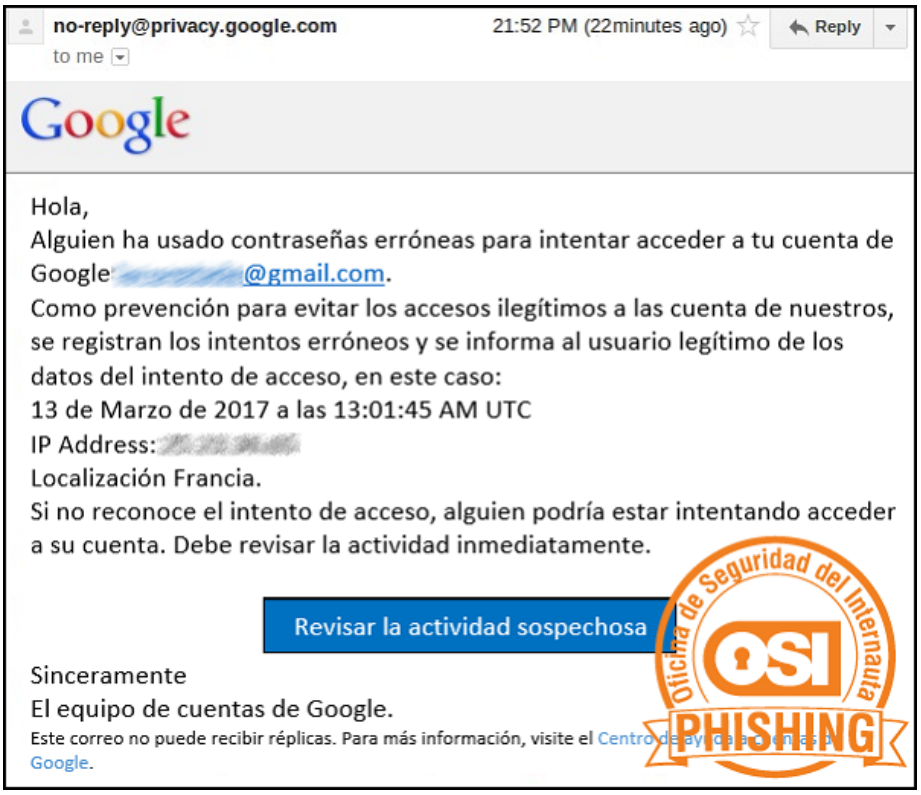
Cómo evitar ser víctima de phishing

- **Sé precavido ante los correos** que aparentan ser de entidades bancarias o servicios conocidos (*Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.*) con mensajes que no esperabas, que son alarmistas o extraños.
- **Sospecha si hay errores gramaticales** en el texto, pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.
- **Si recibes comunicaciones anónimas** del tipo "Estimado cliente", "Notificación a usuario" o "Querido amigo", es un indicio que te debe poner en alerta.
- Si el mensaje **te obliga a tomar una decisión de manera inminente** o en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.
- Revisa si el texto del **enlace que facilitan en el mensaje coincide con la dirección a la que apunta**, y que ésta corresponda con la URL del servicio legítimo.
- Un **servicio con cierto prestigio utilizará sus propios dominios** para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

- Aplica la ecuación: **solicitud de datos bancarios + datos personales = fraude**.

Cómo reconocer un mensaje de tipo phishing



1. ¿El contenido es sospechoso?

El primer paso para identificar un phishing es valorar el contenido del mensaje o correo electrónico. Como hemos mencionado anteriormente, el intento de suplantación puede ser a un banco, una plataforma de pago, una red social, un servicio público, etc.

El objetivo es intentar asustar al usuario e instarle a actuar según las indicaciones del mensaje. Siempre añaden una excusa, ejemplo "problemas técnicos o de seguridad", y proporcionan una solución sencilla del tipo "acceda a su banco utilizando este enlace". Además, es muy habitual que soliciten nombre de usuario, claves y otros datos de acceso a las cuentas, práctica que las entidades legítimas nunca llevarían a cabo.

2. ¿La escritura es correcta?

Si nos fijamos en la imagen anterior, podemos ver que, por ejemplo, no se han utilizado tildes y que hay errores gramaticales (enes en lugar de eñes), y de puntuación. Resulta extraño que una entidad envíe una comunicación a todos sus clientes con una redacción y ortografía descuidadas. Los delincuentes que realizan las campañas de estafa, en ocasiones son extranjeros, y deben por tanto traducir sus mensajes al español, en general con errores. Estos errores en la traducción aparecen en forma de:

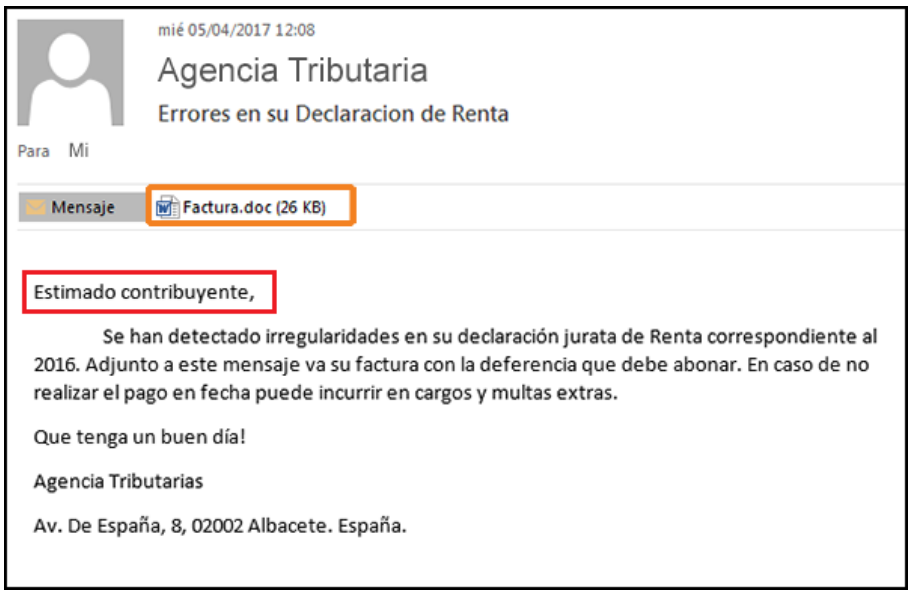
- **Fallos semánticos**: artículos "el" o "la" intercambiados.
- **Palabras con símbolos extraños**: donde deberían estar palabras acentuadas como por ejemplo: "*DescripciÃ?n".* Este caso aparece al intentar escribir vocales acentuadas en un teclado no español.
- **Frases mal construidas**.

Si detectamos que el correo tiene una ortografía pobre y su escritura es informal, debemos estar alerta.

3. ¿A quién va dirigido el correo?

Si un delincuente quiere estafar a cientos de miles de personas, es muy complicado saber el nombre de todas esas personas. Por ello, utilizan fórmulas genéricas como "Estimado cliente", "Hola", "Hola amigo", etc. para evitar decir un nombre:

Cuando una entidad tiene que dirigirse por correo a un usuario o cliente, siempre lo hará enviando correos electrónicos personalizados, donde utilizará el nombre de la persona e incluso en algunas ocasiones, parte de su DNI. Si recibimos un correo no personalizado, estamos probablemente ante un caso de intento de estafa.



4. ¿Pide hacer algo de manera urgente?

Otra técnica utilizada por los delincuentes es la de pedir la realización de una acción en un período de tiempo muy corto: "Una vez emitido este correo electrónico, tendrá un plazo de 8 horas para llevar a cabo dicha acción, de lo contrario…":

Con esta urgencia, los delincuentes intentan que su víctima tome una decisión precipitada y caiga en la trampa, que incluye visitar un enlace e indicar datos personales y/o contraseñas. Este es otro síntoma que nos hace sospechar que el mensaje recibido ha sido enviado por un delincuente.

5. ¿El enlace es fiable?

La intención de los delincuentes es que pinchemos en un enlace para llevarnos a un sitio web fraudulento. En el texto del mensaje hay un enlace que en lugar de llevarte a la web oficial, página legítima, te lleva a otra fraudulenta que estéticamente es igual o muy parecida.

¿Cómo podemos saber la verdadera dirección a la que apunta un enlace? Muy fácil: situando el puntero encima del enlace y observando la verdadera dirección que se muestra en la parte inferior izquierda del navegador.

Una recomendación a seguir es la de no acceder a una web a través de un enlace en el correo electrónico. Si deseamos acceder a la web legítima, la mejor práctica es escribir directamente en la barra de direcciones del navegador la dirección deseada (si se conoce previamente).

6. ¿Quién envía el correo?

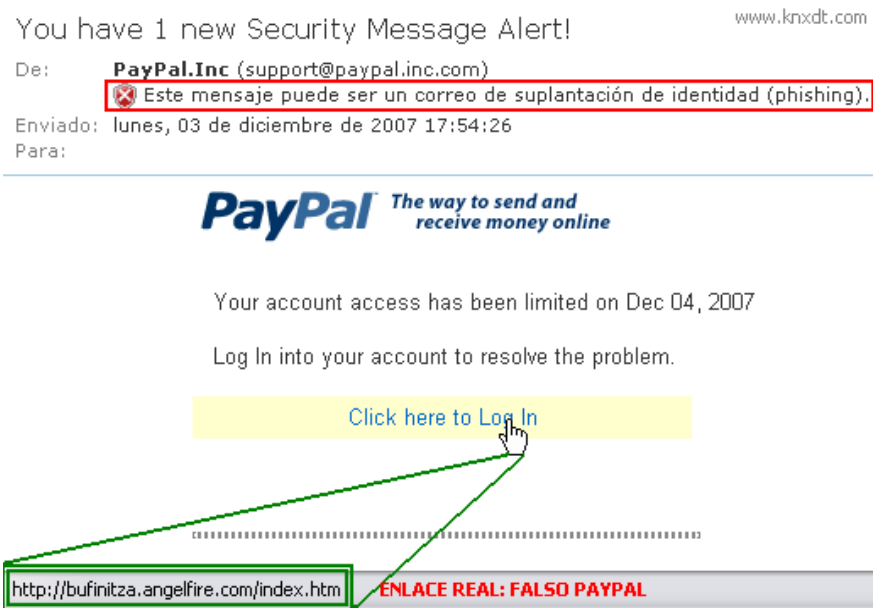
Por último, sólo nos queda comprobar la identidad del remitente. Hemos dejado esta pregunta para el final ya que no ofrece garantías para saber a ciencia cierta si un correo es fiable o no.

Debemos sospechar si el remitente es una dirección de correo que no pertenece a la entidad, como sucede en el siguiente ejemplo, que el mensaje hace referencia a PayPal y el email del remitente no hace ninguna alusión a dicho servicio.

El hecho de que el correo provenga de un correo aparentemente correcto no es indicio concluyente de la legitimidad del mismo. El remitente de un correo electrónico puede ser manipulado y los delincuentes son capaces de enviar correos con el remitente falsificado en nombre de entidades.

Medios usados para propagar phishing

El principal medio de propagación del phishing es el correo electrónico, pero que sea el método más utilizado no implica que sea el único. También pueden utilizarse otros medios como redes sociales, sistemas de mensajería instantánea, etc. Por cualquiera de estas vías es muy sencillo enviar un mensaje que contenga un enlace que nos redirija a un sitio fraudulento.



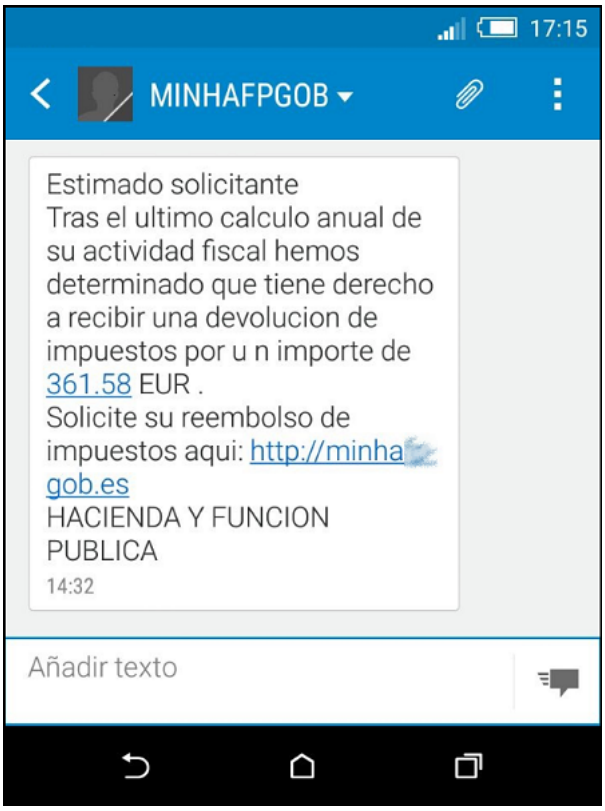
Cómo actuar si detectas un phishing

- No facilites la información que te solicitan ni contestes en ningún caso a estos mensajes. En caso de duda consulta directamente a la empresa o servicio que supuestamente representan a través de sus canales oficiales.
- No accedas a los enlaces facilitados en el mensaje ni descargues ningún documento adjunto que puede contener, podría tratarse de malware.
- Elimínalo y si puedes, alerta a tus contactos sobre este fraude para que ellos no caigan tampoco en la trampa.

Qué hacer si has caído en la trampa

En caso de haber sido víctima de un fraude de tipo phishing, recopila toda la información que te sea posible: correos, capturas de conversaciones mediante mensajería electrónica, documentación enviada, etc. Puedes apoyarte en testigos online para la recopilación de evidencias.

Para los casos de phishing bancario, contacta con tu oficina bancaria para informarles de lo sucedido con tu cuenta online. Adicionalmente, modifica la contraseña de todos aquellos servicios en los que utilizases la misma clave de acceso que para el servicio de banca online. Recuerda: no uses la misma contraseña en varios servicios, es muy importante gestionar de forma segura las contraseñas para evitar problemas. A continuación, presenta una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).



Para la mayoría de usuarios, la cara visible de la informática es Internet. Desde todo tipo de dispositivos (ordenadores, tabletas y smartphones) accedemos a la red en busca de información, entretenimiento y otros servicios.

Para ello, la herramienta fundamental es el navegador. Resultan tan intuitivos y fáciles de usar que muchas veces ni nos damos cuenta de su existencia. Existen varios a nuestra disposición, todos muy conocidos: Chrome, Internet Explorer, Safari, Firefox, etc.

Además, muchos de ellos incorporan un buscador, lo que nos facilita la tarea de localizar aquello que necesitamos.

Poco a poco han ido ganando funcionalidades que nos hacen la vida en Internet más fácil: guardan un historial de los lugares que visitamos, autocompletan las

palabras o frases que escribimos e, incluso, recuerdan las contraseñas de acceso a los servicios.

Estas prestaciones son muy útiles, pero debemos tener en cuenta que los navegadores son empleados también por individuos malintencionados para acceder a nuestros dispositivos. Por ello, hemos de conocer sus riesgos y adoptar precauciones para poder disfrutar de las ventajas de la tecnología de forma segura.

PRIVACIDAD

Los navegadores incorporan muchas funciones para hacernos la vida más fácil. Sin embargo, en ocasiones esto puede suponer un verdadero riesgo para nuestra privacidad:

- El historial de navegación es el registro completo de toda nuestra actividad en Internet. Cualquier persona que tenga acceso a nuestro navegador podrá ver qué hemos estado haciendo y cuándo.
- Normalmente visitamos las mismas páginas web y buscamos cosas parecidas. Por ello cuando tecleamos una búsqueda el navegador nos

ofrece una selección de búsquedas basadas en otras anteriores. Esto nos ahorra el trabajo de escribir, por ejemplo, las direcciones completas.

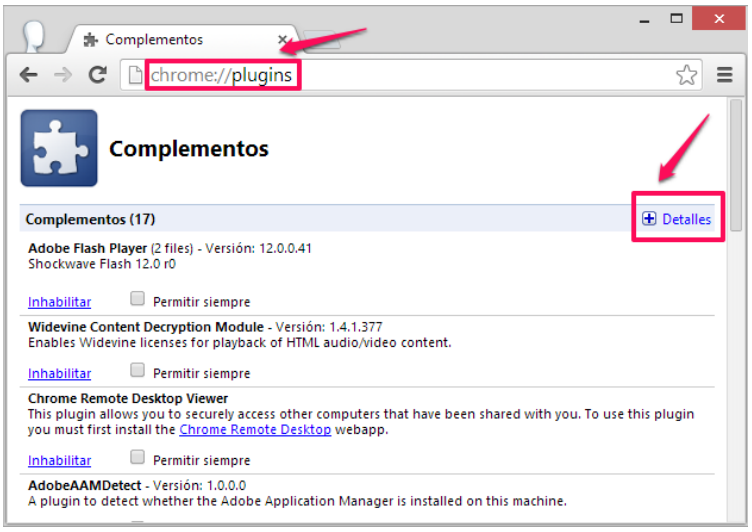
- Sin embargo, cualquier persona que emplee nuestro navegador verá esas mismas sugerencias cuando comience a escribir, lo que le dará pistas acerca de nuestro comportamiento y preferencias.
- Es habitual que cada vez más servicios de Internet requieran que utilicemos un nombre de usuario y contraseña para acceder. Que el navegador los recuerde implica que cualquier persona con acceso a nuestro navegador puede suplantar nuestra personalidad en todos esos sitios.
- Si cuando entramos en las redes sociales (Google+, Facebook, Twitter, etc.) seleccionamos la opción de 'mantener la sesión abierta', no bastará con cerrar la página para cerrar la sesión. Cualquiera que entre a estas redes con nuestro navegador tendrá acceso a nuestro perfil.
- Normalmente, las funciones que nos hacen la navegación más fácil tienen un lado oscuro: la pérdida de privacidad.
- Para limitar los riesgos de privacidad, podemos utilizar las pestañas de navegación privada que existen en los principales navegadores. Éstas reducen la información que el navegador almacena de nosotros, como el historial, cookies, o archivos temporales, lo que resulta muy útil cuando navegamos desde ordenadores públicos.

Los complementos y plugins

Los complementos o extensiones son elementos que se instalan en nuestros navegadores para hacerlos más eficientes, encargándose de funciones específicas: barras de búsqueda, integración con otros servicios, bloqueo de pop-ups, etc.

Sin embargo, algunos de estos complementos pueden estar destinados a fines malintencionados: recopilar información acerca de nuestros hábitos o insertar anuncios. Generalmente, esto se hace de forma encubierta al instalar aplicaciones gratuitas, por lo que es importante revisar las opciones de instalación.

También hay que tener cuidado con algunas aplicaciones asociadas a los navegadores (o plugins) que tenemos instaladas sin ser conscientes de ello: Java, Flash, reproductores de vídeo, etc. Muchas de éstas son utilizadas como vía de acceso para infectar nuestro ordenador debido a sus fallos de seguridad.



Las cookies

Las cookies son pequeños ficheros que los navegadores almacenan en el ordenador con datos del usuario sobre las páginas web visitadas.

Esta información puede contener las opciones de idioma o visualización elegidas, el contenido que ha sido consultado, el identificador de sesión de un usuario o las credenciales de acceso. Su utilidad es facilitar la navegación aunque, una vez guardada, la información puede servir para otros propósitos.

Hoy en día no tenemos, para el usuario medio, muchas alternativas aparte de aceptar el uso de cookies. Si las desactivamos, es posible que algunos servicios no funcionen correctamente. No obstante, puedes borrar periódicamente las cookies instaladas en tu equipo (consulta cómo hacer esto con Chrome, Internet Explorer y Firefox).

Actualizaciones

Los navegadores también están expuestos a fallos de seguridad que pueden suponer una puerta de acceso para que individuos maliciosos accedan a nuestra información o tomen el control de nuestros dispositivos.

Por tanto, hemos de mantenerlos al día, preferiblemente a través de la opción de actualizaciones automáticas. Esta funcionalidad viene incorporada por los principales navegadores.

Navegador	Cómo actualizar
Internet Explorer	En Windows, el navegador se actualiza a través del mismo mecanismo del sistema operativo: activando las actualizaciones automáticas.
Firefox	Se actualiza de forma automática por defecto. Al ejecutarlo, busca actualizaciones, no sólo del navegador, sino de todos los accesorios (complementos o plugins) instalados. Lo descarga y pide permiso para reiniciarlo.

Chrome	Se actualiza de forma automática por defecto. Al ejecutarlo, busca actualizaciones, no sólo del navegador, sino de todos los accesorios (complementos o plugins) instalados.
Safari	Se actualiza de forma automática por defecto. Al ejecutarlo, busca las actualizaciones; si las encuentra muestra una ventana con información acerca de la actualización y de cómo instalarla. Para forzar la actualización se haría del mismo modo que al actualizar el software del sistema operativo.

Las actualizaciones de software son esenciales para mantener la seguridad de nuestros dispositivos y nuestra información.

Recomendaciones

Navegar por Internet no es como ver una revista. Si no somos cuidadosos estamos expuestos a toda una serie de riesgos: robo de información, pérdida de privacidad, o perjuicio económico entre otros.

Por tanto, si queremos disfrutar de las ventajas de la tecnología sin incurrir en riesgos debemos tomar ciertas precauciones al navegar:

- Evitar utilizar la opción de recordar contraseñas.
- Cerrar las sesiones a través de la opción 'logout' o 'cerrar sesión', en lugar de simplemente cerrar la ventana.

- Desmarcar la opción de 'mantener la sesión abierta' al iniciar una sesión en redes sociales o servicios de correo electrónico, especialmente si estamos en un equipo compartido.
- Revisar de vez en cuando los complementos y extensiones instaladas. Instalar sólo aquellos con buena reputación y ofrecidos en las páginas oficiales de los navegadores.
- Emplear la opción de navegación 'en privado' en equipos compartidos o públicos.
- Instalar un verificador de páginas web, normalmente proporcionado por los principales antivirus.
- Proteger nuestra privacidad evitando las opciones que permiten al navegador guardar información sensible.
- Familiarizarnos con las opciones de ajuste que ofrece nuestro navegador.
- Mantener el navegador actualizado.
- Estar alerta y no visitar páginas sospechosas.

NAVEGACIÓN SEGURA

Uno de los métodos de infección más utilizados por el ransomware es la explotación de vulnerabilidades en los navegadores web. Para ello, se recurre a los exploits, que son programas diseñados para explotar vulnerabilidades conocidas en las aplicaciones con el fin de conseguir el control total sobre el sistema atacado.

Sin embargo, éste no es el único método de infección que está relacionado con los navegadores web, también se puede emplear el Phishing o cualquier otro método que termine con la ejecución de código dañino en el equipo víctima (memorias USB de propaganda, regaladas o encontradas, Apps de moda, servicios web, etc.).

Para protegerse de este tipo de ataques, la recomendación básica es mantener actualizado tanto el navegador web como las extensiones o complementos instalados en el mismo.

De ese modo, al navegador se le habrán aplicado todas las correcciones conocidas y con ello se estará disminuyendo el número y extensión de los puntos débiles que puede emplear el atacante (superficie de exposición).

Complementos y extensiones

Además, se recomienda hacer uso de extensiones o complementos del navegador web cuyo fin sea aumentar la seguridad de estos. Las extensiones recomendadas son las que bloquean la apertura de ventanas emergentes, como es el caso de AdBlock24 (Google Chrome y Mozilla Firefox), que evitaría la carga de páginas no solicitadas por el usuario o que son conocidas por ser dañinas. Como complemento, para evitar la aparición de ventanas emergentes, se puede añadir el plugin PopUp Blocker.

También se recomienda utilizar extensiones para protegerse contra Phishing (que están incluidas en los navegadores principales) y otras amenazas, como puede ser la extensión Avast Online Security para Google Chrome.

En caso de utilizar otros navegadores que no permitan este tipo de extensiones, como es el caso de Internet Explorer, se pueden emplear herramientas como el filtro SmartScreen, que indica si la página a la que se está accediendo es legítima o pretende

suplantar la identidad de otra. Para activar ese filtro se selecciona la pestaña Seguridad Filtro SmartScreen Activar el filtro.

Una medida más drástica, pero muy eficaz, es la desactivación de la ejecución de JavaScript, permitiendo su activación sólo en sitios web de confianza. La ejecución de este tipo de código es peligrosa porque puede permitir la activación automática de código dañino que descargue y ejecute el ransomware en la máquina.

La desactivación de JavaScript se puede conseguir en la configuración del propio navegador web o mediante el uso de extensiones como NoScript (FireFox) y ScriptSafe (Chrome). Esta medida, eficaz en la prevención de ejecución de código dañino, es la más intrusiva para el usuario y puede dar problemas con algunos de sus sitios web habituales, haciendo que estos no se muestren como deberían o eliminando algunas funcionalidades.

Entre estas funcionalidades se encuentran algunos plugins, la visualización de datos, presentaciones web, buscadores y elementos gráficos en general. La desactivación de JavaScript, por tanto, da un aspecto mucho más plano de la web.

2. GESTIÓN DE RECURSOS HUMANOS

Fuga de datos

El 43% de las empresas españolas han sufrido la fuga de datos por acciones de sus empleados, y los cuatro perfiles principales de los empleados son:

- **Ambiciosos**: roban información de su empresa para vendérsela a la competencia.
- **Rencorosos**: empleados despedidos que se quieren vengar de sus empresas divulgando información confidencial o manchando su reputación.
- **Despistados**: cometen errores en la gestión de la información por despiste o por falta de formación.
- **Moralistas**: empleados que ponen denuncias a sus empresas o divulgan información porque no consideran que su empresa actúa de forma ética.

La eliminación de la información del equipo por parte del empleado desleal antes de abandonar la empresa así como el envío de información relevante de la empresa a la competencia son los sabotajes habituales en las investigaciones relacionadas con fugas de información.

El descontento a nivel laboral y personal, así como la mala situación económica existente y la posibilidad de obtener ingresos extras de manera fácil son algunos de los aspectos que llevan a los empleados a cometer hurtos en las empresas.

La mitad de los empleados que perdieron sus puestos de trabajo en el último año, mantuvieron en su poder datos confidenciales de su empresa. Además, el 40% tiene planeado usar dicha información en sus nuevos puestos de trabajo. El origen del

problema es que los empleados habitualmente se llevan información de la empresa fuera de la compañía y nunca la eliminan y piensan que no están cometiendo ningún delito.

Ataques dirigidos

Los ataques dirigidos con un objetivo determinado están creciendo espectacularmente en las pymes. Los ciberataques dirigidos y el espionaje son las principales predicciones de ataques para este año contra la seguridad informática.

Cualquiera sin conocimientos informáticos puede adquirir en el mercado negro de Internet un kit que le permite entrar en un ordenador de alguien en particular, en el caso de que no estuviera securizado, y controlarlo remotamente, con lo que perdemos toda nuestra privacidad, datos, correos electrónicos, claves, etc.

Nunca fue tan fácil lanzar un ataque contra una web o espiar a una persona. El comercio clandestino destinado al cibercrimen ha crecido tanto en estos últimos años que la competencia ha provocado que los precios estén actualmente por los suelos. Además estos "kit de ataque" se venden con un manual explicativo para que cualquiera sin conocimiento informático pueda llevar a cabo un ataque con resultado satisfactorio.

En el mercado negro por 500€ ofrecen un programa capaz de desactivar antivirus y robar datos.

La extorsión, el chantaje y las peticiones de rescate son los pilares básicos sobre los que se asienta el cibercrimen. El Ransomware es un tipo de software malicioso que cifra los datos del disco duro del ordenador y deja un mensaje de rescate, que reclama una cantidad de dinero para descifrar los archivos. Hay un tipo de troyano que se está utilizando en ataques dirigidos a empresas que destruye los equipos que infecta después de robar la información que guardan.

El riesgo de sufrir un ataque dirigido y que accedan a toda la información de su ordenador por ex-empleados, competencia o desequilibrados es muy alto, por lo que es totalmente necesario tener securizado el ordenador e implementadas las medidas de seguridad.

Medidas básicas de seguridad

Las medidas básicas de seguridad que debemos implementar en todos nuestros ordenadores para protegernos de los riesgos de seguridad son:

1. Trabajar con usuario sin permiso de administrador
2. Securizar los ordenadores y revisarlos anualmente
3. Tener instalado un UTM (cortafuegos) como seguridad perimetral

Medidas de seguridad en la empresa

La necesaria securización de un ordenador consiste en un conjunto de configuraciones, actualizaciones y utilidades que minimizan el nivel de exposición a ataques, y por lo tanto, los riesgos y vulnerabilidades asociados a éstos. Para convertir el ordenador en

un bastión de seguridad, se aplican, entra otras, técnicas DEP, ASLR y de protección de la información.

Los ataques víricos se aprovechan de las vulnerabilidades o agujeros de seguridad, de ahí que para minimizar los riesgos es necesario mantener actualizado el sistema operativo y programas mediante la aplicación de los parches de seguridad. Por lo tanto, es necesario anualmente una Revisión de Seguridad de todos los ordenadores, con actualización de versiones de productos e instalación de nuevas herramientas de seguridad que garantice que podamos seguir protegidos frente a las nuevas amenazas.

El problema de seguridad de la anunciada muerte del sistema operativo Windows 7 en 2020 es que dejó de tener actualizaciones de seguridad de Microsoft y todas las vulnerabilidades no actualizadas serán foco de ataques y por lo tanto los ordenadores con Windows 7 dejarán de ser seguros por vulnerables. El coste de implementación de las medidas de seguridad es mínimo si tenemos en cuenta los perjuicios tras un incidente de seguridad, como son:

- **Pérdidas de tiempo de trabajo** para tratar de restaurar o regenerar la información perdida.
- Perjuicios ocasionados por la **imposibilidad de acceder a los datos** debido a su pérdida o problemas de conexión.
- **Robo y revelación** de información sensible o confidencial.
- **Impacto negativo en la imagen de la empresa** ante terceros que puede ocasionar una pérdida de confianza.
- **Retrasos** en los procesos de **producción**.
- **Incumplimientos legales** sancionados con elevadísimas multas de la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD) que obliga a que las empresas adopten las medidas necesarias que garanticen la seguridad de los datos y del nuevo Código Penal que hace

responsable penal a la empresa de los delitos cometidos por su falta de control ante el delito.

Como norma general, toda empresa debe tener implementadas las medidas de seguridad que garanticen la **Seguridad de la Información y el cumplimiento normativo**.

El **robo de credenciales** no es un problema exclusivo de las grandes compañías. De hecho, las grandes compañías invierten presupuesto y tecnología para proteger al máximo las credenciales de sus empleados y los accesos a los servicios en la Nube. El hecho de que sufran este tipo de ataques nos da una muestra del valor que tienen sus datos para los atacantes.

Para las pequeñas y medianas empresas, el robo de credenciales es también una vulnerabilidad que tener muy en cuenta. Las pérdidas pueden ser muy importantes, pero basta con establecer ciertas normas y protocolos para mitigar al máximo sus efectos. El robo de credenciales no es más que la **apropiación de los datos de inicio de sesión** en los servicios en la Nube con fines malintencionados.

Para prevenirlo, es necesario adoptar un **sistema de autenticación en dos pasos** y establecer unas pautas a la hora de crear nuevos usuarios y sus contraseñas. Estas

deben ser fuertes (aleatorias, complejas y que involucren varios tipos de caracteres, desde los alfanuméricos hasta los símbolos) y deben renovarse con cierta frecuencia, sobre todo para los accesos a servicios críticos.

Es importante disponer de un control riguroso de los accesos. Para ello, cada usuario debe tener un perfil de seguridad que permita, o deniegue, su acceso a ciertas áreas y servicios. Saber en cada momento qué usuarios acceden a qué servicios es esencial para detectar cualquier irregularidad o intrusión.

El enemigo en casa

Una vulnerabilidad bastante preocupante es la que se da cuando, por error o por desconocimiento, un empleado pone en riesgo datos o accesos a servicios esenciales. Más peligroso, aún, es cuando esta exposición se hace de manera intencionada por parte de un empleado desencantado, frustrado, o que simplemente trabaja para agentes externos malintencionados.

Para el primer caso, **la formación es esencial**. Se hace necesario formar al personal acerca de la importancia de mantener sus credenciales a salvo y de conocer, y seguir al pie de la letra, los protocolos de seguridad. Una buena formación puede minimizar los errores humanos al eliminar el desconocimiento de la ecuación.

Para los casos malintencionados, es necesario **protegerse previamente desde el punto de vista legal.** Esto es, dotar a los contratos laborales de políticas de confidencialidad estrictas que deriven en cláusulas legales disuasorias por la severidad de sus consecuencias. Además, para evitar que la rotación de empleados permita que personas que ya no pertenecen a la organización sigan teniendo sus accesos, es necesario disponer de un protocolo eficiente que elimine sus credenciales.

Por otro lado, garantizar que los procesos de cifrado y claves son fiables y reducir al mínimo el acceso de los usuarios a los sistemas más vulnerables o críticos contribuye a paliar los efectos de estos «*peligros internos*». De la misma manera que en otros casos, es importante contar con claves de cifrado fuertes y fiables e implementar sistemas de autentificación, autorización y auditoría fuertes.

El parque de ordenadores de la empresa puede estar protegida, pero eso no quiere decir que toda la información corporativa esté a salvo. Más allá de las tabletas, los teléfonos móviles o incluso los relojes inteligentes que han entrado recientemente a formar parte de los dispositivos que cualquier corporación debe controlar y proteger para evitar correr riesgos, en cualquier oficina hay un buen número de dispositivos cuyas vulnerabilidades pueden entrañar peligro para los datos confidenciales.

Aunque no se les suela prestar la debida atención en lo que a seguridad se refiere, las webcams constituyen todo un peligro para la privacidad corporativa, hasta tal punto que el mismísimo fundador y CEO de Facebook, Mark Zuckerberg, compartió una foto en la red social en la que se puede ver cómo él también tapa la cámara de su ordenador portátil por motivos de seguridad.

Hace poco se descubrió que una página web de 'streaming' rusa emitía en directo la señal de más de 70.000 webcams privadas que habían sido objeto de un ciberataque. En definitiva, la seguridad de estos pequeños dispositivos útiles para estar en contacto con alguien esté donde esté es tan relevante como la del resto del equipamiento. Tapar las de nuestra empresa cuando no están siendo utilizadas puede servir para poner a salvo la información corporativa.

La presencia de la cámara web es cada vez más común en los equipos de la empresa, sobre todo cuando se trata de ordenadores todo en uno (*ALL in One*) o portátiles que la llevan incorporada de serie.

Desde luego, en circunstancias concretas el valor añadido que presenta este dispositivo está claro, pero la realidad nos dice que estas ocasiones son más bien escasas y que, sin embargo, son demasiado frecuentes aquellas en las que la mera presencia o el uso inadecuado de la cámara web pueden ocasionar serios problemas.

¿Por qué hay que tener cuidado con la webcam?

La webcam ofrece información muy detallada sobre el usuario. Muestra al interlocutor la imagen del rostro, pero también una serie de datos nada desdeñables. La edad aproximada, el estado de ánimo, el lenguaje corporal y la expresividad, el tipo de ropa y de lugar de trabajo, si existen personas cerca y con qué frecuencia aparecen, datos de contextos como la fotografía de un acto empresarial o de un premio…

En el ámbito doméstico, por ejemplo, se dio un caso donde un depredador sexual que llegó a sus víctimas porque vio en su ropa el escudo del centro escolar al que asistían.

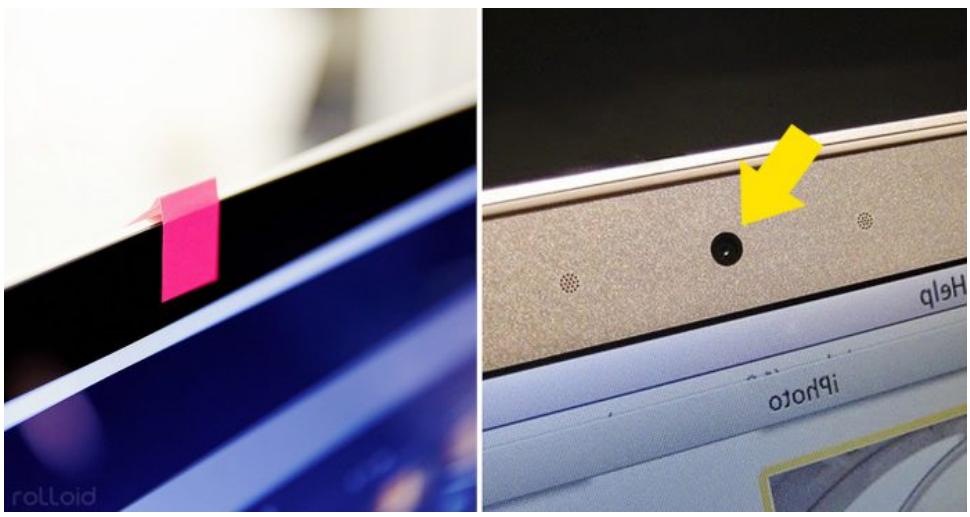
La webcam puede ofrecer información que no se pretendía mostrar

Suele ocurrir de forma accidental. Desde la Policía comentaban el caso de una adolescente chantajeada con hacer daño a su hermano pequeño al que conocían por haberle visto pasear de manera fortuita por delante de la cámara.

También podemos ver en la Red imágenes de adolescentes que ocultaban su rostro pero que, fruto de un descuido, presentan de manera involuntaria su identidad.

Lo que envía la webcam puede ser grabado al otro lado. Es algo evidente pero que con frecuencia obviamos. Consideramos que la secuencia que se muestra empieza y termina cuando se activa y se apaga la cámara y que es ofrecida a un único espectador.

No pensamos que esa secuencia puede ser grabada y que, por lo tanto, cualquiera puede llegar a verla. Es el clásico modus operandi en los casos de *grooming* donde, una vez obtenida y grabada esa imagen o secuencia comprometida, se pasa del engatusamiento al más cruel chantaje.



La cámara web puede ser manipulada de forma remota usando malware

Por desgracia, es algo demasiado sencillo. Instalando determinado programa malicioso en el equipo se puede manipular la cámara consiguiendo incluso desactivar el indicador luminoso que delata que se encuentra en funcionamiento.

No es adecuado usar el intercambio de imágenes para conocer la identidad de la otra persona. En ocasiones se piensa que teniendo webcam se puede conocer el aspecto del interlocutor al proponer cambiar su imagen por la propia.

Desde hace años, la Policía alerta de que las imágenes que creemos vienen de la webcam de la otra persona están en realidad manipuladas por ésta. Si esto ocurre, el efecto es aún más pernicioso porque confiamos en alguien que no es quien dice ser.

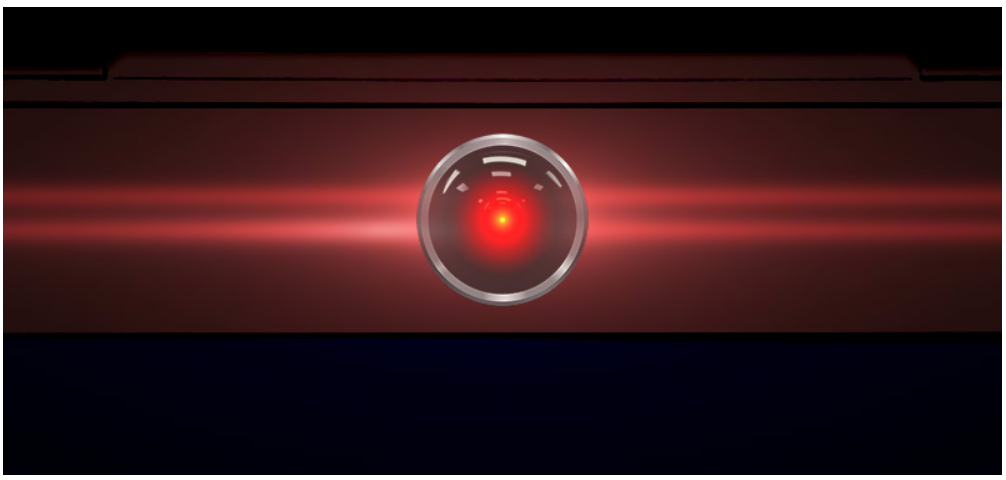
La disponibilidad de la webcam puede facilitar un uso irresponsable

Cierto es que hay otras muchas formas de captar una imagen o un vídeo y enviarlo a otra persona. Sin embargo, la inmediata disponibilidad de la cámara web, a un clic, puede hacer que sea usada en exceso y de forma imprudente. Como en los timos y en las estafas, metidos en situación, se hacen cosas que, meditadas, nunca se harían.

Es condición necesaria para la mayoría de los problemas relacionados con el *grooming* y la *sextorsión*. Aunque no hay datos oficiales, nos lo dicen las noticias. Los depredadores y chantajistas prefieren víctimas con cámara web. Habiendo tantos adolescentes donde elegir, el primer criterio de criba suele ser la existencia de este dispositivo. Facilita mucho las cosas.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

De hecho, en los primeros casos, hace muchos años, donde había acoso sexual y las cámaras digitales no eran tan comunes ni baratas, los depredadores enviaban a sus víctimas como regalo una cámara digital que facilitara la captura y envío de fotografías.



Recomendaciones para el uso sin riesgos de la webcam

Para todas aquellas personas que tengan una cámara web, recomendamos seguir estos cinco consejos básicos para un uso seguro de la webcam:

- Usarla únicamente con interlocutores de máxima confianza y no hacer delante de ella nada que no se haría en público.
- Tener presente siempre la información de contexto que la cámara puede estar transmitiendo.
- Mantener el equipo libre de software malicioso para evitar activaciones remotas.
- Girar la cámara hacia un ángulo muerto cuando no se esté usando porque de esa manera evitamos que, por un descuido o una activación remota, pueda emitir imágenes inadecuadas. Si viene integrada en el equipo es portátil, basta taparla con cinta adhesiva o similar.
- Si se pretende conocer la identidad del interlocutor y se intercambia con él la imagen de la webcam por unos instantes, se le debe pedir en esos momentos

que realice alguna acción particular (por ejemplo, simular unas gafas rodeando sus ojos con los dedos) que nos garantice que no está mostrando una grabación.

Las empresas han de valorar este dispositivo como lo que es: una cámara que captura información audiovisual propia y la envía al interlocutor. No puede ser considerado como un extra de hardware que siempre es bienvenido y sobre el que no hay que hacer ninguna consideración.

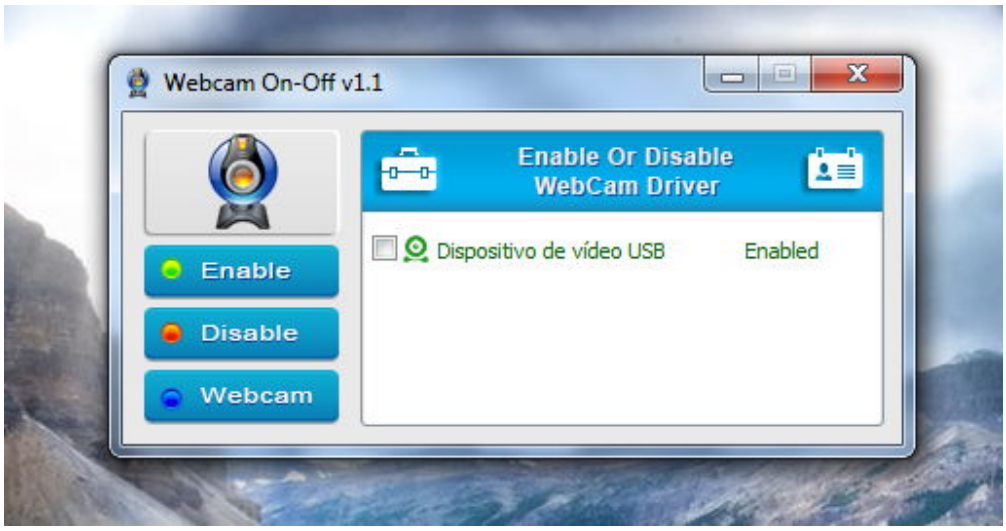
Antivirus y firewall, herramientas imprescindibles

La sofisticación de este tipo de ataques ha crecido exponencialmente, haciendo que sean cada vez más complejos y difíciles de detectar y de detener, por lo que es totalmente necesario contar con soluciones de seguridad actualizadas y realmente eficaces.

Dichas herramientas nos darán la seguridad de que podremos repeler sin problema este tipo de ataques y de que no quedaremos expuestos a ningún tipo de espionaje, garantizando nuestra tranquilidad y el buen funcionamiento de la empresa.

Mantener nuestros sistemas operativos y el software general que utilizamos actualizados es otra de las claves que nos ayudarán a reducir las vulnerabilidades que pueden aprovechar posibles atacantes para hacerse con el control de la webcam de nuestros equipos, así que es importante que los mismos estén, en conjunto, puestos al día.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL



No utilizo la webcam y no quiero correr el más mínimo riesgo

En el caso de que no vayamos a utilizar la webcam tenemos la opción de deshabilitarla, algo que en equipos Windows se puede hacer fácilmente desde el administrador de dispositivos y que, obviamente, podemos revertir en cualquier momento en apenas unos segundos.

Si nuestra webcam es externa y no está integrada basta con desenchufarla, aunque también tenemos otras opciones muy simples e igualmente eficaces, como por ejemplo tapar directamente la webcam.

Sentido común y formación, complemento imprescindible

El auge de las nuevas tecnologías en la empresa, el BYOD y las nuevas amenazas han chocado frontalmente como un tren de alta velocidad con el desconocimiento o falta de formación de ciertos grupos de empleados y profesionales.

Esto fue especialmente notable hace ya unos años, pero todavía se mantiene como un frente abierto en muchas empresas en las que buena parte de sus trabajadores enfrentan un desconocimiento importante en materia de seguridad informática básica.

Instruir a estos empleados, aunque sea a nivel básico, y darles los pilares para que trabajen teniendo unas nociones mínimas de seguridad en nuevas tecnologías también nos ayudará a evitar este tipo de ataques, ya que requieren de una infección previa, y será más difícil que ocurra si tenemos una cierta formación.

ESTAFAS TELEFONICAS

Los ciberdelincuentes establecen contacto telefónico con su víctima potencial, utilizando algunos de los siguientes métodos:

- Una llamada directamente en nuestro teléfono. Al contestarla, éstos se identifican, en inglés o español, como un servicio de soporte técnico. Nos

informan de que nuestros dispositivos están en riesgo y es necesario realizar acciones urgentemente.

- Nos aparece un error en el navegador web, un aparente aviso del sistema u otra ventana emergente, en el que se facilita un número de teléfono de ayuda para solucionar el problema.

Si informamos de que no tenemos ordenador en casa, no cesarán en su empeño e intentarán que sigamos sus órdenes a través del teléfono móvil o tablet.

A partir de este punto, nos proporcionan una serie de instrucciones. Normalmente, comienzan indicando una serie de datos técnicos con la intención de dar mayor peso a la llamada. El siguiente paso es crucial: con la excusa de que se trata de un error muy serio que requiere tomar medidas urgentemente, se solicita la instalación de un programa de acceso remoto.

Estas herramientas permiten el control de un ordenador o un móvil a distancia. Sin embargo, es necesario tener en cuenta que a través de estas herramientas se permite a un tercero el control sobre el dispositivo y acceso a toda nuestra información. Por este motivo, no debemos conceder acceso remoto a nadie salvo que estamos completamente seguros de que se trata de una persona conocida y de confianza.

¿Qué hacer si hemos seguido las indicaciones del supuesto servicio técnico?

En primer lugar, desconectaremos de la red el equipo afectado. Así aseguramos que se corta el acceso remoto y no pueden continuar manipulando nuestros equipos por parte de los estafadores.

Debemos desinstalar cualquier programa que hayamos instalado por indicación de los supuestos técnicos. En caso de duda, acceder al listado de programas de nuestro equipo y localizar los que se hayan instalado en la franja horaria en la que sufrimos este incidente.

Analizaremos el equipo afectado con una herramienta antivirus completa, para eliminar cualquier posible malware, y aplica todas las actualizaciones de seguridad que estén pendientes por instalar. Es importante mantener los equipos actualizados para evitar posibles infecciones.

Cambiaremos las contraseñas que estén almacenadas en el equipo (como por ejemplo accesos a correo electrónico, a cuentas bancarias, o inicios de sesión a perfiles o cuentas).

En caso de que se haya realizado algún pago, valoraremos la opción de cancelar la tarjeta con la que se ha realizado, si se tiene la sospecha de que puedan haber capturado estos datos. En cualquier caso, contactaremos directamente con el banco para solicitar la cancelación de la transacción.

Finalmente, reportaremos el fraude a las Fuerzas y Cuerpos de Seguridad del Estado.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

DISPOSITIVOS USB

Los dispositivos de almacenamiento extraíble (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.) permiten una transferencia rápida y directa de información. Hoy en día son imprescindibles y muy utilizados. Debemos aplicar las medidas de seguridad que este tipo de dispositivos requieren por su susceptibilidad al robo, manipulación, extravío e infección por virus.

La empresa debe decidir si se permite el uso de dispositivos de almacenamiento externo, y de ser así, debe disponer de una normativa que contemple en qué situaciones pueden utilizarse y qué tipo de información se permite guardar en ellos.

Si se necesita almacenar información sensible o confidencial se utilizarán dispositivos externos corporativos debidamente protegidos, se almacenarán en lugares seguros y se informará al responsable si ocurre algún incidente (robo, pérdida, infección del dispositivo, etc.).

En el caso de que se permita el uso de dispositivos personales (dispositivos extraíbles propiedad del empleado) se aplicarán las normas de seguridad recogidas en la política correspondiente.

Para asegurar la información contenida en los dispositivos extraíbles tendremos que aplicar medidas de seguridad como: **cifrar los datos almacenados, establecer permisos de acceso, cambiar periódicamente la contraseña**, etc.

Otro de los aspectos importantes a tener en cuenta es la eliminación de la información almacenada. Para asegurar que estos datos no volverán a ser accesibles, debemos utilizar los métodos de borrado seguro: destrucción física del dispositivo, desmagnetización o sobreescritura, según convenga en cada caso.

En definitiva, debemos aplicar las medidas de seguridad que este tipo de dispositivos requieren, así como concienciar a los empleados para su buen uso. De esta forma protegeremos tanto la información contenida en ellos como la de los dispositivos a los que se conectan.

Controles

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a almacenamiento en dispositivos extraíbles.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico**. El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- **Avanzado**. El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO)**: aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** aplica al personal técnico especializado.
- **Personas (PER):** aplica a todo el personal.

Puntos clave

Los puntos clave de esta política son:

- **Normativa de almacenamiento en dispositivos extraíbles**. Si no disponemos aún de ella tendremos que elaborar una normativa que regule el uso de dispositivos extraíbles que incluya:
  - llevar un registro de los dispositivos autorizados;
  - definir en qué condiciones o casos se permite su uso;
  - definir cómo se accede y si la información debe ir cifrada;,
  - establecer las configuraciones de seguridad necesarias para poder utilizarlos, etc.
- **Concienciación de los empleados**. El robo o extravío, la manipulación, y la infección por virus de los dispositivos extraíbles son las causas más frecuentes por las que puede perderse la información contenida en ellos. Por eso es importante involucrar a los usuarios en la protección, vigilancia y buen uso de estos dispositivos, concienciándolos de la trascendencia de la protección del mismo y de los datos que contiene.
- **Alternativas a los medios de almacenamiento extraíble**. Para evitar la necesidad del uso de estos soportes pueden implantarse las siguientes alternativas:
  - utilizar repositorios comunes para el intercambio de información

  - implantar la posibilidad de acceso remoto para poder trabajar desde fuera de la oficina
  - usar los servicios de almacenamiento en la nube autorizados por la organización
- **Registro de usuarios y dispositivos**. Tenemos que mantener un registro de dispositivos detallando los privilegios de acceso asignados a cada usuario que los necesite.
- **Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información**. Estas medidas podrán aplicarse tanto sobre el dispositivo extraíble como sobre los dispositivos a los que se conecta o sobre los documentos. Por ejemplo:
  - Sobre el dispositivo extraíble:
    - Programar cambios periódicos de contraseña de acceso al dispositivo.
  - Sobre los dispositivos a los que se conectan:
    - Implementar mecanismos de autenticación de usuarios.
    - Evitar que dispositivos no registrados puedan conectarse a cualquier equipo de la organización.
    - Desactivar la opción de autoarranque en los equipos para no permitir posibles ejecuciones automáticas no deseadas cuando los dispositivos extraíbles son enchufados.
    - Deshabilitar por defecto los puertos USB y habilitarlos para el personal que necesite dicha funcionalidad de manera periódica o gestione ficheros de gran tamaño.
  - Sobre los documentos que se transfieren:
    - Establecer control de accesos con permisos de lectura, escritura y ejecución.
    - Implementar mecanismos de cifrado de la documentación.

- Cumplimiento de la normativa. Tendremos que comunicar esta normativa y asegurarnos de que los empleados la conocen y se comprometen a cumplirla antes de utilizar dispositivos extraíbles en el entorno de trabajo.

SEGURIDAD FISICA

Los responsables de seguridad suelen centrar sus esfuerzos en bastionar el perímetro lógico, mediante cortafuegos, segmentación de red u otras técnicas a su alcance, pero esta labor de asegurar el perímetro tiene que ir de la mano con un plan de seguridad que incluya medidas de protección físicas, para obtener una defensa integral. De no ser así, siempre se dejaría un riesgo sin contemplar en nuestro plan de ciberseguridad.

La seguridad física de los dispositivos industriales, y de los datos asociados de estos equipamientos, debe ser tratada como una pieza más de la ciberseguridad industrial. El principal objetivo de la seguridad física es mantener a las personas alejadas de situaciones peligrosas, permitiéndolas seguir desarrollando su trabajo, teniendo en cuenta siempre, que estas medidas no impliquen un impedimento en situaciones de emergencia.

Pero otro de los objetivos principales es mantener un control preestablecido de las personas y las áreas a las que éstas pueden acceder.

Diferentes sistemas de seguridad física

Conseguir acceso físico a un centro de control, y más concretamente a dispositivos pertenecientes a la red de control, normalmente implica ganar acceso lógico a todo el sistema de procesos. Del mismo modo, conseguir acceso lógico a los sistemas de la sala de control permitirá probablemente ejercer cambios en las medidas de seguridad y autorizaciones de acceso físico.

Como se ha visto, la línea que separa la relación entre seguridad lógica y la seguridad física es difusa. Por esto, debe prestarse especial atención a las protecciones físicas de nuestros dispositivos lógicos, dentro de las infraestructuras industriales.

Normativa relativa a la seguridad física

Todas las normativas y guías de buenas prácticas de seguridad en ICS recogen, de alguna manera, los requerimientos de seguridad física. Las más representativas podrían ser:

- El estándar internacional IEC 62443-2-1 'Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program'. Punto 4.3.3.
- NERC CIP-005-5 'Cyber Security - Electronic Security Perimeter(s)'.
- NERC CIP-014-2 'Physical Security'.

Otra que no es específica del entorno industrial, pero que podría considerarse referente a la hora de implementar controles de seguridad tanto a nivel físico como especialmente al lógico es:

- ISO/IEC 27001:2013 'Information technology -- Security techniques -- Information security management systems – Requirements'. Puntos A.11.1, A.11.2, A.11.4.

Por otra parte, la guía de buenas prácticas del NIST 800-82 'Guide to Industrial Control Systems (ICS) Security', recoge de manera muy acertada los atributos que deben considerarse a la hora de realizar una defensa en profundidad aplicada a la seguridad física, que resumimos a continuación:

- **Protección de las ubicaciones físicas:** Se refiere a las consideraciones clásicas de seguridad física, estableciendo perímetros de seguridad segmentados, con medidas de seguridad específicos aplicados por capas.
- **Control de acceso:** Controles de seguridad que deben garantizar que solo las personas autorizadas tengan acceso a los espacios controlados. Un sistema debe

poder verificar que las personas a las que se les concede acceso, son quienes dicen que son (habitualmente usando algo que la persona tiene, como una tarjeta o clave de acceso; algo que conocen, como un número de identificación personal (PIN); o algo que demuestre quien son, un lector biométrico).

- **Sistemas de monitorización de accesos**: Se incluyen aquí cámaras fijas y de video, sensores o sistemas de identificación. Estos sistemas no previenen un acceso no autorizado, sino que los almacenan y registran.
- **Sistemas de limitación de acceso**: Dentro de este atributo entrarían vallas, cerraduras, o personal de seguridad, por ejemplo.
- **Sistemas que permitan el seguimiento de personas o activos**: Tecnologías que permitan rastrear los movimientos de personas o vehículos para asegurar que permanecen en las áreas autorizadas.
- **Sistemas de gestión de factores ambientales**: Entornos limpios, libres de electricidad estática, vibraciones, campos magnéticos, etc.
- **Sistemas de control de condiciones ambientales**: Sistemas denominados en inglés (HVAC), control de humedad, ventilación y aire acondicionado.
- **Sistemas de protección de corriente**: Sistemas de protección y alimentación ininterrumpida, conocidos como UPS por sus siglas en inglés.
- **Sistemas de protección adicionales para centro de control**: Adicionalmente a los anteriores, las salas de control pueden tener necesidades más específicas de seguridad física como pueden ser: centros de control a prueba de explosiones, o incluso tener redundando el espacio físico del centro de control fuera de las instalaciones, para poder seguir controlándola si fuera necesario.
- **Sistemas de control de los dispositivos de configuración portables**: Sistemas que impidan la movilidad de ciertos equipos de configuración de PLC, puestos de operador, considerados críticos.
- **Sistemas de protección de cableado**: Este atributo es muy importante ya que el diseño e implementación del cableado para la red de control debe abordarse en el plan de ciberseguridad. El cable de comunicaciones de par trenzado sin

blindaje, aunque aceptable para el entorno de IT, generalmente no es recomendable para el entorno OT, debido a su susceptibilidad a la interferencia de campos magnéticos, ondas de radio, etc. Se recomienda el uso de conectores industriales RJ-45, pues proporcionan protección contra la humedad, el polvo y la vibración. El cable de fibra óptica y el cable coaxial son mejores opciones, porque son inmunes a las interferencias eléctricas y de frecuencia de radio que se encuentran típicamente en un entorno de control industrial. El cable y los conectores deben estar codificados por colores y etiquetados para que las redes ICS e IT estén claramente delineadas y se reduzca la posibilidad de una conexión cruzada inadvertida.

Interacción entre la seguridad física y la seguridad lógica

Todas las normativas y guías de buenas prácticas nombradas disponen de requerimientos de seguridad física bastante claros, en los que se engloban todos o la mayoría de los descritos. Pero la implementación de éstos y, sobre todo, cómo gestionarlos dentro de la red de la propia infraestructura, no se encuentra definido.

Todos los beneficios que puede aportar la seguridad física pueden verse diluidos por una mala implementación o una incorrecta gestión dentro de la red, o incluso peor, suponer un riesgo adicional por una mala praxis.

Es clave no olvidar que, toda la monitorización de las diferentes medidas de seguridad física (cámaras IP, controles de acceso, etc.) y el procesamiento de alertas y logs generados por estos sistemas físicos, entran a formar parte de nuestra infraestructura industrial.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

SEGURIDAD INALAMBRICA

Como nuevos integrantes de la red, estos dispositivos deben ser tratados dentro del plan general de ciberseguridad, realizar un correcto análisis de riesgos, diseñar una arquitectura segura que los englobe, así como segmentar de manera correcta estos sistemas, pensando en una defensa en profundidad.

El tráfico generado por estos nuevos dispositivos es bastante predecible y limitado, por lo que gestionarlo mediante elementos de red o reglas dentro de los cortafuegos focalizados, elevaría el nivel de seguridad de manera fácil. A continuación, se indica alguna recomendación a muy alto nivel:

- Todos estos dispositivos deberían tener su propio dominio de colisión, por ejemplo, dentro de una VLAN dedicada. Los usuarios o grupos con permisos de gestión, configuración y acceso a estos dispositivos físicos, es muy reducido, por lo que es recomendable disponer de reglas específicas dentro de los cortafuegos con un nivel de detalle casi de IP-Puerto-Usuario.
- El sistema de recolección de alertas y logs, o el envío de señales en caso de cámaras IP, tienen un solo sentido, si hablamos a nivel de red, por lo que limitar dentro de los cortafuegos el tráfico como solo saliente y no permitir el tráfico entrante, puede evitar propagaciones no deseadas.

- Minimizar la superficie de ataque mediante reglas específicas a nivel de aplicación y protocolo, permitirá reducir el nivel de amenaza que, adicionalmente, puedan haber introducido estos nuevos dispositivos en la red industrial.

Considerar las medidas y sistemas de seguridad físicos, como parte del plan de ciberseguridad, es una práctica que tiene que ser tomada muy en serio. Tener en cuenta, desde el inicio del diseño de una nueva infraestructura, todos los elementos que van a formar parte, de una manera u otra, en la red industrial, es crítico.

Realizar un análisis de riesgos de estos dispositivos, conocer cómo puede afectar a la red si alguno de ellos es comprometido, mediante pruebas test de intrusión, son tareas que debe realizar el equipo de ciberseguridad. Al fin y al cabo, la seguridad física es el pilar de la seguridad lógica.

Las redes inalámbricas nos permiten utilizar el ordenador virtualmente desde cualquier lugar, además de conectarte con otros ordenadores de la red o acceder a Internet.

No obstante, si la red inalámbrica no es segura, existen riesgos muy importantes. Por ejemplo, un hacker podría:

- Interceptar los datos que envíes o recibas
- Acceder a tus archivos compartidos

Para ello es necesario dotar de cierta seguridad a la red inalámbrica tanto de casa como de la oficina. Pero antes vamos a ver cuáles son los protocolos de seguridad en este tipo de redes.

Hay varios tipos de seguridad inalámbrica con los que te encontrarás: aquí tienes un breve resumen de los detalles.

Privacidad de equivalencia por cable (WEP)

Las siglas se corresponden con Wired Equivalent Privacy. Desarrollado a finales de la década de 1990 como el primer algoritmo de cifrado para el estándar 802.11.

WEP se diseñó con un objetivo principal en mente: evitar que los hackers fisgoneen en los datos inalámbricos a medida que se transmiten entre clientes y puntos de acceso (AP). Sin embargo, desde el principio, WEP carecía de la fuerza necesaria para lograrlo.

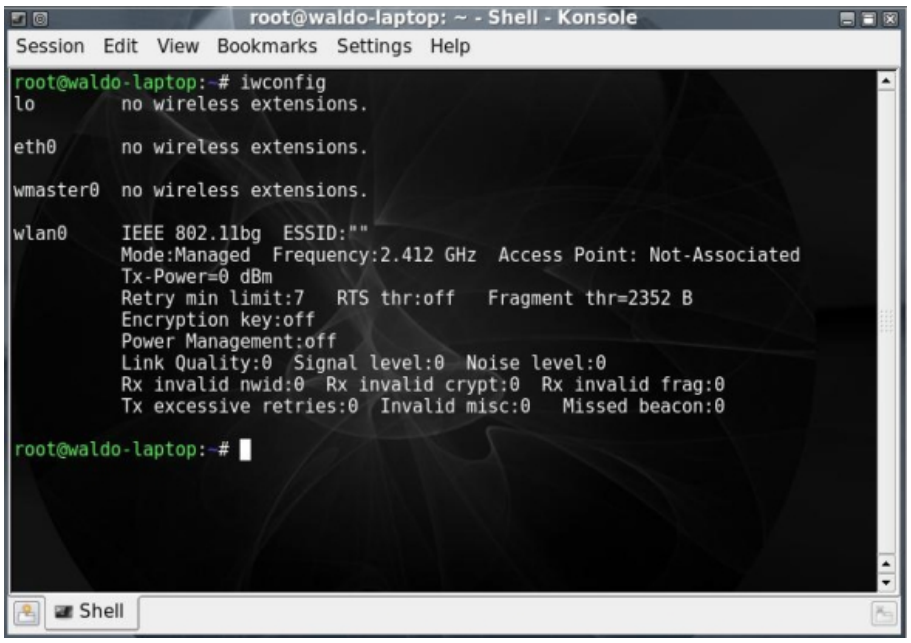
Los expertos en ciberseguridad identificaron varios defectos graves en 2011, lo que finalmente dio lugar a recomendaciones a nivel de toda la industria para eliminar gradualmente su uso tanto en los dispositivos empresariales como en los de consumo.

El Ciber ataque WEP

Después de que un ataque cibernético a gran escala ejecutado contra T.J. Maxx en 2009 fuera rastreado hasta las vulnerabilidades expuestas por WEP, el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago prohibió a los minoristas y otras entidades que procesaban datos de tarjetas de crédito el uso de WEP.

WEP utiliza el cifrado de flujo RC4 para la autenticación y el cifrado. El estándar originalmente especificaba una clave de encriptación pre-compartida de 40 bits.

Se mejoró con una clave de 104 bits después de que se levantara una serie de restricciones del gobierno de los Estados Unidos. La clave debía ser introducida manualmente y actualizada por un administrador.



Esta clave se combina con un vector de inicialización de 24 bits en un esfuerzo por reforzar el cifrado. Sin embargo, esto aumenta la probabilidad de que las claves sean reutilizadas, lo que, a su vez, las hace más fáciles de romper.

Esta característica, junto con otras vulnerabilidades, incluyendo mecanismos de autenticación problemáticos, hacen de WEP una opción arriesgada para la seguridad inalámbrica.

Acceso Protegido Wi-Fi (WPA)

Los numerosos fallos de WEP revelaron la urgente necesidad de una alternativa, pero los procesos deliberadamente lentos y cuidadosos que se necesitaban para escribir una nueva especificación de seguridad plantearon un conflicto.

En respuesta, en 2003, la Wi-Fi Alliance lanzó WPA como un estándar provisional, mientras que el Institute of Electrical and Electronics Engineers (IEEE) trabajó para desarrollar un reemplazo más avanzado y a largo plazo para WEP.

WPA tiene dos modos: para usuarios empresariales y para uso personal. El protocolo empresarial, WPA-EAP, utiliza una autenticación 802.1x más estricta con el Protocolo de autenticación extensible (Extensible Authentication Protocol, o EAP).

El protocolo de seguridad wireless personal, WPA-PSK, utiliza claves pre-compartidas para una implantación y una gestión más sencilla para los consumidores y las pequeñas oficinas. El modo Enterprise requiere el uso de un servidor de autenticación (Radius).

Aunque WPA también se basa en el cifrado RC4, introdujo varias mejoras al cifrado, como por ejemplo, el uso del Protocolo de Integridad de Clave Temporal (TKIP).

Las Mejoras del Protocolo WPA

El protocolo contiene un conjunto de funciones para mejorar la seguridad de la LAN inalámbrica:

- El uso de claves de 256 bits
- La mezcla de claves por paquete
- Generación de una clave única para cada paquete
- Transmisión automática de claves actualizadas
- La comprobación de la integridad de los mensajes
- Un tamaño cuatro veces mayor (48 bits)
- Mecanismos para reducir la reutilización de claves

WPA fue diseñado para ser compatible con WEP para fomentar una adopción rápida y fácil.

Los profesionales de la seguridad de red pudieron soportar el nuevo estándar en muchos dispositivos basados en WEP con una simple actualización del firmware.

Sin embargo, este marco también significaba que la seguridad que proporcionaba no era tan sólida como podría serlo.

Acceso protegido Wi-Fi 2 (WPA2)

Como sucesor de WPA, el estándar WPA2 fue ratificado por el IEEE en 2004 como 802.11i. Al igual que su predecesor, WPA2 también ofrece modos empresariales y personales.

Aunque WPA2 todavía tiene vulnerabilidades, se considera el estándar de seguridad inalámbrica más seguro disponible actualmente.

WPA2 reemplaza el cifrado RC4 y TKIP con dos mecanismos de cifrado y autenticación más potentes: el Advanced Encryption Standard (AES) y el Counter Mode con Cipher Block Chaining Message Authentication Code Protocol (CCMP), respectivamente.

WPA2 también está diseñado para ser compatible con versiones anteriores y admite TKIP como solución alternativa en caso de que un dispositivo no sea compatible con CCMP.

AES fue desarrollada por el gobierno de los EEUU para la protección de datos clasificados, y se compone de tres cifras de bloque simétricas.

Cada uno cifra y descifra datos en bloques de 128 bits utilizando claves de 128, 192 y 256 bits.

Aunque el uso de AES requiere más potencia de computación por parte de los APs y clientes, las mejoras continuas en el hardware de los ordenadores y de la red han mitigado los problemas de rendimiento.

Protocolo CCMP

El Protocolo de código de autenticación de mensaje de encadenamiento de bloque de cifrado de modo contador, o CCMP protege la confidencialidad de los datos al permitir que sólo los usuarios autorizados de la red reciban los datos, y utiliza un código de autenticación de mensajes encadenado por bloques de cifrado para garantizar la integridad de los mensajes.

WPA2 también introdujo una itinerancia más fluida, permitiendo a los clientes pasar de un AP a otro en la misma red sin tener que volver a autenticarse, mediante el uso de la caché de claves maestras de Pairwise o la preautenticación.

Seguridad Wireless bajo el protocolo WPS

En 2007, comenzó a aparecer un nuevo método de seguridad: la configuración protegida WiFi (WPS) en los puntos de acceso inalámbricos.

Con este tipo de seguridad, un usuario puede añadir nuevos dispositivos a su red simplemente pulsando un botón (dentro del software de administración o físicamente en el router) e introduciendo un número PIN de 8 dígitos en el dispositivo cliente.

La función PIN actúa como una especie de atajo para introducir una clave WPA (WiFi Protected Access) más larga.

La primera idea detrás de WPS era que necesitábamos tener acceso físico al AP para presionar un botón y leer una pegatina. Esto proporcionaría una implementación más segura de la autenticación WiFi.

Así es como funciona:

1. El octavo y último dígito del número PIN es una suma de comprobación, que se utiliza para asegurarse de que los 7 dígitos que importan no se corrompan.
2. De estos 7 dígitos, podemos ver que hay 10.000.000 de posibilidades (ya que cada uno de los 7 dígitos puede ser 0-9, con repeticiones permitidas). Esto es todavía una cantidad bastante enorme de posibilidades, y solo se podría considerar bastante seguro – pero hay un defecto en el proceso de comprobación.

3. Cuando un PIN está siendo examinado por el AP, los primeros 4 dígitos (10.000 posibilidades) se comprueban por separado de los últimos 3 dígitos (1.000 posibilidades).

Esto se traduce en un usuario malicioso que sólo necesita hacer un máximo de 11.000 combinaciones, algo que un ordenador puede realizar en cuestión de horas.

Como vemos, si estamos utilizando actualmente WPS en un punto de acceso, debemos desactivar la función lo antes posible.

Recomendación de Seguridad Wireless

Si el punto de acceso que usamos sólo puede utilizar WEP, es hora de que se plantee la posibilidad de actualizar su tecnología para aumentar tu sistema y seguridad, por no hablar del aumento de la velocidad de transferencia en los dispositivos más nuevos.

Ahora mismo, la mejor seguridad para su red WiFi es WPA2 con WPS desactivado. El uso de esta combinación de seguridad proporciona la red WiFi más segura posible hoy en día.

Además, ¿realmente quiere confiar en un solo botón para proporcionar toda la seguridad de su red?.

Auditoria Seguridad Inalámbrica

Una auditoría de redes de seguridad es una evaluación sistemática de la seguridad del sistema de información de una empresa mediante la medición de su conformidad con un conjunto de criterios establecidos.

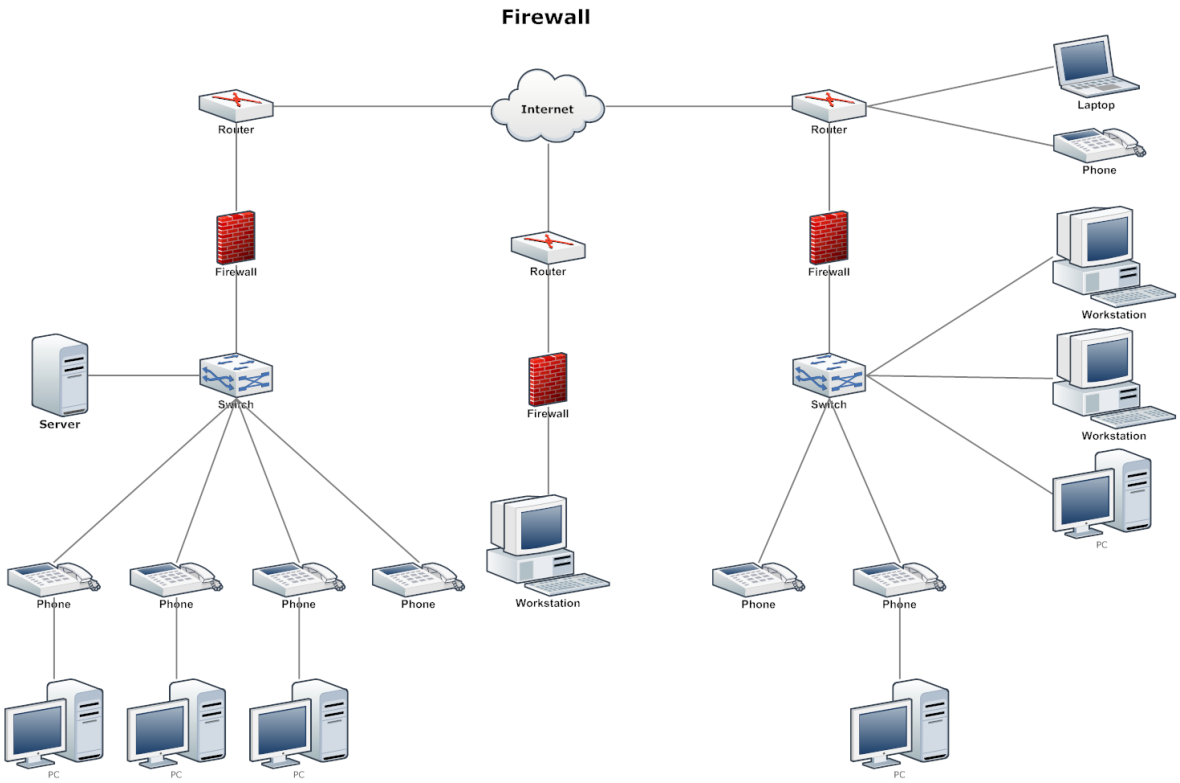
Una seguridad de red completa normalmente evalúa la protección de la configuración física y el entorno del sistema, el software, los procesos de manejo de la información y las prácticas de los usuarios.

Las auditorías de seguridad redes wifi se utilizan a menudo para determinar el cumplimiento de la normativa, a raíz de la legislación específica de cada país, generalmente bajo la Ley de Información sobre Violaciones de la Seguridad, que especifica cómo deben tratar las organizaciones la información.

3. ALMACENAMIENTO EN LA RED.

En primer lugar, tendremos que definir en que consiste una red corporativa. Para empezar, no existe un tamaño determinado, puede abarcar desde 2 ordenadores a miles, dependiendo del tamaño de la empresa. Asimismo, geográficamente puede estar localizada en una ciudad, en todo un país, en un continente o en todo el planeta.

Una red corporativa consiste en un conjunto de ordenadores, dispositivos, terminales y bases de datos conectadas por líneas de comunicación. En otras palabras, las redes de ordenadores se usan para conectar ordenadores a otros ordenadores o dispositivos como impresoras, equipos multifunción o servidores de almacenamiento.



Como hemos comentado antes, las redes se pueden diseñar para conectar equipos en una misma oficina, o en oficinas repartidas por todo el mundo. Las redes de área local (*LAN*) son las que se usan para conectar dispositivos que estén en una misma

localización. Las redes de área amplia (*WAN*) son las que se usan para interconectar las redes de área local (*LAN*). Un ejemplo de red *WAN* podría ser Internet.

Los dispositivos de una red se pueden conectar entre ellos a través de un cable *UTP* (par trenzado) o inalámbricamente por Wifi. La tecnología que se usa para estas conexiones se llama Ethernet.

Historia de las redes locales

1973: Nacimiento de Ethernet

El Doctor Robert M. Metcalfe inventó Ethernet en 1973. Su trabajo consistió en interconectar todos los equipos de un edificio y que pudieran usar la primera impresora laser del mundo, una Xerox. En sus anotaciones usó el nombre Ethernet porque el cable coaxial que usaba para conectar entre si a los ordenadores le recordaba a las teorías físicas relativas al Éter.

La idea de Metcalfe fue usada por ARPANET — la internet original desarrollada por el Departamento de Defensa de los Estados Unidos — y la ALOHAnet, que era una red de radio inalámbrica de conmutación de paquetes para ordenadores desarrollada por la Universidad de Hawái.

Ethernet permitía a los ordenadores enviar paquetes de datos a través de un cable coaxial para comunicarse entre sí y con la impresora. Empleó un esquema de detección de colisiones. Si los nodos de la red se activaran al mismo tiempo, causando una colisión, el servidor no respondería y los nodos esperarían un número aleatorio de milisegundos para volver a activarse.

1977: Primera LAN comercial

Cuatro años más tarde, Datapoint Corp. instaló la primera LAN comercial en el Chase Manhattan Bank en Nueva York. A diferencia de Ethernet de Metcalfe, la LAN de Datapoint utilizaba la red de computadora de recursos conectada (ARC). Mientras que Ethernet empleaba la detección de colisiones, ARC empleaba un esquema de paso de testigos para evitar transmisiones simultáneas por nodos.

En otras palabras, los nodos se turnaban para transmitir señales en lugar de depender de la retransmisión aleatoria. Otras compañías, como IBM, adoptaron el esquema de paso de testigos para luchar contra Ethernet por la supremacía de LAN a lo largo de los años 80.

1979: Ethernet disponible al público

Metcalfe creó la compañía 3Com para desarrollar y vender productos Ethernet.

1985: IEEE se convierte en el estándar para LAN

Ethernet se convirtió en el estándar del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) para LAN.

1990: Ethernet gana sobre LAN

Ethernet había ganado la batalla de la LAN, en parte cambiando a un cable de par trenzado (el que usamos actualmente), lo que reduce la diafonía y la inducción electromagnética. En otras palabras, Ethernet era más rápido.

1991: Comienza el trabajo en la LAN inalámbrica

El IEEE comenzó a trabajar en la LAN inalámbrica (WLAN), que se basa en el prototipo ALOHAnet.

1997: Nace el Wi-Fi

IEEE lanzó el estándar 802.11 (Wi-Fi).

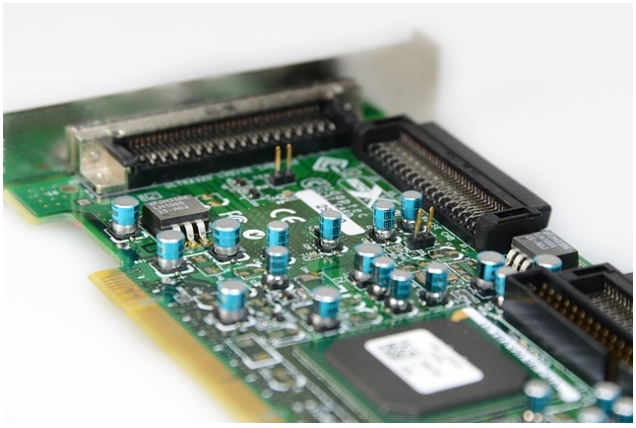
En lugar de la detección de colisiones, Wi-Fi emplea un esquema de acceso múltiple/prevención de colisiones (CSMA/CA) de detección de portadora de espera y ver. Un dispositivo Wi-Fi escucha las ondas de radio emitidas por la LAN durante un período de tiempo aleatorio, y cuando la red está inactiva, el dispositivo transmite una señal (fotograma).

Cuando el receptor consigue la trama intacta, envía detrás un acuse de recibo (ACK) al remitente. Las LAN inalámbricas (WLAN) y las LAN pueden acceder a Internet o a las redes de área extensa (WAN) a través de una puerta de enlace (router).

Componentes necesarios para una conexión LAN

Para construir una LAN o WLAN, los componentes necesarios serían los siguientes:

- *Ordenadores con tarjetas de interfaz de red*:



La mayoría de los PC, portátiles y tablets modernas vienen con una tarjeta de interfaz de red (NIC) para Ethernet y otra para Wi-Fi. Esto permite que la máquina se conecte a una red.

La NIC debe venir con software de controlador que el sistema operativo configura y actualiza automáticamente.

- *Cables*:

Los cables de par trenzado sin blindar (UTP) son el estándar (cables CatX, donde X es un número que indica la velocidad que obtendrá un cable).

En el caso que estemos buscando velocidades increíblemente rápidas, los cables de fibra óptica son la mejor opción aunque son mucho mas caras.

- *Conmutadores y concentradores*:

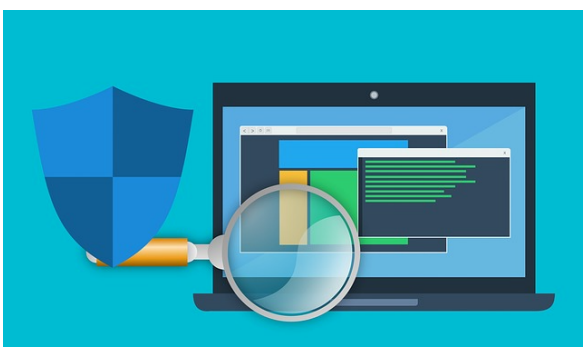
Un concentrador divide y comparte la transmisión de paquetes de datos con todos los equipos de una LAN, mientras que los conmutadores dedican la transmisión de paquetes a un único equipo, lo que reduce el tráfico de red.

- *Enrutadores*:

Los enrutadores de red le permiten conectarse a otras LAN (si es necesario) y asignan direcciones IP a sus dispositivos. Un router inalámbrico permitirá que las computadoras con NIC Wi-Fi se conecten entre sí y con Internet.

Si va a conectar una LAN a otras LAN y a Internet para formar una WAN, un enrutador (router) facilita la conversión y reversión de la señal.

- *Software*: El software de red debe venir con el sistema operativo de su elección, pero también deberá usar un software de seguridad antivirus, ya que su equipo estará mas expuesto.



- *Servidor de protocolo de configuración dinámica de host (DHCP)*:

Necesitará un equipo con mucha ram y espacio en el disco duro para actuar como su servidor DHCP.
Aunque puede estar integrado en el router en redes pequeñas.

En resumen, la configuración de una LAN, WLAN o WAN puede ser muy compleja dependiendo del tamaño de la organización.

Una vez que tenemos claro el concepto de red corporativa y los distintos componentes ya podemos comenzar con el almacenamiento.

¿Qué es el almacenamiento de datos?

El almacenamiento de datos significa esencialmente que los archivos y documentos se graban digitalmente y se guardan en un sistema de almacenamiento para su uso futuro.

Los sistemas de almacenamiento pueden depender de medios electromagnéticos, ópticos u otros medios para preservar y restaurar los datos si es necesario. El almacenamiento de datos facilita la copia de seguridad de los archivos para su custodia y recuperación rápida en caso de un bloqueo informático inesperado o un ciberataque.

El almacenamiento de datos puede ocurrir en discos duros físicos, unidades de disco, unidades USB o virtualmente en la nube. Lo importante es que sus archivos están respaldados y fácilmente disponibles en caso de que sus sistemas alguna vez se bloqueen más allá de la reparación.

Algunos de los factores más importantes a considerar en términos de almacenamiento de datos son la confiabilidad, la solidez de las características de seguridad y el costo de implementar y mantener la infraestructura. El llegar a conocer las diferentes soluciones y aplicaciones de almacenamiento de datos puede ayudarle a llegar a la elección que mejor se adapte a las necesidades de su negocio.

Tipos de almacenamiento de datos

Existen dos tipos amplios de almacenamiento de datos: el *almacenamiento con conexión directa* y el *almacenamiento conectado en red*.

Hay muchos dispositivos que encajan en cada una de estas categorías, cada uno con sus propias ventajas y desventajas únicas, que explicaremos con más detalle a continuación.

Almacenamiento de información con conexión directa (DAS).

Como su nombre indica, el almacenamiento con conexión directa (DAS) incluye tipos de almacenamiento de datos que están conectados físicamente al equipo.

Este almacenamiento es generalmente accesible a una sola máquina. Algunos dispositivos comunes en esta categoría incluyen:

- Unidades de disco duro
- Unidades de estado sólido (SSD)
- Unidades flash USB

Las soluciones DAS son excelentes para crear copias de seguridad locales y pueden ser más asequibles que las soluciones NAS, pero compartir datos entre máquinas puede ser engorroso.

Almacenamiento de información conectado en red (NAS).

El almacenamiento conectado en red (NAS) permite que varias máquinas compartan el almacenamiento a través de una red. Esto se logra con varias unidades de disco duro u otros dispositivos de almacenamiento en una configuración RAID.

Uno de los beneficios clave de NAS es la capacidad de centralizar los datos y mejorar la colaboración. Los datos se pueden compartir fácilmente entre máquinas conectadas y los niveles de permisos se pueden establecer para controlar el acceso.

Si bien las soluciones NAS tienden a ser más costosas que las soluciones DAS, siguen siendo muy asequibles, ya que la tecnología de almacenamiento de información ha avanzado significativamente.

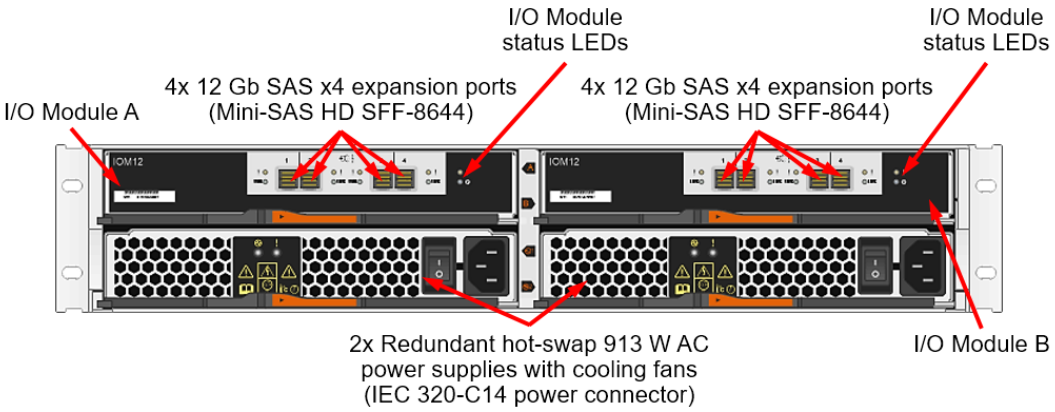
Tipos de dispositivos de almacenamiento de datos

Existe una variedad tremenda de dispositivos de almacenamiento de datos que proporcionan una protección confiable de archivos importantes, pero existen algunas diferencias que pueden ayudarnos a la hora de elegir la mejor opción para su negocio.

La memoria del equipo y el almacenamiento local pueden no ser suficientes para mantener sus datos protegidos. La mejor manera de protegerse es el almacenamiento de datos persistentes, que no requiere energía continua para almacenar y preservar los datos. Tenga en cuenta estas opciones de almacenamiento de datos persistentes:

- *Cabina de unidades flash SSD*. Utilizando solo memoria flash, estos sistemas de almacenamiento de estado sólido ofrecen una rápida transferencia de datos entre SSD y un tamaño físico más pequeño que una cabina de discos. El costo inicial tiende a ser más alto, pero cada vez el precio es menor en este tipo de discos.

- *Cabinas Flash híbridas*. Estos dispositivos de almacenamiento incluyen unidades de memoria flash y unidades de disco duro para un rendimiento equilibrado. Las cabinas flash híbridas ofrecen una menor inversión, costos de rendimiento razonables y acceso rápido a los datos bajo demanda. Las cabinas All-flash (solo almacenamiento flash) ofrecen una latencia más baja y un rendimiento más rápido que el flash híbrido, pero pueden costar mucho más.



- *Almacenamiento en la nube híbrida*. El almacenamiento en la nube híbrida, flexible y económico, ofrece una opción segura y compatible que ayuda a garantizar la continuidad del negocio. Este tipo de almacenamiento de datos se adapta a copias de seguridad frecuentes y archivos a largo plazo, así como a escalado futuro y disponibilidad siempre continua. La combinación de

almacenamiento en la nube y local agrega una capa de seguridad para garantizar que los datos estén protegidos y disponibles, y el espacio de almacenamiento podría ser potencialmente ilimitado.

Software de Backup

El software para copias de seguridad de sistemas y empresas normalmente viene con una licencia o una tarifa de suscripción facturada mensual o anualmente.

El principal problema que nos encontramos es que muchas veces lo instalamos y no nos preocupamos de revisar si se están haciendo bien las copias. Lo recomendable es que se revise periódicamente e incluso se haga alguna prueba de restauración para ver que está todo correcto.

Dispositivos de backup

Los servidores de copia de seguridad, los dispositivos de copia de seguridad y recuperación y otros dispositivos para este propósito tienen un precio considerable. Las configuraciones pueden ser complicadas y la integridad puede estar en riesgo con configuraciones incorrectas y ajustes de software incorrectos.

Almacenamiento en la nube

Las soluciones completas de almacenamiento en línea o basadas en la nube ofrecen almacenamiento de datos virtuales y un acceso a sus datos desde cualquier lugar, no solo desde un ordenador local o un disco duro externo. Este sistema es seguramente el más recomendable, pero las organizaciones deben considerar una estrategia de seguridad de almacenamiento en la nube antes de implementarlo.

Para obtener los mejores resultados en la protección de sus datos, debe esforzarse por mantener tres copias de sus archivos importantes. Almacene sus datos y añada dos copias de seguridad, preferiblemente una copia en remoto y otra en una localización distinta de su lugar de trabajo.

Beneficios del almacenamiento eficiente de datos

Como empresario, puede preguntarse: "¿Qué va a hacer el almacenamiento de datos para proteger y preservar la información de mi empresa?"

Es posible que desee saber cuánto dinero puede ahorrar una solución de almacenamiento de datos a su negocio, o cómo de rápido puede hacer que su empresa vuelva a funcionar después de un fallo o un ciberataque con la solución de almacenamiento y recuperación de datos correcta.

Tenga en cuenta estos beneficios del almacenamiento de datos para determinar cuál es el impacto que puede tener en su negocio.

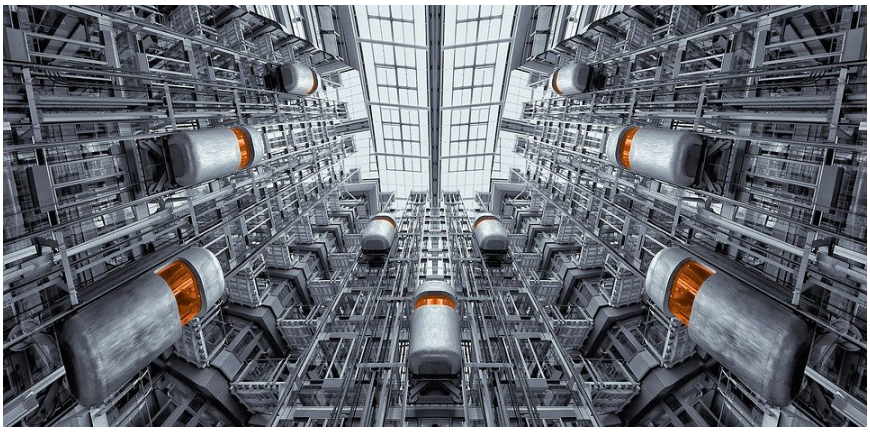
- Preservación confiable de datos
- Continuidad y accesibilidad de los datos
- Recuperación de datos más rápida y fácil
- Precios flexibles y opciones de capacidad
- Seguridad eficaz para los archivos protegidos

El futuro del almacenamiento de datos

Las soluciones de almacenamiento de datos destacadas anteriormente representan la gama actual de soluciones, pero el mundo del almacenamiento de datos está en continua evolución.

Las últimas innovaciones en almacenamiento en red pueden proporcionar soluciones integrales y con visión de futuro para las empresas que necesitan almacenar un gran volumen de información confidencial.

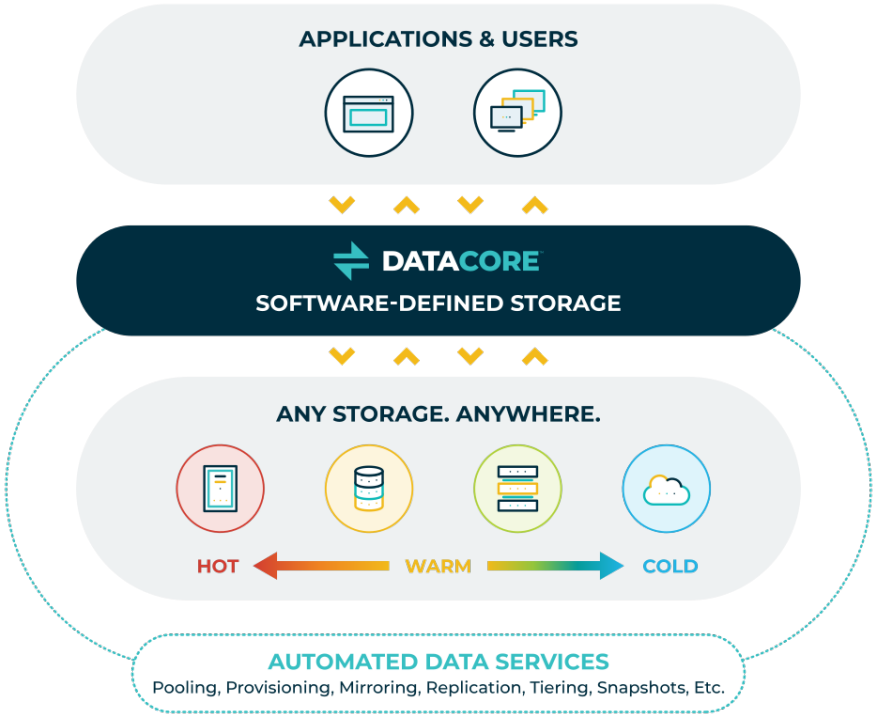
Si su empresa tiene necesidades de almacenamiento de datos más complejas, es posible que desee considerar una de estas opciones de almacenamiento más avanzadas. Echemos un vistazo a dos de estas tecnologías emergentes de almacenamiento de datos.



- *Almacenamiento definido por software*. El almacenamiento de datos tradicional requiere hardware y software para ejecutarlo. Cuando necesite ampliar su almacenamiento, tendrá que ampliar como consecuencia el hardware.

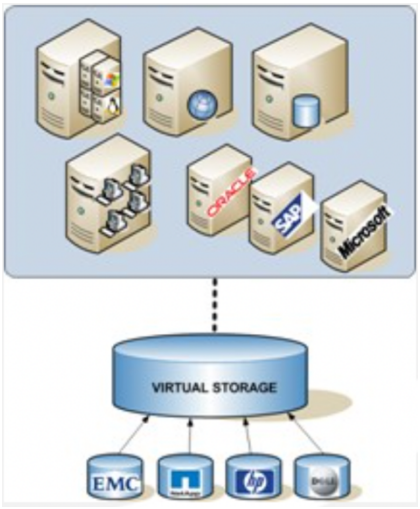
  Por el contrario, el almacenamiento definido por software (SDS), desacopla la capa de software entre el lugar donde se almacenan físicamente los datos y cómo se recuperan. Separar el software de almacenamiento de su hardware, le

permite ampliar su capacidad de almacenamiento en cualquier servidor estándar de la industria o sistema, para que no tenga que seguir comprando hardware cada vez que necesite más almacenamiento y no tenga que usar dispositivos de almacenamiento del mismo proveedor. Al abstraer la capa de software, puede colocar sus datos dondequiera que los necesite, con la flexibilidad de aumentar la capacidad como mejor le parezca, o incluso reducirla en el caso de que sea necesario.



SDS ofrece beneficios adicionales, como administración automatizada, rentabilidad y la capacidad de unir muchas fuentes de datos diferentes para construir una infraestructura de almacenamiento de información común.

- *Virtualización del almacenamiento de información*. La virtualización del almacenamiento de la información se refiere a la capacidad de almacenamiento que se acumula desde varios dispositivos físicos y luego se hace disponible para su reasignación en un entorno virtualizado.



Es la agrupación de almacenamiento físico desde múltiples dispositivos en lo que parece ser un solo dispositivo de almacenamiento administrado desde una consola central.

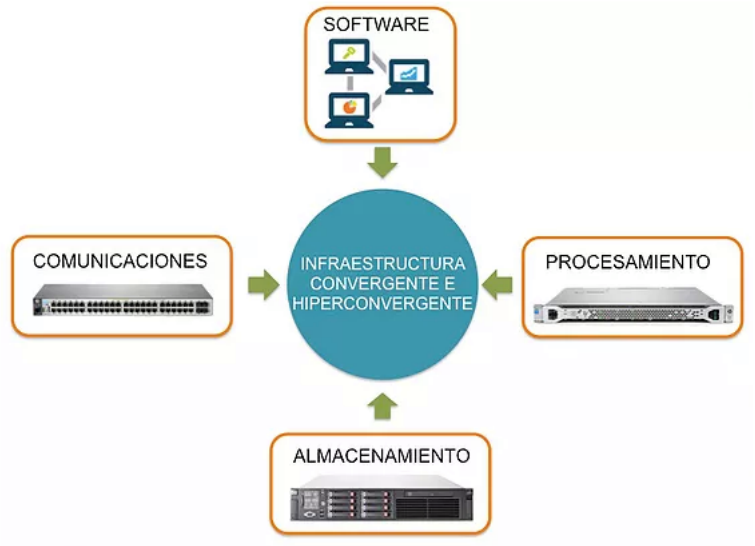
Al depender del software para identificar la capacidad de almacenamiento disponible, la tecnología agrega esa capacidad como un grupo de almacenamiento que las máquinas virtuales pueden usar en un entorno virtual.

A diferencia de SDS, que separa la capa de software del hardware para crear una infraestructura de almacenamiento, la virtualización del almacenamiento simplemente agrupa los recursos de almacenamiento para que aparezca a los usuarios como una sola lectura o escritura estándar en una unidad física.

Oculta la complejidad del sistema de almacenamiento, lo que permite a los usuarios y administradores realizar tareas como backup, archiving y recuperación de una manera más fácil y lenta. La virtualización también puede ayudarle a aumentar la capacidad sin necesidad de comprar nuevos dispositivos de almacenamiento.

Almacenamiento hiperconvergente.

El almacenamiento hiperconvergente (HCS) es el siguiente paso después de la virtualización del almacenamiento y SDS.



HCS utiliza la nube para combinar las funciones de computación, virtualización y almacenamiento como una unidad física que se puede administrar como un solo sistema.

Se trata de un tipo de almacenamiento definido por software porque cada nodo tiene una capa de software que ejecuta software de virtualización idéntica a todos los demás nodos del clúster.

Este software virtualiza los recursos en el nodo individual y los comparte con los otros nodos, lo que permite que el almacenamiento y otros recursos se utilicen como un único almacenamiento o grupo de computación.

Beneficios de HCS:

- *Virtualización*. Este aspecto de virtualización es una ventaja del almacenamiento hiperconvergente, ya que permite utilizar hardware comercial listo para usar para componer los nodos individuales. Esto significa que un dispositivo hiperconvergido puede ser más barato de construir si lo hace usted mismo o

puede resultar en un costo mensual o anual menos costoso si utiliza un proveedor.

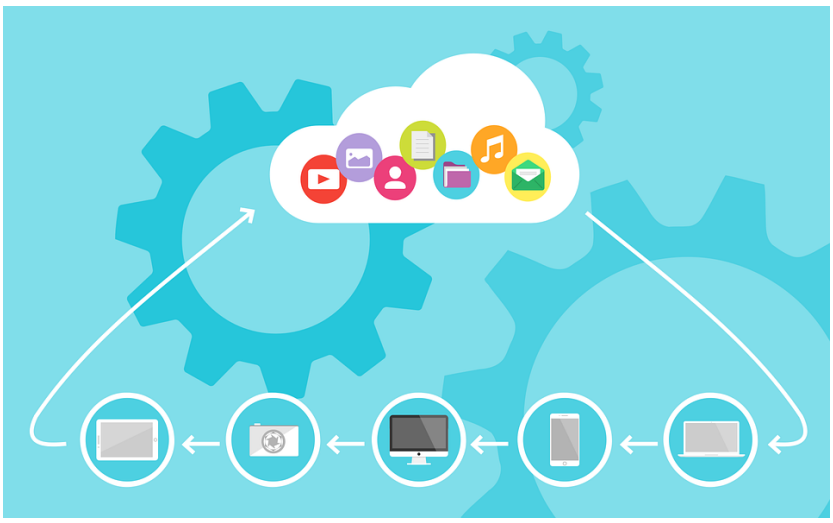
- *Experiencia del usuario*. Para los usuarios, el almacenamiento virtual aparece como una lectura o escritura estándar en una unidad física. Oculta la complejidad del sistema de almacenamiento, lo que permite a los usuarios y administradores realizar tareas como backup, archiving y recuperación de una manera más fácil y lenta.
- *Mayor capacidad de almacenamiento*. La virtualización del almacenamiento también puede ayudarle a aumentar la capacidad de almacenamiento sin necesidad de comprar nuevos dispositivos de almacenamiento.
- *Mejora de la eficiencia*. La combinación de las funciones de almacenamiento en una sola entidad hace que la transferencia de datos sea rápida y eficiente. En el pasado, para transferir los datos almacenados en un dispositivo a otro, tendría que descargar datos de un punto a otro y, a continuación, poner en línea el dispositivo de punto final. Con las técnicas de almacenamiento en disco virtual, como la visualización de almacenamiento y HCS, puede especificar el número de unidad lógica de la unidad y especificar que los datos deben ir ahora a una nueva unidad.

Otras tendencias emergentes de almacenamiento de datos.

El futuro del almacenamiento de datos parece alejarse de las unidades en niveles tradicionales en favor de servicios combinados que brindan a las organizaciones más control sobre sus datos y eliminan la necesidad de un gran personal de TI, ya que muchas funciones se pueden manejar de forma remota.

- *El almacenamiento en la nube* que es accesible desde diferentes dispositivos para los usuarios es otro segmento en crecimiento que se muestra prometedor para ser aún más rápido y más eficiente.

- *El almacenamiento flash* y los chips de almacenamiento flash dentro de las unidades SSD se están desarrollando como una opción de almacenamiento en la que puede confiar.
- *La inteligencia artificial (IA)* también es cada vez más frecuente en los nuevos tipos de almacenamiento de datos para manejar tareas repetitivas, como la administración de programaciones de copia de seguridad y la configuración de puntos de recuperación personalizados para conjuntos de datos específicos.



Consejos para el uso del almacenamiento en la nube

- *Uso de contraseñas seguras y seguras y autenticación de 2 factores*: elegir contraseñas alfanuméricas llenas de caracteres especiales es la mejor manera de mantener sus archivos almacenados en las cuentas de almacenamiento en la nube de una manera segura. Hacer uso de una autenticación de 2 factores tiene todo el sentido.

- *Realice un seguimiento de los archivos y carpetas*: auditar archivos y carpetas a intervalos regulares puede ayudar a mantener su información alejada de miradas indiscretas. Por ejemplo, mantenga una pestaña de los archivos y carpetas que

está compartiendo con sus pares y realice un seguimiento de los permisos (lectura o escritura) que les está entregando.

- *Eliminar archivos*: Casi todos los servicios de almacenamiento en la nube de renombre como Dropbox, One Drive, Google Drive ofrecen una papelera de reciclaje para almacenar todos sus archivos eliminados. De forma predeterminada, los archivos y carpetas eliminados se almacenan durante un mes y luego se borran de los servidores en la nube de forma permanente. Por lo tanto, si alguien que comparte su plataforma de almacenamiento en la nube elimina un archivo, no se asuste, ya que se puede recuperar de la papelera de reciclaje, solo en caso de que sea el administrador de la cuenta en la nube.

- *Mantenga un registro de las aplicaciones conectadas al almacenamiento en la nube*: tiene sentido tener su almacenamiento en la nube en tiempo real. Pero conectar sus aplicaciones como el calendario y el correo electrónico con la plataforma de almacenamiento en la nube a veces puede comprometer la seguridad de sus aplicaciones y luego apoderarse de su cuenta. Así que monitoree las aplicaciones conectadas al almacenamiento.

- *Alertas de cuenta*: la mayoría de las plataformas de almacenamiento de información mediante IP envían alertas cada vez que se realiza un nuevo intento de inicio de sesión y en caso de que se realicen cambios en los archivos o carpetas compartidos. Por lo tanto, opte por plataformas que ofrezcan estos servicios, ya que ayuda a controlar los cambios realizados en los archivos y carpetas almacenados en su plataforma en la nube.

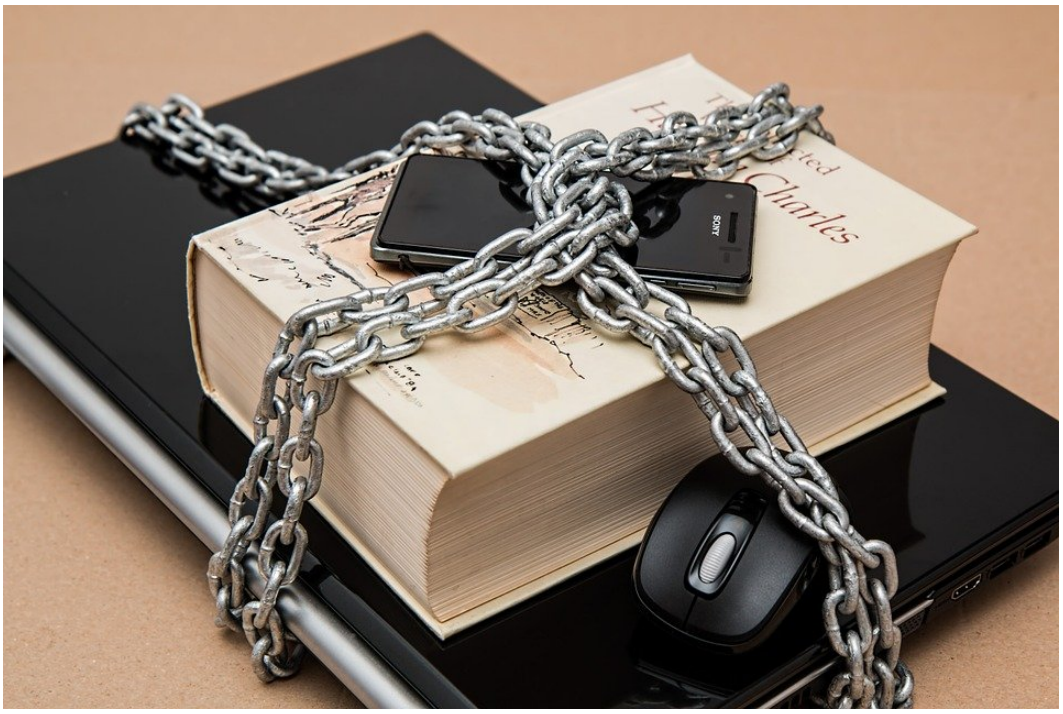
- *Desactivar cuentas obsoletas*: normalmente, cada vez que un empleado abandona una empresa, el personal del Departamento de Informática debe eliminar sus cuentas del acceso de almacenamiento en la nube. De lo contrario,

pueden hacer un mal uso del acceso para llevar a cabo algo malicioso. Desactivar el acceso a dispositivos antiguos o perdidos también tiene sentido, ya que todos los proveedores de servicios en la nube ofrecen dicha facilidad a través del navegador web.

- *La recuperación de la cuenta es vital*: tener una dirección de correo electrónico de recuperación junto con un número de teléfono ayuda a recuperar una cuenta de almacenamiento en la nube cuando surge la necesidad y ayuda a restablecer la contraseña.

- *Cerrar sesión es importante*: siempre asegúrese de cerrar la sesión de su cuenta en la nube, ya que ayuda a evitar que las personas fraudulentas accedan a sus archivos.

- *La seguridad de los dispositivos es esencial*: es importante mantener los teléfonos y ordenadores portátiles físicamente seguros al optar por aquellos dispositivos que tienen autenticación por huella dactilar o facial, ya que ayuda a mantener los datos seguros en caso de que el dispositivo se pierda o sea robado.



¿Está utilizando las soluciones de almacenamiento de datos adecuadas para su negocio?

El acto de preservar la información y los archivos importantes es vital para garantizar la continuidad y la integridad de su centro de datos e infraestructura de red durante las operaciones comerciales diarias. Al igual que nunca pensamos en la necesidad de un seguro para el hogar o para cualquier otro aspecto, pensamos que en las empresas no necesitan la recuperación ante desastres para sus datos.

Un experto en almacenamiento de datos puede ayudarlo a decidir el tipo correcto de almacenamiento de datos y diseñar un plan para garantizar que sus datos estén siempre protegidos, conservados y listos para la restauración sin interrumpir las operaciones de su negocio.

4. ALMACENAMIENTO EN LOS EQUIPOS DE TRABAJO.

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. Para ello debe cumplir los siguientes requisitos:

- El sistema proporcionará la **mínima funcionalidad requerida** para que la organización alcance sus objetivos.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son **accesibles por las personas**, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se **eliminarán o desactivarán**, mediante el control de la configuración, las **funciones que no sean de interés**, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser **sencillo y seguro**, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Para poder mantener de un modo seguro y eficaz todos estos sistemas de información es importante que la empresa especifique cuáles son las reglas, criterios y procedimientos que deben seguir todos los usuarios de los sistemas para:

• Que se garantice el acceso de los recursos de información por los usuarios o programas autorizados
• Evitar la fuga de información
• Evitar el deterioro de la información almacenada o que deba ser conservada
• Evitar el uso de dispositivos no autorizados
• Proveer métodos de recuperación de la información y la actividad en caso de fallos técnicos, accidentes o desastres

• Garantizar que al terminar su vida útil los soportes son desechados correctamente

• Conocer cómo tratar las incidencias, las fugas de información y los desastres u otras contingencias

Así, se identifican relacionadas con el almacenamiento las siguientes políticas necesarias en la empresa, para que sean conocidas por los propios usuarios y controladas por los responsables:

- Política de almacenamiento local en los equipos de trabajo
- Política de almacenamiento en la red corporativa
- Política sobre el uso de dispositivos externos
- Política de almacenamiento en cloud
- Política de copias de seguridad

Otras políticas necesarias para la buena gestión de la información en la organización son:

- Política de conservación o archivo de documentos
- Política para el uso de dispositivos móviles personales o BYOD

Políticas de almacenamiento local en los equipos de trabajo

En primer lugar, la empresa establece unas normas de almacenamiento para los equipos de trabajo (equipos de sobremesa, equipos portátiles, teléfonos y otros dispositivos) que los usuarios deben cumplir.

Esta política incluye al menos los siguientes aspectos:

- Qué tipo de información se puede almacenar en los equipos locales
- Cuánto tiempo debe permanecer dicha información en los mismos
- Permanencia de la información en la red local una vez transmitida a los servidores corporativos
- Ubicación dentro del árbol de directorios del equipo
- Utilización de sistemas de cifrado de información en los documentos empresariales
- Normativa para los empleados relativa al almacenamiento de documentos personales, archivos de música, fotografías, etc., y en concreto relativa a archivos que estén bajo algún tipo de regulación en cuanto a derechos de autor (descargas desde los equipos de trabajo)

Políticas de almacenamiento en la red corporativa

En la red corporativa es necesario distinguir entre información general de la empresa que deben utilizar todos los usuarios, e información de trabajo de los empleados almacenada en esta red corporativa. Hay que advertir a los usuarios que el almacenamiento de la información tiene un coste, tanto económico al ocupar espacio de disco, como de tiempo al hacer copias de seguridad, por lo que almacenar información no válida para la empresa es algo a evitar.

Estas políticas se basan en:

- Los servidores de almacenamiento disponibles en la red corporativa están configurados para poder almacenar y compartir aquella información de la empresa que deba ser utilizada por los empleados.
- Los controles de acceso son definidos por la dirección y el responsable de sistemas, con el objetivo de definir quién puede acceder y a dónde.
- El contenido de la información almacenada se determina a través de una política de uso específica que debe cubrir al menos los siguientes aspectos:
  - Tipo de información almacenada, momento de su almacenamiento y ubicación dentro de los directorios del sistema
  - Personas encargadas de la actualización de dicha información en caso de modificación
  - Los empleados pueden disponer de buzones o carpetas personales dentro de la misma red corporativa. En estas carpetas se almacena información que, si bien tiene relación con su trabajo, no necesariamente es compartida por otros miembros del equipo. Para controlar dicha información, se deben especificar políticas que incluyan los mismos aspectos que los relacionados con el almacenamiento local.

  • Es importante concienciar al empleado que toda aquella información almacenada en estos espacios debe ser relevante para el trabajo. La información carente de valor se elimina una vez que se haya utilizado. Así se evita que la capacidad de almacenamiento se vea desbordada innecesariamente.

Políticas sobre el uso de dispositivos externos conectados

Especialmente importante son las normas relativas al uso de equipos externos, -conocido como *BYOD (Bring Your Own Device*)- que, conectados directamente a los equipos de trabajo, permiten el almacenamiento extra de información con el objeto de trasportarla a otra ubicación o simplemente disponer de una copia de seguridad personal.

Esta política incluye al menos los siguientes aspectos:

- Si está permitido o no el uso de estos dispositivos
- En caso afirmativo, qué tipo de información en ningún caso está permitido almacenar, como aquella que contiene datos personales de clientes, etc.
- Qué medidas de borrado se han de utilizar cuando esta información deja de ser necesaria

PASSWORDS

La tecnología se desarrolla y sigue evolucionando, tanto en lo positivo como en lo negativo. Los ciberataques también se adaptan y se sofistican con el tiempo. Los ciberdelincuentes ponen a punto nuevas herramientas y técnicas maliciosas mientras

los proveedores de ciberseguridad diseñan nuevas formas de detectar y bloquear esas amenazas.

Dicho esto, en el clima actual hay ciertas estrategias que debes tener en cuenta, enfocadas a reducir tu exposición y mejorar tus defensas. Elegir una buena plataforma, ser prudente y aprender de la experiencia son una ayuda para mantenerse al margen de la mayoría de las amenazas, así como para detectar y responder más rápidamente a los ataques.

Una de las razones que hace que la ciberseguridad sea un reto es que su que su perímetro ha cambiado. Antes, las herramientas de protección se construían alrededor de un concepto: proteger el interior contra amenazas exteriores. Los servidores, aplicaciones, usuarios y datos dentro de la red eran siempre fiables, mientras que todo lo que venía del exterior suponía una amenaza potencial. Pero la generalización de las redes Wi-Fi públicas gratuitas, los dispositivos móviles, los ordenadores portátiles y la computación en nube han anulado la idea de que existe un único perímetro que defender. La mayoría de los ataques se aprovechan de credenciales robadas y suplantan a usuarios legítimos, por lo que ese viejo modelo de defensa ya no es válido.

Una de las respuestas ante esta nueva realidad, de cara a implantar nuevas plataformas y tecnologías, es que los proveedores de ciberseguridad inevitablemente deben desarrollar soluciones que se adapten para cada tipo de usuario. Mientras, en el otro lado del espectro, los ciberdelincuentes también se adaptan y ponen a punto nuevas técnicas: el aprendizaje automático y la inteligencia artificial se usan para automatizar el proceso de desarrollo de ataques personalizados y evitar la detección.

En este módulo vamos a repasar los principales puntos débiles en materia de ciberseguridad, las amenazas actuales y cómo mejorar nuestra seguridad.

Tanto en el ordenador del trabajo, como en el propio del hogar existe información y se realizan operaciones cuya repercusión económica y personal es muy importante. Esto afecta al los sistemas de las empresas y equipos informáticos, así como a la privacidad del usuario. A ninguno se nos ocurriría dejarle la llave de nuestro hogar a cualquier desconocido que nos la pidiera, incluso al perderla se procede a cambiarla inmediatamente. Algo parecido sucede con nuestras contraseñas.

A nadie se le ocurriría dejarle el nombre de usuario y contraseña de acceso a nuestros servicios bancarios por la Red a un desconocido, o siquiera, a un conocido. La repercusión de este hecho puede suponer desde que nos vacíen la cuenta suplantando nuestra persona, o en el caso de nuestro trabajo, que se apoderen de todos los datos en nuestro equipo contenidos o, incluso, puedan eliminarlos, perdiendo hasta años de trabajo por una descuidada gestión de nuestras contraseñas.

Un reciente estudio elaborado entre 325 empleados señala que un 30% de trabajadores americanos guarda sus contraseñas, apuntadas en un papel cerca del propio equipo, y un 66% lo hace en un archivo en su propio ordenador o en su móvil. Estas conductas poco cuidadosas facilitan enormemente las incidencias de seguridad que, de ocurrir, pueden llegar a tener consecuencias graves.

Así, el "phishing", uno de los fraudes más extendidos últimamente por la Red, precisamente centra su objetivo en conseguir las claves y contraseñas del usuario, para usarlas con fines espurios. Así, en el caso más habitual se suplanta la página web de una entidad bancaria o financiera (aunque pueden ser también páginas de la administración, buscadores, subastas) para de este modo, robar los datos del usuario y realizar operaciones y transacciones económicas en su cuenta bancaria.

Consecuencias de la sustracción o revelación de nuestras contraseñas

El objetivo de la sustracción de nuestras contraseñas para con ellas apropiarse de información sensible para el usuario con una finalidad de tipo económico o bien realizar otras acciones dañinas o delictivas como borrado de toda información, chantaje, espionaje industrial, etc. Las consecuencias son diversas y varían según el valor que cada usuario haya establecido para la información.

Por ejemplo, si la contraseña corresponde a la de un servicio bancario podrían sustraernos dinero de la cuenta o efectuar otras operaciones con perjuicio económico para el usuario.

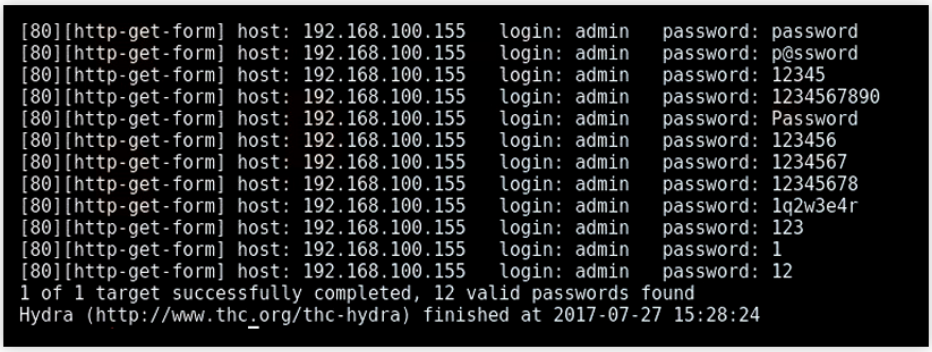
Si la contraseña pertenece al ordenador de nuestro hogar podrían tomar su control o robar toda la información contenida en él: como otras contraseñas o listados de usuarios y correos electrónicos o archivos personales y documentos. Otra consecuencia podría ser el borrado completo de toda la información allí incluida.

En el ámbito laboral, las consecuencias pueden llegar a ser catastróficas si un tercero suplanta nuestra identidad utilizando nuestro usuario y contraseña. Así, podría acceder a los sistemas corporativos con nuestro usuario y, bien sustraer todo tipo de información del trabajador y/o la empresa, o bien utilizar esta entrada para modificar o incluso eliminar archivos, con las consecuencias económicas, de responsabilidad jurídica y pérdidas de imagen que ello supondría.

Métodos por los que nuestras contraseñas quedan al descubierto Los métodos para descubrir las contraseñas de un usuario son variados. En primer lugar, se basan en la utilización de la "ingeniería social", por ejemplo utilizando el teléfono o un correo electrónico para engañar al usuario para que éste revele sus contraseñas. Dentro de este grupo destaca el fraude conocido como "phishing". En este tipo de estafa online el objetivo consiste en obtener las contraseñas o número de la tarjeta de un usuario, mediante un e-mail, sms, fax, etc. que suplanta la personalidad de una entidad de confianza y donde se le insta al usuario que introduzca sus contraseñas de acceso.

También es posible que el usuario se la comunique o ceda a un tercero y, por accidente o descuido, quede expuesta al delincuente, por ejemplo, al teclearla delante de otras personas. Puede ser que el atacante conozca los hábitos del usuario y deduzca el sistema que éste tiene para crear contraseñas (por ejemplo, que elige personajes de su libro favorito) o que asigne la misma contraseña a varios servicios (correo electrónico, código PIN de las tarjetas de crédito o teléfono móvil, contraseña de usuario en su ordenador, etc.).

Otro método, consiste en que el atacante pruebe contraseñas sucesivas hasta encontrar la que abre el sistema, lo que comúnmente se conoce por "ataque de fuerza bruta". Hoy en día un atacante, con un equipo informático medio de los que hay en el mercado, podría probar hasta 10.000.000 de contraseñas por segundo. Esto significa que una contraseña creada con sólo letras minúsculas del alfabeto y con una longitud de 6 caracteres, tardaría en ser descubierta, aproximadamente, unos 30 segundos.



Igualmente, se aplican técnicas más sofisticadas para realizar la intrusión. Se trata de métodos avanzados que en consiguen averiguar la contraseña cifrada atacándola con un programa informático ("crackeador") que la descodifica y deja al descubierto.

Un último grupo de técnicas se basan en la previa infección del equipo mediante código malicioso: con programas "sniffer" o "keylogger". Un programa "sniffer" o "monitor de red" espía las comunicaciones del ordenador que tiene residente dicho malware, a través de la red, y de ellas obtiene los datos de las claves. El "keylogger" o "capturador de pulsaciones de teclado" consiste en un programa que se instala en el ordenador del usuario de modo fraudulento, y almacena en un archivo toda aquella información que se teclea en el ordenador. Más adelante dicho archivo puede ser enviado al atacante sin conocimiento ni consentimiento del usuario y, con ello, el intruso puede obtener las distintas contraseñas que el usuario ha utilizado en el acceso a los servicios online o que ha podido incluir en correos electrónicos .

Recomendaciones en relación a la gestión y establecimiento de contraseñas.

Para gestionar correctamente la seguridad de las contraseñas, se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

1. Se deben utilizar al menos 8 caracteres para crear la clave.
2. Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.
3. Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.
4. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.
5. Las contraseñas hay que cambiarlas con una cierta regularidad. Un 53% de los usuarios no cambian nunca la contraseña salvo que el sistema le obligue a ello cada cierto tiempo. Y, a la vez, hay que procurar no generar reglas secuenciales de cambio. Por ejemplo, crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña. P. ej.: pasar de “01Juitnx” a “02Juitnx”.
6. Utilizar signos de puntuación si el sistema lo permite. P. ej.: “Tr-.3Fre”. En este caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, hay que comprobar primero si el sistema permite dicha elección y cuáles son los permitidos. Dentro de ese consejo se incluiría utilizar símbolos como: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Existen algunos trucos para plantear una contraseña que no sea débil y se pueda recordar más fácilmente. Por ejemplo se pueden elegir palabras sin sentido pero que sean pronunciables, etc. Nos podemos ayudar combinando esta selección con números

o letras e introducir alguna letra mayúscula. Otro método sencillo de creación de contraseñas consiste en elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc.

Con ello, mediante esta sencilla mnemotecnia es más sencillo recordarla. Por ejemplo:: de la frase "Comí mucho chocolate el domingo 3, por la tarde", resultaría la contraseña: "cmCeD3-:xLt". En ella, además, se ha introducido alguna mayúscula, se ha cambiado el "por" en una "x" y, si el sistema lo permite, se ha colocado algún signo de puntuación (-).

Acciones que deben evitarse en la gestión de contraseñas seguras

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas. Un 55% de los usuarios indican que utilizan siempre o casi siempre la misma contraseña para múltiples sistemas, y un 33% utilizan una variación de la misma contraseña.
2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el DNI o número de teléfono.
3. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" ó "98765")
4. No repetir los mismos caracteres en la misma contraseña. (ej.: "111222").
5. Hay que evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).

8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador).
9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios: Este método de ataque es conocido como "ataque por diccionario".
10. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
11. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos. En este caso debe existir un sistema de recarga de la contraseña o "vuelta atrás".
12. No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
13. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
14. Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

Herramientas y soluciones informáticas

Existe también la posibilidad de recurrir a herramientas y soluciones de software que creen las contraseñas seguras que vamos a utilizar. A continuación, ofrecemos una recopilación de enlaces que pueden ser de utilidad al usuario:

- LastPass: https://www.lastpass.com/es/password-generator
- Password Strength Analyser and Generator: https://pwdstr.sourceforge.io/
- Clave segura: https://www.clavesegura.org/es/
- Generador de contraseñas únicas: https://www.roboform.com/es/password-generator
- Dashlane: https://www.dashlane.com/es/features/password-generator
- Perfect Passwords: https://www.grc.com/passwords.htm

Cómo hacer una copia de seguridad de los nombres de usuario y contraseñas almacenados en Windows

Una característica poco conocida de Windows es que se puede hacer una copia de seguridad manual de los nombres de usuario y contraseñas almacenados en un archivo cifrado y bloqueado con una contraseña. Este archivo tiene la extensión ".crd" (Credential Backup Files) y se puede almacenar en un disco duro externo, una tarjeta de memoria o cualquier carpeta del ordenador.

Para hacer una copia de seguridad, seguiremos los siguientes pasos:

1. Hacer clic en el enlace que dice "Copia de seguridad de credenciales" en la sección Credenciales de Windows.
2. Se muestra la ventana "Nombres de usuario y contraseñas almacenados". En este apartado, hacemos clic en "Examinar", seleccionamos la ubicación donde deseamos guardar el archivo, le ponemos un nombre y presionamos "Guardar".
3. Para ir al siguiente paso, presione "Siguiente". Presionamos "Ctrl + Alt + Supr" para continuar la copia de seguridad en un escritorio seguro, que no puede ser interceptado tomando capturas de pantalla remotas o cualquier tipo de herramientas de monitoreo remoto.

4. La pantalla se volverá negra y solo veremos la ventana "Nombres de usuario y contraseñas almacenados". Aquí nos pide que escribamos una contraseña para proteger el archivo que vamos a crear. Escribiremos una contraseña larga, utilizando las recomendaciones que hicimos anteriormente en esta lección, y luego presionamos "Siguiente".
5. Ahora nos informa que la copia de seguridad se realizó correctamente. Las credenciales ahora se almacenan en el archivo que hemos creado, en la ubicación que seleccionamos anteriormente. Presionamos "Finalizar" para cerrar el asistente.

Ahora podemos usar este archivo de respaldo para restaurar los nombres de usuario y contraseñas en otro equipo o en el mismo equipo en el caso que tuviéramos que reinstalar el sistema operativo.

Cómo restaurar los nombres de usuario y contraseñas almacenados por Windows

Si disponemos de un archivo de respaldo con todos los nombres de usuario y contraseñas que hemos utilizado en un ordenador con Windows, podemos usarlo en cualquier momento para restaurarlo en el mismo equipo, en caso de que hayamos reinstalado el sistema operativo u en otro equipo que estemos usando.

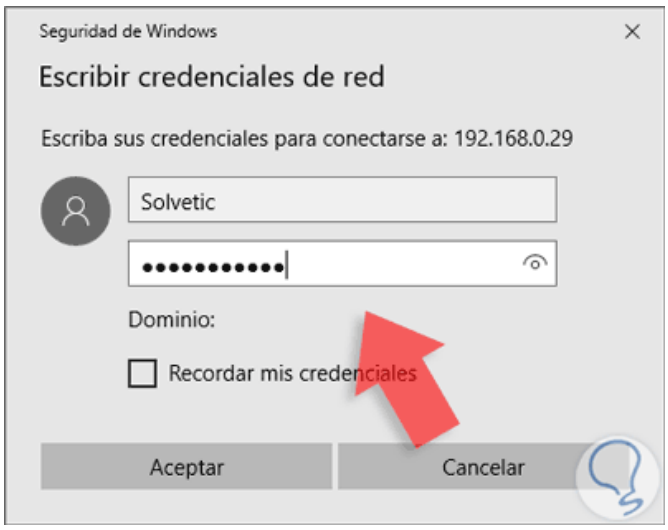
Para restaurar los nombres de usuario y contraseñas:

1. Tendremos que acceder al Administrador de credenciales y luego a la sección Credenciales de Windows. Buscamos el enlace que dice "Restaurar credenciales" y hacemos clic en él.
2. Nos mostrará la ventana "Nombres de usuario y contraseñas almacenados". Hacemos clic en "Examinar" y seleccionamos el archivo de respaldo que deseamos usar, luego presionamos "Siguiente".

3. Presionamos "Ctrl + Alt + Supr" para continuar la copia de seguridad en un escritorio seguro, que no puede ser interceptado tomando capturas de pantalla remotas o cualquier tipo de herramientas de monitoreo remoto.
4. La pantalla se volverá negra y solo veremos la ventana "Nombres de usuario y contraseñas almacenados". Aquí nos pide que escribamos la contraseña utilizada para proteger el archivo. Lo escribimos y presionamos "Siguiente".
5. Nos informa que las credenciales han sido almacenadas.
6. Presionamos "Finalizar" para cerrar el asistente. Windows usará automáticamente los nombres de usuario y las contraseñas que hayamos restaurado cuando sea necesario.

CREDENCIALES ALMACENADAS

Los equipos basados en Windows utilizan dos formas de caché de contraseñas: las credenciales de dominio y credenciales genéricas.



Credenciales de dominio

Las credenciales de dominio son utilizadas por los componentes del sistema operativo y se autentican por la autoridad de seguridad Local (LSA). Normalmente, se establecen las credenciales de dominio para un usuario cuando un paquete de seguridad

registrada autentica los datos del usuario de inicio de sesión. Este paquete de seguridad registrada puede ser el protocolo Kerberos o NTLM.

Credenciales genéricas

Las credenciales genéricas se definen y se autentican por programas que administración la autorización y la seguridad directamente en lugar de delegar estas tareas al sistema operativo. Por ejemplo, un programa podría requerir que el usuario escriba un nombre de usuario y una contraseña que proporciona el programa. O bien, un programa podría requerir que un usuario genere un certificado para tener acceso a un sitio Web.

Los programas utilizan las funciones de administración de credenciales para pedir a los usuarios las credenciales definidas por él mismo. Estas credenciales pueden adoptar la forma de un nombre de usuario, una contraseña, un certificado o una tarjeta inteligente. Las credenciales que el usuario especifica se devuelven al programa para la autenticación.

La administración de credenciales le permite personalizar la administración de la caché. También proporciona un almacenamiento a largo plazo para credenciales genéricas. Las credenciales genéricas pueden ser leídas y escritas por procesos de usuario.

Funcionalidad de las credenciales de dominio almacenadas en caché

Proporcionan la funcionalidad siguiente:

- **Single Sign-On. Inicio de sesión único (SSO)** utiliza las credenciales que se recopilan durante un inicio de sesión interactivo de dominio para que el usuario pueda autenticarse en una red una vez. Posteriormente, el usuario tiene acceso

a todos los recursos autorizados de la red sin tener que proporcionar las credenciales de nuevo. Estos recursos de red pueden oscilar entre dispositivos de hardware a programas, archivos y otros tipos de datos. Todos estos recursos pueden estar repartidos por toda la empresa en servidores de distintos tipos. Los recursos pueden estar en dominios diferentes o pueden estar en diferentes sistemas operativos.

- **Acceso a los recursos de la máquina cuando un controlador de dominio no está disponible.** Después de un inicio de sesión de dominio con éxito, una forma de la información de inicio de sesión se almacena en caché. Más tarde, un usuario puede iniciar sesión en el equipo mediante la cuenta de dominio, incluso si está disponible el controlador de dominio que autenticó al usuario. Porque el usuario ya ha sido autenticado, Windows utiliza las credenciales almacenadas en caché para iniciar una sesión el usuario localmente. Por ejemplo, supongamos que un usuario móvil utiliza una cuenta de dominio para iniciar sesión en un equipo portátil que está unido a un dominio. A continuación, el usuario toma el equipo portátil a una ubicación donde el dominio no está disponible. En esta situación, Windows utiliza las credenciales almacenadas en caché desde el último inicio de sesión para la sesión del usuario local y asignar acceso a los recursos del equipo local.

Seguridad de las credenciales de dominio almacenadas en caché

El término “credenciales en caché” no describe con precisión cómo Windows almacena en caché información de inicio de sesión para inicios de sesión de dominio. En Windows, el nombre de usuario y la contraseña no están en caché. En su lugar, el sistema almacena un verificador cifrado de la contraseña. Este comprobador es un hash de MD4 salt que se calcula dos veces. El doble cómputo convierte realmente en el Comprobador de un hash del hash de la contraseña del usuario.

Si un atacante intenta realizar un ataque en el verificador, este cifrado tiene dos consecuencias:

- Debe crearse una tabla precompilada para cada valor salt.
- El verificador no puede utilizarse para iniciar sesión en cualquier otro lugar.

Opciones de configuración de las credenciales de dominio almacenadas en caché

Tenemos las siguientes opciones:

- Número de credenciales de dominio almacenadas en caché que se almacena en el cliente. De forma predeterminada, el sistema operativo almacena en caché el Verificador para diez más reciente válida inicios de sesión cada usuario concreto. Este valor puede establecerse en cualquier valor entre 0 y 50.
- Notificación de inicio de sesión utilizando las credenciales de dominio almacenadas en caché. Cuando intenta iniciar sesión en un dominio desde un equipo cliente basado en Windows y un controlador de dominio no está disponible, no recibe un mensaje de error. Por lo tanto, puede que no perciba que inicia sesión con credenciales de dominio almacenadas en caché.

Consideraciones de seguridad para las credenciales de dominio almacenadas en caché

Independientemente de qué algoritmo de cifrado se utilice para cifrar el comprobador de contraseñas, se puede sobrescribir un comprobador de contraseñas para que un atacante se pueda autenticar como el usuario al que pertenece el comprobador. Por lo tanto, la contraseña del administrador puede sobrescribirse. Este procedimiento requiere acceso físico al equipo. Existen utilidades que pueden ayudar a sobrescribir el

verificador en caché. Utilizando una de estas utilidades, un atacante se puede autenticar utilizando el valor sobrescrito.

Sobrescribir la contraseña del administrador no ayuda al atacante a tener acceso a los datos que se cifran mediante esa contraseña. Asimismo, sobrescribiendo la contraseña no implica que el atacante acceda a los datos del sistema de archivos cifrados (EFS) que pertenecen a otros usuarios de ese equipo. Al sobrescribir la contraseña un atacante no podrá reemplazar el verificador, ya que el sistema de claves base es incorrecto. Por lo tanto, no descifrará los datos cifrados mediante el sistema de archivos cifrados o utilizando la API de protección de datos (DPAPI).

Una cuenta de usuario es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.

Para usar el ordenador de una manera organizada y segura se recomienda crear una cuenta por cada usuario que vaya a utilizar el ordenador. De esta forma, cada usuario podrá tener su propio escritorio, con una configuración y preferencias personalizadas.

El usuario administrador debe relegarse a los casos en los que sea necesario.

Para el resto de usos del equipo, hay que utilizar usuarios estándar.

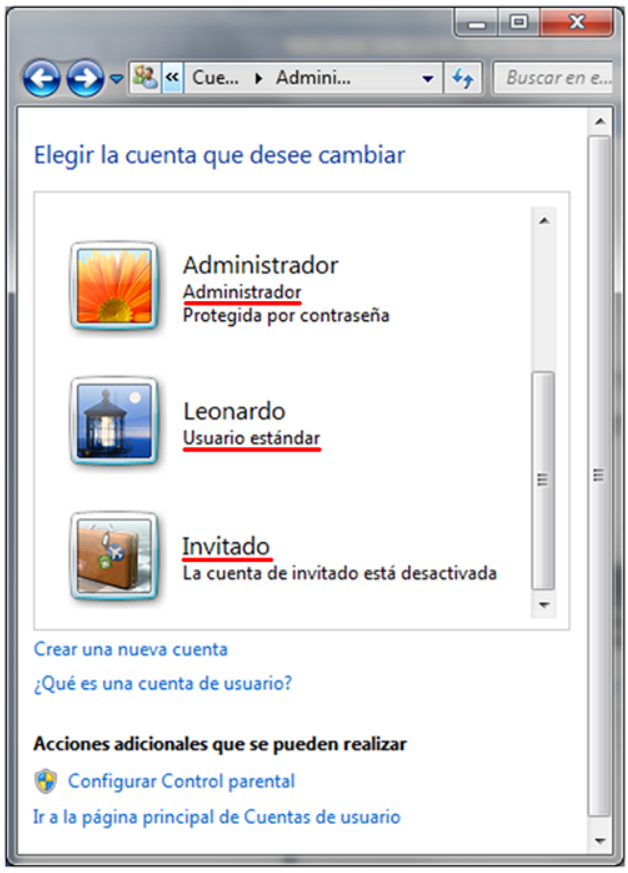
Tipos de cuentas de usuario

Para poder gestionar las cuentas de usuario de un ordenador, crearlas, eliminarlas o cambiar sus características es necesario que exista un usuario especial con permisos para administrarlas.

Este es el usuario administrador. Sólo los usuarios de este tipo pueden instalar aplicaciones en el ordenador o modificar aspectos importantes de la configuración, como la conexión a Internet.

Todo equipo debe tener una cuenta de usuario administrador, para configurarlo y administrar el resto de cuentas de usuario que serán las de los usuarios normales, los usuarios estándar, para el uso cotidiano del ordenador.

Existe un tercer tipo de cuenta: el usuario invitado que sirve para que usuarios sin una cuenta personal, pueda iniciar una sesión y utilizar el equipo puntualmente.



Las cuentas de usuario y la seguridad

El uso de la cuenta de administrador debe limitarse a aquellas situaciones en las que necesitamos disponer de privilegios: realizar cambios en la configuración, instalar una nueva aplicación, dar de alta un nuevo usuario, etc. Al finalizar estas tareas, debemos seguir trabajando con una cuenta estándar.

Cualquier cosa que hagamos con la cuenta de administrador afecta a todo el ordenador, y por tanto al resto de cuentas de usuario. Si cometemos un error o un descuido como administradores, esto afecta a todos los usuarios.

Además, si un virus infecta el ordenador cuando estamos utilizando una cuenta de administrador, podrá tener control total sobre el equipo, resultando más difícil de eliminar. Sin embargo, si la infección se produce utilizando una cuenta de usuario estándar, la limitación en los permisos reducirá mucho los efectos nocivos del virus.

Es muy importante habilitar el uso de contraseñas para poder abrir una sesión en el equipo desde el punto de vista de la seguridad.

En el caso de las cuentas de usuario administrador esta práctica es necesaria dados los permisos de administración que estas cuentas tienen sobre las otras cuentas y sobre la configuración del equipo. Para el resto de cuentas de usuario también es necesario establecer una contraseña de acceso para proteger el espacio privado de cada usuario del equipo.

Debemos saber que la cuenta de usuario invitado tiene los mismos privilegios que un usuario estándar, pero es anónima y sin contraseña. Por defecto, viene deshabilitada, y desde el punto de vista de la seguridad es conveniente que se mantenga así.

ACTUALIZACIONES

Las actualizaciones son añadidos o modificaciones realizadas sobre los sistemas operativos o aplicaciones que tenemos instalados en nuestros dispositivos y cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

Si no mantenemos nuestros equipos al día nos exponemos a todo tipo de riesgos: robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, etc.

Por tanto si queremos disfrutar de las ventajas de la tecnología debemos:

- Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
- Elegir la opción de actualizaciones automáticas siempre que esté disponible.
- Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
- Evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.

¿Por qué son tan importantes las actualizaciones?

Cualquier programa es susceptible de tener fallos de seguridad. Por este motivo, puede necesitar ser actualizado independientemente del dispositivo en el que se encuentre instalado. Esto incluye los programas y sistemas operativos de ordenadores, tabletas, smartphones, consolas de videojuegos e incluso televisiones inteligentes.

Las actualizaciones de software no son un fastidio. Al contrario, son esenciales para mantener la seguridad de nuestros dispositivos.

Debemos ser conscientes de que en nuestros dispositivos también hay instalados navegadores, programas, plugins, etc. que por supuesto, también necesitan ser actualizados para mantenerlos al día y bien protegidos.

Un caso especial, son las actualizaciones de las herramientas antivirus ya que sólo serán eficaces si están a la última. De nada sirve tener instalado un antivirus si no es capaz de detectar las últimas amenazas que circulan por la red.

Importante, no debemos confundir tener una aplicación actualizada con tener la última versión. Podemos tener instalado y actualizado Microsoft Office 2007 a pesar de no tratarse de la última versión de este paquete de herramientas ofimáticas. Los fabricantes no sólo comercializan nuevas versiones que incorporan mejoras, sino que mantienen un largo periodo de tiempo las antiguas versiones a través de actualizaciones.

¿Quién se encarga de publicarlas?

Las actualizaciones son elaboradas y ofrecidas por los propios desarrolladores y fabricantes. En algunos casos publican los parches (así se llaman también las actualizaciones de seguridad) con gran rapidez. En otras ocasiones, los fabricantes tienen que adaptar los parches a sus dispositivos y el proceso no es tan rápido.

En este caso último caso poco podemos hacer más allá de ser conscientes del riesgo y no realizar acciones que nos puedan comprometer hasta que la actualización esté disponible.

Qué debemos hacer ante una nueva actualización

Hemos de ser conscientes del riesgo que supone utilizar un equipo no actualizado. Una vez que se hace público un fallo de seguridad, cualquiera con los conocimientos adecuados puede utilizarlo para causarnos un perjuicio. Por tanto, todos hemos de adoptar el hábito de mantener nuestros dispositivos al día.

En muchos casos, las aplicaciones y dispositivos disponen de opciones de actualización automática, de manera que las instalan, de forma transparente para nosotros, tan pronto el fabricante o desarrollador las publican. Esta es la opción más recomendada ya que evita que tengamos que estar nosotros pendientes de esta tarea, que en ocasiones resulta un poco molesta.

Para facilitarnos el trabajo, existen herramientas que nos ayudan a saber si nuestros equipos están a la última. Un ejemplo es PSI (Personal Software Inspector), que recopila el software que está instalado en el sistema y alerta de las aplicaciones que no están actualizadas. De esta manera cubrimos aquellas aplicaciones que no poseen un sistema de actualizaciones automático.

Algunas precauciones

Los delincuentes han descubierto que la instalación de parches constituye un nuevo modo de infectar un dispositivo. Por ello ciertos sitios de Internet y ciertas aplicaciones nos ofrecen la instalación de actualizaciones falsas. Al aceptarlas, nuestro equipo quedaría infectado. Por tanto, no debemos instalar nada que no provenga de los canales oficiales que proporcionan los fabricantes y desarrolladores de los dispositivos o el software.

Debemos huir de sitios "pirata", especialmente de aquellos que ofrecen aplicaciones o servicios gratuitos o extremadamente baratos.

Otra situación que debemos tener en cuenta es la instalación o actualización de una aplicación que necesita ciertos privilegios para funcionar correctamente. Es recomendable revisarlos, para evitar que individuos maliciosos que buscan tomar control de nuestro dispositivo puedan usarlos. En cualquier caso, instalemos aplicaciones sólo de fuentes de confianza y siempre revisemos los privilegios por si fuesen excesivos o innecesarios para el propósito a que están destinadas.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

5. ALMACENAMIENTO EN LA NUBE

Cada vez se usa más el entorno cloud tanto a nivel doméstico como empresarial. La facilidad de uso y el bajo coste económico de almacenamiento ha propiciado su rápido crecimiento.

En el caso de que la empresa ponga a disposición de los empleados algún tipo de almacenamiento cloud (en la nube), esta política debe incluir al menos los siguientes aspectos:

- Si está permitido o no el uso de servicios cloud públicos
- En caso afirmativo, qué tipo de información en ningún caso está permitido almacenar, como aquella que contiene datos personales de clientes, etc.
- Qué medidas de borrado se han de utilizar cuando esta información deja de ser necesaria
- En los servicios cloud privados se establecerán los criterios para su contratación de manera que se cumplan los criterios de la organización y legales para la información que allí se almacene.

Uno de los aspectos en los que más han hecho énfasis los proveedores de servicios en la nube es sin duda el de la seguridad. Compañías como Google, Amazon o Microsoft dedican colosales presupuestos a asegurar las infraestructuras con las que dan sus servicios o las que las empresas "alquilan" en plataformas en la nube como Azure, Google Cloud o AWS.

Sin embargo, a pesar de la seguridad de estos sistemas, los datos, aplicaciones y servicios que se implantan en ellos no siempre están seguros y siguen siendo un objetivo muy interesante para los atacantes.

Así, si tienes parte de tu infraestructura en servicios en la nube hay al menos 12 vulnerabilidades muy importantes a las que siguen expuestas si no tomas precauciones.

Es lo que afirma la llamada Cloud Security Alliance (CSA) que ha publicado su último informe de amenazas Treacherous 12 Top Threats to Cloud Computing Plus: Industry Insights report.

Y es que, a pesar las ideas preconcebidas sobre la seguridad en entornos cloud (que por otro lado han sido los proveedores los que se han encargado de extender), la responsabilidad de proteger los datos de las empresas en la nube no recae en el proveedor de servicios sino en el usuario.

Por ello, el destinar ingentes recursos a examinar si un proveedor es más o menos seguro no tiene mucho sentido si no se tienen en cuenta estas 12 vulnerabilidades que apunta CSA y que se centran en problemas que tienen que ver con la propia naturaleza de los servicios en la nube, que son habitualmente compartidos y se consumen bajo demanda.

Las conclusiones del informe se basan en las aportaciones de expertos en tecnología cloud y seguridad encuestados por CSA y han sido ordenados por orden de relevancia o gravedad.

1. **Violaciones de datos**. Una brecha de datos o el robo de estos puede ser provocada por un ataque dirigido o el resultado de un error humano, así como vulnerabilidades de una aplicación o sencillamente malas prácticas de seguridad, según explica la CSA. En este caso puede ser cualquier tipo de información que no debería hacerse pública, como información de salud, financiera, información de identificación personal, secretos comerciales y propiedad intelectual. Por supuesto, este robo de datos puede realizarse tanto en infraestructuras en la nube como en las basadas en las de la propia organización (on premises) pero es una de las principales preocupaciones para las organizaciones que usan servicios cloud. Y es que da igual que los servicios cloud aseguren su hardware o las máquinas virtuales que ofrecen si los responsables de las organizaciones no no configuran correctamente el acceso a los datos y dejan una puerta abierta a los intrusos.
2. **Gestión de la identidad y los accesos deficientes**. Los ciberatacantes que consiguen hacerse pasar por usuarios legítimos, ya sean operadores o desarrolladores de las aplicaciones pueden leer, modificar y eliminar datos, robar la información o espiar, así como inyectar aplicaciones o código malicioso que parece provenir de un usuario legítimo. Según CSA, una mala gestión de la identidad, de las claves o credenciales puede hacer que un ciberatacante acceda

a las infraestructuras con resultados desastrosos como han revelado ataques a grandes redes sociales o empresas como Equifax.

3. **APIs inseguras**. Uno de los aspectos clave de la seguridad de servicios en la nube se encuentra en muchas ocasiones en la de las interfaces de programación o las APIs de los servicios que ofrecen para crear aplicaciones. Estas API son uno de los elementos más diferenciales que ofrecen los proveedores, pero tienen que diseñarse para evitar cualquier intento de sobrepasar las políticas de seguridad.

4. **Vulnerabilidades de los sistemas**. Las vulnerabilidades del sistema son bugs explotables en programas que los atacantes pueden usar para infiltrarse en un sistema para robar datos, tomar el control o interrumpir el servicio. Las vulnerabilidades del sistema operativo ponen la seguridad en riesgo según la CSA y el hecho de que los servicios y aplicaciones de distintos clientes compartan elementos como el procesador o la memoria física de los equipos proporciona una nueva superficie de ataque.

5. **Robo de cuentas**. El robo de cuentas o servicios no es nuevo, señala CSA, pero los servicios en la nube añaden una nueva amenaza. Si los atacantes consiguen acceso a los datos de acceso de un usuario, pueden interceptar actividades y manipular datos, devolver información falsificada y redirigir a los usuarios a sitios engañosos. Con credenciales robadas, los atacantes pueden acceder a las áreas críticas de los servicios en la nube para causar daños mayores o llevar a cabo robos más importantes de información.

6. **Ataques desde el interior**. Un usuario malintencionado, como un administrador, puede acceder a información confidencial y puede tener niveles crecientes de acceso a sistemas más críticos y, finalmente, a datos. Según algunos estudios como el de Broadcom (empresa de software y electrónica de comunicaciones),el 90 por ciento de las organizaciones es consciente de que es vulnerable a estos ataques por parte de sus propios empleado. Según CSA, los sistemas que dependen exclusivamente de proveedores de servicios en la nube

para la seguridad corren un mayor riesgo. Para evitar estos ataques, las organizaciones adoptan sistemas de monitorización de los usuarios, sistemas de detección y prevención de intrusiones (IDS), sistemas de prevención de pérdida de datos (Data Loss Prevention DLP) y sistemas de gestión de acceso y de las identidades.

7. **Amenazas persistentes avanzadas** (APT). Según CSA, las: Amenazas Avanzadas Persistentes son una forma de ataque que se infiltra en los sistemas para comprometer un sistema que albergue información valiosa, pero puede ser también para establecer un punto de apoyo en la infraestructura de las empresas que se trata de atacar, y a partir de los cuales roban datos. Las APT persiguen a sus objetivos de forma sigilosa durante largos periodos de tiempo, a menudo adaptándose a las medidas de seguridad destinadas a defenderse contra ellos. El problema en los servicios en la nube se encuentra que una vez instaladas, los ataques pueden moverse lateralmente a través de las redes del centro de datos y mezclarse con el tráfico de red normal para lograr sus objetivos.

8. **Pérdida de datos**. Según CSA, los datos en la nube se pueden perder por razones distintas un ataque: un borrado accidental por el proveedor de servicios o una catástrofe como un incendio o terremoto puede ocasionar la pérdida permanente de datos. Por ello, tanto el proveedor como el usuario deben tomar medidas de seguridad contar con un respaldo de los datos más importantes.

9. **Análisis de riesgos insuficiente**. Cuando las empresas definen nuevas estrategias o servicios, es importante evaluar las tecnologías en la nube que se van a utilizar, sopesar los riesgos y contar con una hoja de ruta adecuada y una lista de verificación adecuada para que estos servicios no supongan exponerse a ataques o al robo de información sensible.

10. **Abuso y uso nefasto de servicios cloud**. Servicios cloud con deficientes medidas de seguridad, versiones y servicios prueba que se ofrecen en ellos y registro de cuentas utilizando medios de pago fraudulentos como tarjetas robadas pueden hacer que estos servicios en la nube se vean atacados de muy

diversos modos, según CSA. Los atacantes pueden usar estos servicios en la nube para crear bots atacantes hacia usuarios, empresas, o incluso a otros servicios en la nube. Entre los ataques se encuentran ataques DDoS, envío de correo basura o campañas de phising.

11. **Ataques de denegación de servicio** (DoS). Los ataques DoS se han diseñado para detener máquinas o servicios y evitar que los usuarios puedan acceder a sus datos o aplicaciones. Al forzar a un servicio cloud a consumir cantidades excesivas de recursos como potencia del procesador, memoria, almacenamiento o ancho de banda, los atacantes pueden ralentizar los sistemas de los usuarios legítimos (lo que se denomina en ocasiones "los vecinos ruidosos") o incluso dejarlos sin acceso.

12. **Vulnerabilidades por tecnologías compartidas**. Los proveedores de infraestructuras cloud ofrecen sus servicios de forma escalable compartiendo infraestructura física, plataformas o aplicaciones. En ocasiones, los componentes que hay bajo la infraestructura pueden no ofrecer el aislamiento necesario para ser utilizados por múltiples clientes, lo que puede conducir a vulnerabilidades de tecnologías compartidas.

Con la aparición del cloud computing se ha creado una amplia gama de posibilidades tanto para empresas y organizaciones (públicas o privadas) como para particulares, ya que ha hecho posible la existencia de sistemas que ofrecen recursos de procesamiento y almacenamiento de datos bajo demanda y la creación de bases de datos de alta escalabilidad.

Sin embargo, la seguridad se está presentando como una de las barreras que tiene que vencer este tipo nuevo de servicios para desarrollar todo su potencial. Existen cinco riesgos principales que centran actualmente el debate en torno a la seguridad y el cloud computing.

Uno de los riesgos más importantes a la hora de utilizar el cloud computing es la pérdida de control en el uso de las infraestructuras de la nube. Esto sucede porque el cliente cede necesariamente control al proveedor de la nube en algunos asuntos que pueden afectar a la seguridad. Además, los acuerdos de nivel de servicio (SLA, en sus siglas en inglés) pueden no ofrecer un compromiso concreto por parte del proveedor de la nube para prestar dichos servicios, con lo que deja espacio para potenciales problemas de seguridad.

Otro problema es el *Lock-In*, término que se refiere a la falta de herramientas, procedimientos y servicios de interfaz que puedan garantizar la seguridad de los datos y las aplicaciones cuando se lleva a cabo la portabilidad a otro proveedor. Por tanto, pueden aparecer problemas cuando una organización o una empresa han externalizado los servicios de almacenamiento, o de gestión de las infraestructuras de almacenamiento, y se quiere cambiar de un proveedor a otro, migrar los datos a otro sistema o volver a gestionarlos internamente. Este tipo de técnicas introduce una dependencia de los proveedores de servicios cloud para la provisión de estos servicios, sobre todo para la portabilidad de datos.

Los fallos de aislamiento también son otros de los riesgos que entraña el cloud computing. Esto se debe a que una de las características con la que operan estos sistemas es la tenencia múltiple (multi-tenancy) y la compartición de recursos. Estos fallos se producen, en ocasiones, a la hora de aislar y separar los mecanismos de almacenamiento, la memoria, el enrutado o diferentes usuarios que han contratado servicios de la nube. Sin embargo, es necesario precisar que los ataques a los

mecanismos de aislamiento son mucho menores y mucho más complicados de penetrar por un atacante que con los sistemas operativos tradicionales.

En cuanto al cumplimiento de requisitos, podemos encontrar riesgos importantes a la hora de invertir en certificaciones externas de seguridad o calidad de los servicios, que presta la empresa u organización, cuando se están utilizando servicios en la nube. Estos problemas se dan porque, en muchas ocasiones, el proveedor de la nube no puede reportar evidencias de sus propios procesos de cumplimiento o porque tampoco se permite al usuario auditar a su proveedor sobre el cumplimiento de sus políticas internas de seguridad.

Así, estos puntos pueden conllevar que una empresa no pueda cumplir con sus propios requisitos al no saber cuál es el trato que está recibiendo la información que ellos han almacenado en el servicio cloud que tienen contratado.

Otro riesgo más es el de la gestión de interfaces comprometidas. Con los servicios de la nube para almacenar datos, la gestión de las interfaces se realiza a través de Internet. Este medio, a pesar de ser más rápido y más económico para gestionar grandes cantidades de información, entraña ciertos riesgos al estar expuesto al tráfico de Internet. Especialmente cuando se combinan accesos remotos y navegadores web que son más vulnerables a los ataques.

Riesgos añadidos

A estos riesgos y problemas, a los que aún no se les ha encontrado una respuesta adecuada y efectiva, se les suma la dificultad de borrar datos de forma efectiva y segura y los riesgos propios de sufrir ataques por parte del propio personal que gestiona las infraestructuras del proveedor de servicios cloud.

El primero se debe a que los sistemas cloud realizan migraciones de la información entre los diferentes recursos de la nube para su almacenamiento. Si estos datos no se borran efectivamente en todas las fases de la evolución, podrían caer en manos de personas no autorizadas.

En cuanto al segundo problema, para gestionar los servidores de almacenamiento del proveedor de servicios cloud se tienen que crear perfiles con acceso a puntos donde un tercero (la compañía que utiliza los servicios cloud) tiene almacenada información que puede resultar muy sensible. Por este motivo, las políticas del proveedor de servicios cloud deben ser muy estrictas para controlar a su propio personal y el tratamiento que hacen con la información almacenada por terceros.

Por todo lo expuesto anteriormente, el cloud computing, a pesar de su enorme potencial, cuenta con una serie de debilidades ligadas a la seguridad en las que actualmente se está trabajando.

En lo que se refiere a las soluciones big data, este nuevo paradigma tecnológico puede suponer, desde el punto de vista de la seguridad, tanto una amenaza como una oportunidad.

Como se ha visto anteriormente, el análisis de grandes cantidades de información es una gran oportunidad para mejorar la inteligencia de los sistemas de ciberseguridad y la prevención de incidentes de seguridad.

Sin embargo, el almacenamiento y tratamiento de enormes cantidades de datos supone un riesgo para la seguridad, ya que filtraciones o robos de información pueden tener importantes efectos legales y reputacionales para una organización.

El cloud computing y el big data van inexorablemente unidos, pues es poco probable que una organización almacene in house tal cantidad de datos. Por ello, los riesgos para la seguridad que ya hemos mencionado para el cloud computing son, en general, aplicables al big data. Otros riesgos más concretos a los que se enfrenta el big data son:

- Al tratarse de una tecnología nueva, el desconocimiento por parte de las organizaciones que lo aplican puede hacer que sea más vulnerable.
- La autenticación de usuarios y el acceso a los datos desde múltiples ubicaciones pueden no estar suficientemente controlados.
- Se puede ofrecer una oportunidad significativa para la entrada de datos maliciosos o para una inadecuada validación de los datos.

Soluciones de seguridad

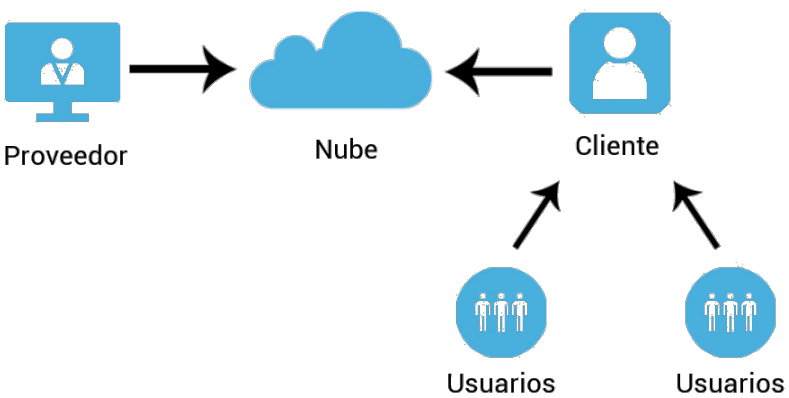
Dentro de los sistemas tradicionales de seguridad, la encriptación de los datos de la red y la resiliencia de la red (que es la habilidad de proveer y mantener un nivel aceptable del servicio con el que poder hacer frente a los fallos y los retos que surgen diariamente por la utilización de la red) son las medidas de seguridad de mayor importancia.

El cifrado resulta fundamental para la protección de infraestructuras críticas que se van a servir de la nube. A través de los protocolos de capa 2 y 3 del modelo OSI se puede proveer de unos niveles aceptables de aseguramiento sobre la seguridad de conexión.

En cuanto a la resiliencia, tras asegurar la infraestructura de la nube y sus comunicaciones, se necesita conseguir que la conexión resulte confiable. Para ello se requerirá un nivel constante y permanente de conectividad con el que asegurarnos de que no se puede producir ninguna disrupción del servicio que le afecte con severidad.

Hay dos aspectos fundamentales que tener en cuenta. Uno es la necesidad de reforzar el mecanismo de enrutado y otro prevenir los ataques malévolos al servidor. En el primer caso se necesita mejorar la arquitectura mediante un fortalecimiento del enrutado, que lo haga más fiable y ofrezca una garantía sobre la conexión de extremo a extremo.

En el segundo, es necesario proteger la conectividad de ataques, como los de Denegación de Servicios Distribuidos (DDoS, según sus siglas en inglés), que han hecho populares organizaciones como Anonymus y que se han vuelto un quebradero de cabeza para los administradores ITEn este campo aún se siguen buscando fórmulas efectivas de protección porque hasta ahora las que se han puesto en marcha no se han mostrado infalibles o efectivas al 100%.



En el ámbito del big data, el mecanismo más efectivo para hacer frente a los riesgos inherentes es el cifrado de los datos, que asegura la protección de los mismos desde el principio del proceso hasta el final y que solo sean utilizados por el personal autorizado a trabajar con ellos.

También las soluciones de control de acceso granular están resultando muy útiles para que los administradores puedan acceder y compartir los datos de una forma más selectiva y precisa, al prevenir el mismo problema que con la encriptación.

Como se ha comentado en repetidas ocasiones a lo largo del capítulo anterior, también es muy importante la monitorización continua para estar informados en todo momento de si se ha producido un ataque y así poder evitar de la forma más rápida posible una pérdida de información delicada.

6. APLICACIONES PERMITIDAS.

En cualquier empresa, uno de los principales requisitos en cuanto a propiedad intelectual se refiere, se basa en el uso de software legal. Utilizar software ilegal adquirido de forma fraudulenta podría conllevar sanciones económicas e incluso, penales.

Por otro lado, hacer uso de software del que no se puede saber si lleva asociado algún tipo de malware o agujero de seguridad, no hace más que aumentar las posibilidades de riesgo por infección.

Además, si tenemos como fin evitar fugas de información o garantizar la privacidad de los datos de carácter personal, será necesario determinar por parte de cualquier empresa qué tipo de aplicaciones serán las que estén autorizadas para el tratamiento de este tipo de información.

Para garantizar el uso de un determinado tipo de software, la empresa deberá disponer de una política que cuente con:

- Listado de software autorizado.
- Repositorio de software autorizado y registro de licencias.
- Sanciones disciplinarias asociadas al incumplimiento de esta normativa.

Además, desde la empresa se deberá identificar a los responsables de controlar que la empresa usa software autorizado así como la realización de auditorías necesarias en cuanto a su uso.

¿Cuáles son los puntos clave en este tipo de políticas?

- *Llevar un registro actualizado de licencias*, que cuente con datos como nombre y versión del producto, autor, fecha de adquisición, vigencia de la licencia, número de usuarios permitidos por licencia, etc.

- *Identificar quién tiene la competencia para la instalación, actualización y borrado del software.* De esta forma nos aseguraremos que únicamente el personal autorizado podrá ejecutar este tipo de acciones. En caso de no disponer de esta figura o que sea personal externo quien lleve a la práctica estas acciones, se deberá documentar y notificar la autorización y operativa.

- *Documentar y dar a conocer las sanciones disciplinarias derivadas del uso de software ilegal no autorizado*, así como las responsabilidades civiles y penales según la legislación vigente en materia de protección de propiedad intelectual. Esta medida va encaminada a concienciar de las consecuencias del uso de software ilegal.

- *Contar con un repositorio de software*. De esta manera, si se quiere instalar un determinado programa de forma rápida y eficiente, se establecerá una ubicación donde localizarlo así como claves de activación, números de serie, licencias, etc.

- *Realizar auditorías del software instalado* en cualquier momento y en cualquier equipo para verificar que se cumple con las políticas establecidas.

- *Comprobar tanto las autorizaciones como las licencias*. Será necesario garantizar que los programas instalados (incluidos los dispositivos BYOD), estén debidamente autorizados y que cuenten con las licencias necesarias.

- *No permitir que se realicen copias del software* disponible sin el debido consentimiento.

Controlar el software que se instala en una empresa será una tarea necesaria si queremos reducir los riesgos asociados a la instalación de software ilegal, que pueden venir acompañados de código malicioso que podría provocar infecciones en los equipos locales o incluso fugas de información.

Evitar este tipo de riesgos está en tu mano. Establece una política que regule qué aplicaciones serán las permitidas en el marco tecnológico de tu organización.

Proteja su PC de aplicaciones potencialmente no deseadas (Windows 10)

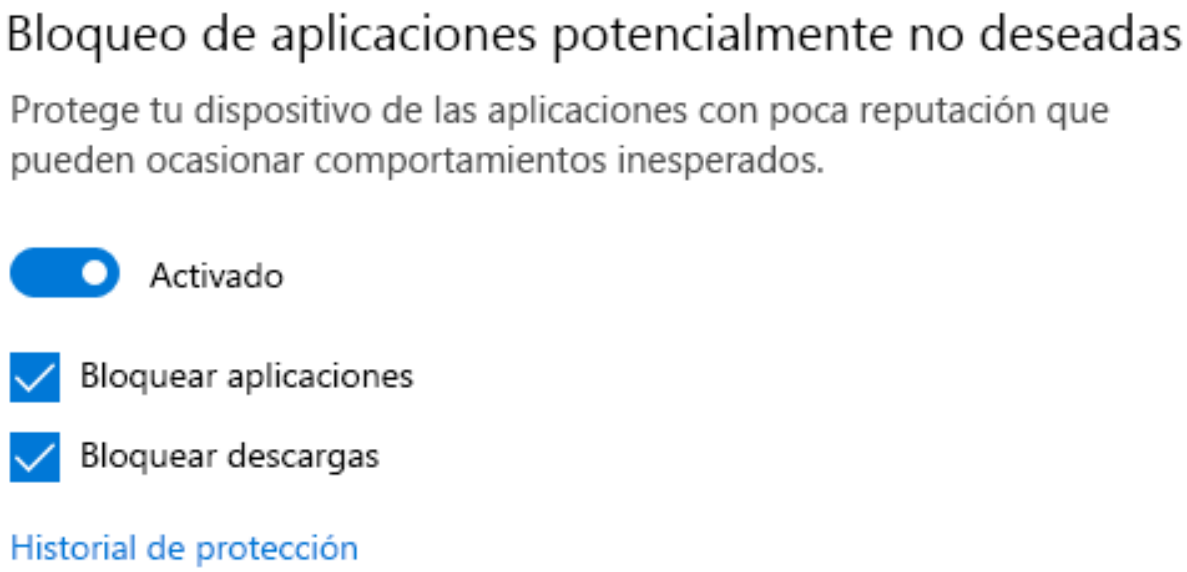
Entre las aplicaciones potencialmente no deseadas (PUA) se encuentran una categoría de software que puede hacer que su equipo funcione despacio, mostrar anuncios inesperados o, en el peor de los casos, instalar otro software que pueda resultar más dañino o molesto.

La seguridad de Windows tiene protección basada en su reputación que puede ayudar a proteger el equipo de aplicaciones potencialmente no deseadas. El bloqueo de aplicaciones potencialmente no deseadas se presentó por primera vez en la actualización de Windows 10 de mayo de 2020 y está desactivado de forma predeterminada. (Es posible que los clientes empresariales lo tengan activado de forma predeterminada).

¿Cómo lo activo?

Para activar el bloqueo de aplicaciones potencialmente no deseadas, vaya a Inicio > Configuración > Actualización y seguridad > Seguridad de Windows > Control de aplicaciones y navegador > Configuración de la protección basada en reputación.

Allí encontrará un control que le permite activar el bloqueo de aplicaciones potencialmente no deseadas, y seleccionar si desea bloquear aplicaciones, descargas o ambas.



¿Por qué no veo estas opciones en mi ordenador?

Esta característica se ha estrenado con la actualización de mayo de 2020 de Windows 10. Si aún no la ve, ejecute Windows Update y asegúrese de que tiene la versión más reciente.

El bloqueo de aplicaciones potencialmente no deseadas (PUA) requiere al menos:

Para buscar las versiones actuales instaladas en el sistema, vaya a Seguridad de Windows, seleccione Configuración en la esquina inferior izquierda de la ventana y, a continuación, Acerca de. Si su sistema aún no cumple estos requisitos, vaya a Windows Update e instale las actualizaciones más recientes.

- Versión del cliente Antimalware: 4.18.2003.8
- Versión del motor: 1.1.16900.4

- Versión antivirus: 1.1311.560.0
- Versión de AntiSpyware: 1.311.560.0

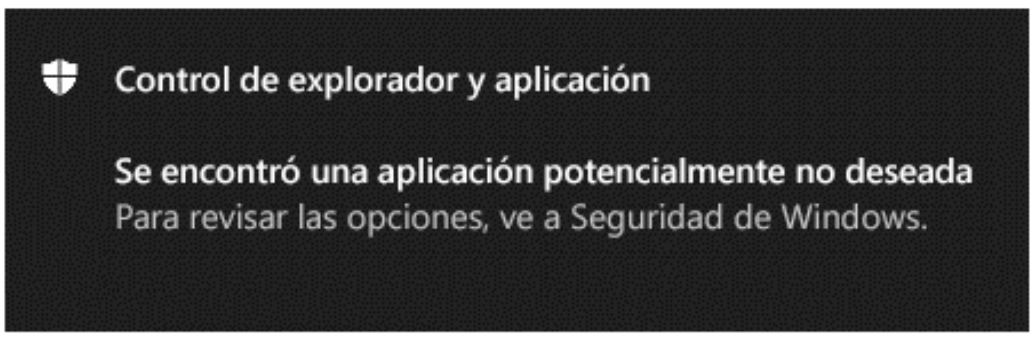
Se recomienda activar esta característica, que permite bloquear aplicaciones y descargas.

- Bloquear aplicaciones detectará PUA que ya ha descargado o instalado, por lo que si usa un explorador distinto, la seguridad de Windows aún podrá detectar PUA después de descargarlos.

- Bloquear descargas busca el PUA durante la descarga, pero solo funciona con el nuevo navegador Microsoft Edge.

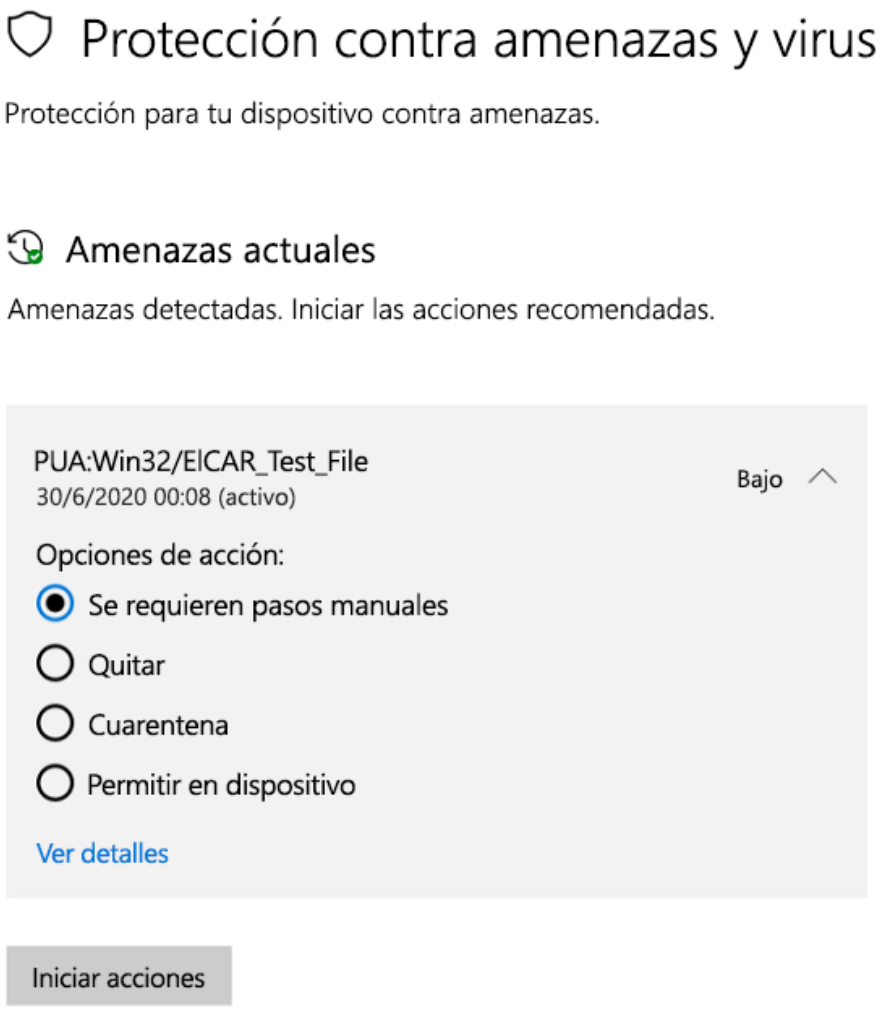
¿Qué ocurre cuando se detecta un PUA?

Cuando la seguridad de Windows detecta una aplicación potencialmente no deseada, recibirá una notificación que le pedirá llevar a cabo acciones al respecto.



Haga clic en la notificación para ir al área Protección contra virus y amenazas de Windows y, después, haga clic en el nombre de la PUA para seleccionar la acción que se llevará a cabo.

Nota: Es posible que no tenga todas las opciones que se muestran en el ejemplo siguiente.



Importante: Hasta que seleccione una acción para llevar a cabo y que la seguridad de Windows realice dicha acción, la PUA que se ha detectado solo está bloqueado en su sistema; no se elimina. Es posible que los exámenes futuros puedan seguir detectando el PUA hasta que realice una acción.

Una vez que haya realizado la selección, seleccione Acciones de inicio.

7. CLASIFICACIÓN DE LA INFORMACIÓN.

La clasificación de la información nos ayuda a categorizar los datos de una manera que transmita la sensibilidad de la información, como los datos que deben salvaguardarse para garantizar la confidencialidad, integridad y disponibilidad.

Esto es lo que necesita saber sobre la importancia de las directivas de clasificación de datos, cómo funcionan y las prácticas recomendadas para el desarrollo de directivas.

Definición de una política de clasificación de información

Una política de clasificación se ocupa principalmente de la gestión de los datos para garantizar que la información confidencial se maneje bien con respecto a la amenaza que representa para una organización.

También tiene en cuenta la forma en que estos datos recopilados se utilizan y estructuran dentro de una organización para permitir que el personal autorizado obtenga la información correcta en el momento adecuado, al tiempo que ayuda a garantizar que solo aquellos que están autorizados puedan ver o acceder a la información.

La base de datos de cualquier organización contiene datos que difieren en su nivel de sensibilidad, es decir, algunos datos son más sensibles que otros.

La clasificación de la información, la directiva de seguridad y el análisis de riesgos son funciones relacionadas que las organizaciones utilizan junto con la seguridad:

- Una *directiva de clasificación* de datos es la personificación de la tolerancia de riesgo de una organización.

- Una *directiva de seguridad* es un plan de alto nivel que indica la intención de administración correspondiente a cómo se supone que la seguridad es competente en una organización, qué acciones son aceptables y la magnitud del riesgo que la organización está dispuesta a aceptar. Por ejemplo, una directiva de seguridad de datos podría realizar una evaluación de riesgos o podría tener los datos de la organización clasificados.

- El *análisis de riesgos* equilibra los activos de una organización con las amenazas de pérdida y es el catalizador para implementar salvaguardas o contramedidas que mitiguen el riesgo.

Por lo tanto, las directivas de clasificación de datos y el análisis de riesgos son conceptos separados que caen bajo el paraguas de la política de seguridad.

Cómo funcionan las directivas de clasificación de información

Una directiva de clasificación de información muestra los diferentes componentes de una organización. A continuación, considera cada tipo de datos que pertenecen a la organización y, posteriormente, clasifica los datos según los derechos de almacenamiento y permiso.

Estos datos pueden ser categorizados como sensibles, públicos, confidenciales o personales. Una política de clasificación de datos también debe tener en cuenta los niveles o categorías de clasificación de datos específicos adoptados por las regulaciones o normas de la industria.

Las políticas de clasificación de datos permiten a las organizaciones aplicar el nivel adecuado de seguridad a los datos, lo que reduce el riesgo general de la empresa.

Ventajas de aplicar las directivas de clasificación de información

Las empresas se benefician de varias maneras del desarrollo de una política de clasificación de datos, como pueden ser:

- Las directivas de clasificación de datos ayudan a una organización a comprender qué datos se pueden usar, su disponibilidad, dónde se encuentran, qué niveles

de acceso, integridad y seguridad se requieren, y si las implementaciones actuales de manejo y procesamiento cumplen o no con las leyes y regulaciones vigentes.

- Es el sistema más eficaz y eficiente para proteger los datos, ya que ayuda a categorizar los datos para proteger la información crítica, confidencial y clasificada. Si los datos confidenciales llegan a las manos equivocadas, las organizaciones pueden ser responsables de sanciones por violar las leyes y regulaciones y pueden sufrir pérdidas financieras o daños a la reputación.
- Las políticas de clasificación de datos ayudan a las organizaciones a cumplir con las normas, así como con las mejores prácticas de la industria y las expectativas de los clientes.
- También ayuda a optimizar los fondos de seguridad designados al permitir que las organizaciones determinen en qué medidas de seguridad invertir en función de la cantidad de datos confidenciales que requieren protección, dónde se encuentran y el panorama de amenazas.

Ejemplos de directivas de clasificación de datos

Ejemplo 1:

Programa: Antecedentes Penales

Sistema de Información: Fuerzas y Cuerpos de Seguridad del Estado

Tipos de información:

- Registros criminales: Información sobre órdenes de arresto.
- Investigación y servicios criminales: Datos relacionados con investigaciones en curso e información resumida sobre investigaciones pasadas.

Tipo de información	Clase de datos	Impacto de la confidencialidad	Impacto de la capacidad de información	Impacto de la capacidad de disponibilidad
Registros criminales	Públicos	Bajo	Medio	Medio
Investigación criminal y servicios	Confidenciales	Alto	Medio	Medio

Ejemplo 2:

Programa: Hospitales

Sistema de información: Sistema de Administración Hospitalaria

Tipos de información:

- Servicios de atención médica: Contiene los registros médicos de todos los pacientes anteriores y actuales.

- Administración de atención médica: Proporciona servicios de facturación y contabilidad en apoyo de las actividades del hospital.
- Control de inventario: Realiza un seguimiento de todos los activos tangibles del hospital desde la adquisición hasta la enajenación.

Tipo de información	Clase de datos	Impacto de la confidencialidad	Impacto de la capacidad de información	Impacto de la capacidad de disponibilidad
Servicios de atención médica	Confidenciales	Alto	Alto	Alto
Administración de atención médica	Confidenciales	Alto	Medio	Medio
Control de inventario	Confidenciales	Alto	Medio	Medio

Recomendaciones a la hora de desarrollar una directiva de clasificación de información

Algunas de las prácticas recomendadas para desarrollar una directiva de clasificación de datos incluyen:

1. **Aprovechar las herramientas automatizadas** que pueden ayudar a agilizar el proceso de clasificación de datos, analizando y categorizando automáticamente los datos en función de parámetros predeterminados.
2. **Identificar el área responsable del programa**, la caracterización del negocio y las necesidades. Para entender la caracterización y las necesidades del negocio, las preguntas clave que se deben hacer incluyen:

- ¿Qué programa recopiló la información?
- ¿Dónde está contenida la información?
- ¿Qué programa es responsable de la integridad de los hechos y la verificación de precisión?
- ¿Qué programa presupuesta los gastos incurridos en la recopilación, el procesamiento, el almacenamiento y la distribución de la información?
- ¿Qué programa ha aprendido más sobre el valor útil de la información?

3. **Establecer una persona Responsable de la Información** cuya función es administrar los registros dentro de la organización.
4. **Realizar evaluaciones regulatorias y legales**. Se debe hacer un trabajo exhaustivo para saber qué ley o reglamento es aplicable a la organización; es importante y no debe pasarse por alto, ya que muchas leyes de seguridad y privacidad hoy en día tienen sanciones económicas elevadas por incumplimiento.

Para las empresas de hoy en día, una política de clasificación de datos sirve como base de medidas de seguridad eficaces. Sin un sistema coherente para clasificar los datos, es imposible proteger adecuadamente los datos confidenciales: después de todo, no se pueden proteger si no se sabe que existen, dónde se encuentran o si requieren protección en absoluto.

8. CONCIENCIACIÓN Y FORMACIÓN

La diferencia entre vulnerabilidad y amenaza es muy interesante, aunque son términos que se confunden a menudo. Veamos cómo se definen:

• Una **vulnerabilidad** (en términos de informática) 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. Estos «agujeros» pueden tener distintos orígenes por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

• Por su parte, una **amenaza** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

Por tanto, las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas. El problema es que en el mundo real, si existe una vulnerabilidad, siempre existirá alguien que intentará explotarla, es decir, sacar provecho de su existencia.

Una vez que tenemos clara la diferencia entre amenaza y vulnerabilidad, es interesante introducir el concepto de riesgo. El riesgo es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus…

El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo.

Algunas de las fuentes de amenazas más comunes en el ámbito de sistemas de información son:

- **Malware o código malicioso**: permite realizar diferentes acciones a un atacante. Desde ataques genéricos mediante la utilización de troyanos, a ataques de precisión dirigidos, con objetivos específicos y diseñados para atacar a un dispositivos, configuración o componente específico de la red.
- **Ingeniería social**: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible

o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.

• **APT o Amenazas Persistentes Avanzadas** (Advanced Persistent Threats): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.

• **Botnets**: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.

• **Redes sociales**: el uso no controlado de este tipo de redes puede poner en riesgo la reputación de la empresa.

• **Servicios en la nube**: una empresa que contrate este tipo de servicios tiene que tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios. Se ha de asegurar de contratarlos con empresas cuya seguridad este demostrada, y firmar SLA o ANS (Acuerdos de Nivel de Servicio) en los que quede definida la seguridad que necesita la empresa.

Algunos incidentes pueden implicar problemas legales que pueden suponer sanciones económicas y daños a la reputación e imagen de la empresa. Por eso, es importante conocer los riesgos, medirlos y evaluarlos para evitar en la medida de lo posible los incidentes, implantando las medidas de seguridad adecuadas.

Malware

Cuando hablamos de amenazas de seguridad a los sistemas de información, hay una entre todas ellas que es recurrente y que ha logrado sobrevivir a más de tres décadas. Ha crecido, evolucionado y se ha adaptado conforme ha ido avanzando la tecnología:

es el código malicioso (malware) o, en lenguaje coloquial más conocido como los «virus».

Actualmente, la variedad es tal, que referirse a estos como «virus» es hablar únicamente de una de las formas que pueden adoptar estos programas. Es más, el término «virus» hace referencia a una característica muy particular, la capacidad para copiarse a sí mismos, de forma similar a como lo hacen los que atacan a organismos biológicos, como es el caso de los virus humanos. Esta analogía con los virus biológicos va más allá de la capacidad de auto replicarse en el sistema atacado, ya que ambos causan daños al sistema que los alberga, se pueden prevenir o incluso eliminar, pero también pueden mutar y evolucionar, adaptándose al medio.

La tipología es muy extensa, tanto como lo son las actividades para las cuales son diseñados. Algunos de los más conocidos son los siguientes:

- **Virus**. Son programas capaces de crear copias de sí mismos, de forma que anexan estas copias a otros programas legítimos o en zonas especiales de soportes de almacenamiento, como en el caso de los discos duros o los sistemas de almacenamiento externo. Necesitan de la intervención del usuario para propagarse, utilizando diversas vías para conseguirlo como ingeniería social, descarga de ficheros, visita a páginas web de dudosa reputación, utilización incorrecta de dispositivos externos de memoria, correo electrónico, etc. Los virus suelen diseñarse para producir todo tipo de problemas en un ordenador, como volverlo más lento, bloquearlo o impedir el acceso a la información.
- **Gusanos**. Son un tipo de código malicioso que se diseñó originalmente para su propagación a través de redes de comunicaciones, mediante el uso de servicios como el correo electrónico. En la actualidad, son capaces de replicarse y propagarse a través de la red sin necesidad de la intervención del usuario, a través de servicios de mensajería instantánea o de redes de intercambio de ficheros (P2P).

Suelen aprovechar las vulnerabilidades de los sistemas operativos o de las aplicaciones instaladas (sobre todo en las que no están debidamente actualizadas), y su velocidad de propagación es muy alta en comparación con los virus, alcanzando además, zonas geográficas muy amplias. En realidad las técnicas de propagación de los gusanos son usadas por otros tipos de código malicioso

- **Troyanos**. Son programas que se ocultan o esconden en programas legítimos, como aplicaciones de ofimática, facturación, documentos de trabajo, fotos, etc. para proporcionar acceso no autorizado al sistema infectado. Su propagación requiere de la acción directa del usuario para su descarga e instalación. Los troyanos se han especializado en el robo de credenciales bancarias y son una de las mayores amenazas en la actualidad, por la proliferación de este tipo de código malicioso, muy utilizado por los ciberdelincuentes. Existen diferentes tipos, en función de la forma en que afectan el comportamiento del equipo infectado:
    - Backdoors, o troyanos de acceso remoto, que proporcionan un acceso total del equipo para que el atacante pueda realizar cualquier tarea en él.
    - Keyloggers, o malware que registra las pulsaciones que realizamos con el teclado, permitiendo averiguar las contraseñas o cualquier otro tipo de información privada que hayamos tecleado.

- Stealers, que acceden y roban información privada almacenada en los equipos para enviárselas al atacante. Información como las contraseñas que se almacenan o memorizan en los diversos programas como navegadores, mensajería instantánea, correo electrónico, etc.
- Ransomware, que tiene como objetivo bloquear y secuestrar el acceso a un equipo de trabajo o a la información que contiene -cifrando el contenido bloqueado-, con el fin de pedir un rescate económico a cambio de su desbloqueo.

- **Spyware**. Son programas destinados a la recolección de información sobre la actividad de un usuario. Están diseñados para pasar inadvertidos, de forma que el usuario no perciba ningún tipo de actividad fuera de lo normal. Cuanto más tiempo pasen sin ser detectados, más información serán capaces de recopilar, que luego es enviada a servidores o direcciones de correo que la recogen y la usan para todo tipo de fines.

- **Adware**. Son programas diseñados para mostrar publicidad al usuario. Suelen ser instalados junto con otros programas legítimos. Estos programas pueden recopilar información sobre la actividad del usuario con objeto de mostrar publicidad dirigida y específica. En general este tipo de aplicaciones son más bien una molestia, pero su instalación puede suponer un peor funcionamiento del ordenador y también, el acceso a sitios y páginas web que pueden contener a su vez código malicioso.

Hoy en día, el malware se ha vuelto muy complejo, hasta el punto de que es difícil clasificarlo o saber cómo actúa, puesto que existen algunos tipos que incorporan características de los virus, pudiendo actuar como un troyano, con las capacidades de propagación de un gusano y recopilando información como si se tratara de spyware. En definitiva, el código malicioso es capaz de propagarse a través de diversas vías y medios y, una vez llega a un sistema, es capaz de realizar múltiples tareas, incluso son capaces de recibir órdenes o funcionar como parte de un grupo de programas maliciosos.

Ingeniería social

Cuando hablamos de ingeniería social realmente hablamos de persuasión, de la capacidad de valerse de la buena voluntad y de la falta de precaución de la víctima.

¿Cuál es su objetivo?

Obtener información: contraseñas, cuentas bancarias, o cualquier dato privado que pudiera ser de interés. En algunas ocasiones esta información es utilizada posteriormente para realizar otro tipo de ataques más sofisticados, en otras ocasiones se vende al mejor postor.

¿Cómo lo hacen?

Suelen hacerse pasar por algún responsable, persona o empresa conocida, para ganarse la confianza de las víctimas. Los medios que suelen utilizar para persuadir suelen variar. Puede ser una visita presencial o una llamada telefónica.

Pero también usan el correo electrónico, las redes sociales o incluso un SMS. Suele ser bastante habitual cuando navegamos por páginas web y se presenta algún tipo de ventana emergente como supuestas peticiones de inicio de sesión legítimas, o incluso nos alertan sobre algo para que hagamos clic sobre un enlace para solucionarlo o ver más información.

¿Cómo proteger mi empresa frente a este tipo de técnicas?

Para protegerse de estas técnicas, la formación y concienciación es una pieza fundamental para saber distinguir estos tipos de mensajes.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Además, podemos adoptar un Plan Director de Seguridad, que va mucho más allá de un mero plan de concienciación y formación interno, pero que sin duda alguna será mucho más efectivo para proteger su principal activo: la información.

Completando las buenas prácticas destinadas a concienciar y formar al personal en materia de seguridad, existen algunas medidas específicas para este tipo de ataques de ingeniería social:

- No abrir correos de usuarios desconocidos o que no hayas solicitado: elimínalos directamente.
- No contestar en ningún caso a los mensajes sospechosos.
- Tener precaución al seguir enlaces en correos electrónicos, SMS, mensajes en WhatsApp o redes sociales, aunque sean de contactos conocidos.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus comprobar que está activo.
- Verificar la seguridad de las páginas web donde introducimos datos personales. Deben utilizar certificado de seguridad y utilizar el protocolo HTTPS.
- Verificar la seguridad de las redes wifi públicas a las que nos conectamos. En caso de dudas, no compartir información confidencial ni introducir credenciales de usuario o contraseñas que puedan ser robados.
- Escribir las URL manualmente, en vez de usar los enlaces de los mensajes sospechosos.

APT o Amenazas Persistentes Avanzadas

Las amenazas persistentes avanzadas, denominadas por sus siglas en inglés Advanced Persistent Threat (APT) son una tipología de ciberataque muy sofisticado. Según el –NIST: National Institute of Standards and Technology (https://www.nist.gov/) – se define así esta tipología de ataque "Una amenaza persistente avanzada es ejecutada por un adversario que posee niveles sofisticados de experiencia e importantes recursos

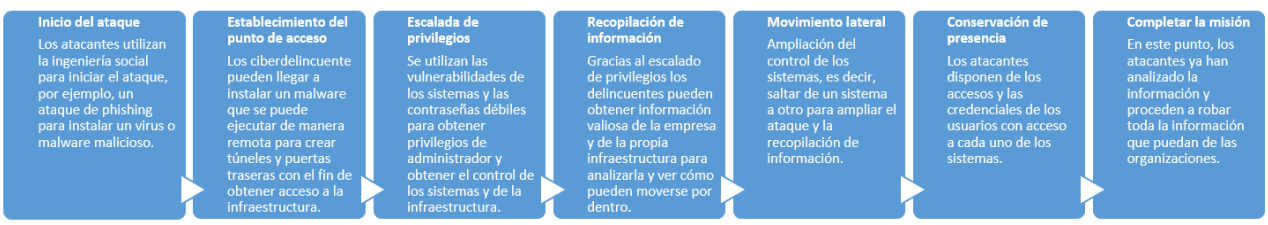
que le permiten crear oportunidades para lograr sus objetivos utilizando múltiples vectores de ataque (por ej: cibernéticos, físicos y engaños).

Estos objetivos, normalmente, incluyen establecer y extender los puntos de apoyo dentro de la infraestructura de IT de las organizaciones atacadas con el propósito de extraer información, perjudicar o dificultar los aspectos críticos de una misión, programa u organización; posicionarse para llevar a cabo estos objetivos en el futuro.

Las amenazas persistentes avanzadas, buscan sus objetivos repetidamente durante un periodo de tiempo prolongado, se adaptan a los esfuerzos de los defensores para resistirlo y se proponen mantener el nivel de interacción necesaria para ejecutar sus objetivos".

Ciclo de vida de las APT

Según diferentes estudios realizados esta tipología de ataques tiene su propio ciclo de vida:



Protección frente a las APT

Las empresas deben afrontar este tipo de incidente de seguridad dentro de su plan de respuesta ante incidentes desde una perspectiva de detección, prevención y respuesta.

A continuación, os dejamos algunos consejos para protegerse de ataques ATP:

• Disponer de un Plan Director de Seguridad y de un análisis de riesgo que tenga en cuenta esta amenaza, para poder analizar para cada empresa cuál es la mejor solución frente un ataque de esta tipología.

• Actualización de todos los dispositivos de la infraestructura.

• Concienciación de todos los empleados para proteger la infraestructura de la organización.

• Disponer de sistemas de doble factor de autenticación para proteger los sistemas y las cuentas de administrador.

• Disponer de sistemas de monitorización de eventos de seguridad que generen alertas para detectar posibles accesos no autorizados

Botnets

Una botnet, o mejor dicho, una red de bots (también conocida como ejército zombi) es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por malware, de forma que quedan a disposición de un hacker. Al tomar el control de cientos o miles de equipos, las botnets se suelen utilizar para enviar spam o virus, para robar información personal o para realizar ataques de denegación de servicio distribuido (DDoS). A día de hoy, se consideran una de las mayores amenazas en Internet.

¿De dónde provienen las botnets?

Para que su equipo forme parte de una botnet, primero es necesario que se infecte con algún tipo de malware que se comunica con un servidor remoto o con otros equipos infectados de la red. De esta forma, recibe instrucciones de quien controla la botnet, normalmente hackers y ciberdelincuentes. A pesar de su gran alcance y envergadura, la infección de malware botnet no es diferente de una infección normal.

¿Cómo se reconocen las botnets?

Puede saberse que un equipo está infectado por una botnet fundamentalmente del mismo modo que se puede identificar que ha sido infectado por cualquier otro tipo de malware. Algunos síntomas pueden ser que el equipo funcione lento, que actúe de forma extraña, que muestre mensajes de error o que su ventilador comience a funcionar de repente mientras está inactivo. Todos estos son síntomas de que alguien puede estar utilizando su equipo de forma remota como parte de una red de bots.

¿Cómo quito mi equipo de una botnet?

Para quitar un equipo de una red botnet, debe desinstalar el software malicioso que lo controla. La mejor forma de hacerlo es realizando un análisis antivirus de su equipo, que debería localizar el malware botnet y eliminarlo. Una solución sencilla para un problema grave.

Cómo evitar el malware botnet:

• Teniendo instalado en nuestro equipo un software antivirus potente y de confianza

• Configurando el software para que se actualice automáticamente

• Teniendo mucho cuidado con dónde hacemos clic, qué descargamos o qué archivos abrimos

VULNERABILIDADES

Como hemos visto, una vulnerabilidad es una debilidad de cualquier tipo que compromete la seguridad del sistema informático.

Se plantea las siguiente cuestion. Normalmente hay más de 20 nuevas vulnerabilidades diarias. Si se anuncia una nueva vulnerabilidad hoy, ¿cuál es su proceso actual para proteger la red?

- Es importante saber si estas vulnerabilidades afectan a la organización.
- Se debe tener un historial de sus vulnerabilidades y su corrección.
- Es clave saber cuándo y cómo fueron corregidas.
- La comunidad informática ha creado bases de datos formales donde se encuentra información crítica como: cuál es vulnerabilidad, a qué sistemas impacta, cómo se activa la vulnerabilidad, cuál es el código que la activa, cómo se corrige la vulnerabilidad.

Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

- **Diseño**
  - Debilidad en el diseño de protocolos utilizados en las redes.
  - Políticas de seguridad deficientes e inexistentes.
- **Implementación**

  - Errores de programación.
  - Existencia de "puertas traseras" en los sistemas informáticos.
  - Descuido de los fabricantes.
- **Uso**
  - Configuración inadecuada de los sistemas informáticos.
  - Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
  - Disponibilidad de herramientas que facilitan los ataques.
  - Limitación gubernamental de tecnologías de seguridad.
- **Vulnerabilidad del día cero**
  - Cuando no exista una solución "conocida" para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como "vulnerabilidad 0 day".

Globalmente clasificamos las vulnerabilidades en:

- **Vulnerabilidades de desbordamiento de buffer**. Se produce cuando un programa no controla la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Se puede aprovechar para ejecutar código que nos de privilegios de administrador.
- **Vulnerabilidades de condición de carrera** (race condition). La condición de carrera se da principalmente cuando varios procesos acceden al mismo tiempo a un recurso compartido, por ejemplo una variable, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma.
- **Vulnerabilidades de error de formato de cadena** (format string bugs).La principal causa de los errores de cadena de formato es aceptar sin validar la entrada de datos proporcionada por el usuario.Es un error de programación y el lenguaje más afectado es C/C++. Un ataque puede conducir de manera inmediata a la ejecución de código arbitrario y a revelación de información.

- **Vulnerabilidades de Cross Site Scripting** (XSS). Abarcaban cualquier ataque que permitiera ejecutar scripts como VBScript o JavaScript, en el contexto de otro sitio web. Estos errores se pueden encontrar en cualquier aplicación que tenga como objetivo final presentar la información en un navegador web. Un uso de esta vulnerabilidad es hacer phishing. La víctima ve en la barra de direcciones un sitio, pero realmente está en otro. La víctima introduce su contraseña y se la envía al atacante.
- **Vulnerabilidades de Inyección SQL**. Una inyección SQL se produce cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.
- **Vulnerabilidades de denegación del servicio**. La denegación de servicio provoca que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.
- **Vulnerabilidades de ventanas engañosas** (Window Spoofing). Las ventanas engañosas son aquellas que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que des información. Hay otro tipo de ventanas que, si las sigues, obtienen datos del ordenador para luego realizar un ataque.
-

Algunos portales importantes son:

http://www.securityfocus.com/

Es una de las bases de datos mas consultadas por los profesionales en seguridad informática por el contexto técnico aportado.

http://www.osvdb.org/

Esta base de datos tiene la mejor información sobre vulnerabilidades en el software open source.

http://secunia.com/

Secunia, tienen las mejores estadísticas de la aparición de vulnerabilidades por sistema operativo.

http://www.kb.cert.org/vuls/

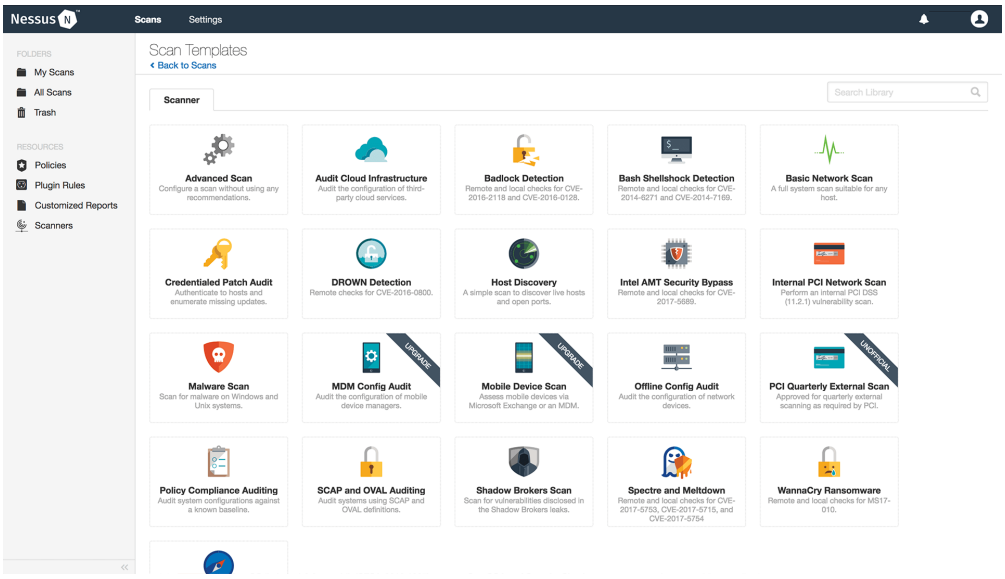
Al igual que securityfocus, es una de las bases de datos más consultadas por los profesionales en seguridad informática por el contexto técnico aportado**.**

Herramientas más conocidas para analizar vulnerabilidades

En el caso de servidores Linux/Unix para hacer el análisis de vulnerabilidades se utiliza el programa 'Nessus'.

Nessus es de arquitectura cliente-servidor OpenSource, dispone de una base de datos de patrones de ataques para lanzar contra una máquina o conjunto de máquinas con el objetivo de localizar sus vulnerabilidades.

Existe software comercial que utilizan Nessus como motor para el análisis. Por ejemplo está Catbird (www.catbird.com) que usa un portal para la gestión centralizada de las vulnerabilidades, analiza externamente e internamente la red teniendo en cuenta los accesos inalámbricos. Además hace monitoreo de servicios de red como el DNS y la disponibilidad de los portales web de las organizaciones.



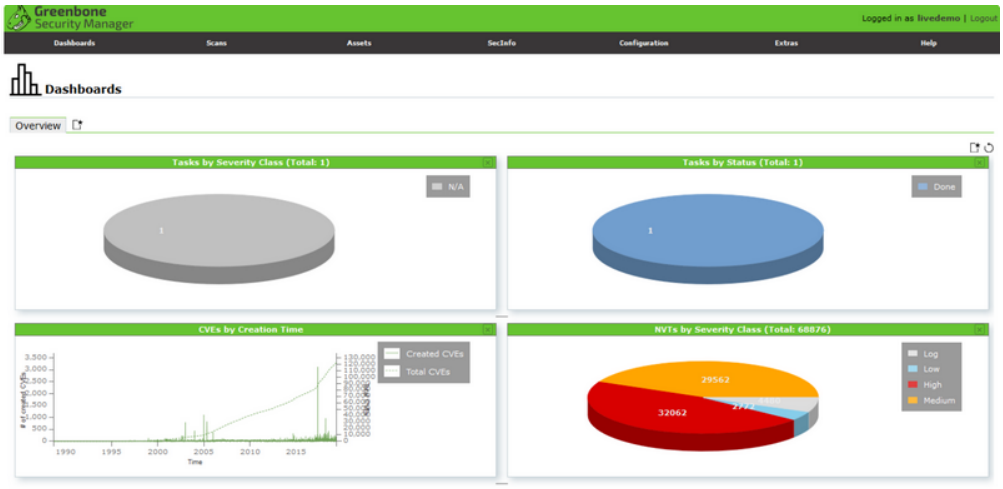
OpenVAS es otro escáner de vulnerabilidades con todas las funciones que podemos esperar encontrar en un software de este tipo. Sus principales características son: pruebas no autenticadas, pruebas autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.

El escáner viene con un gran catálogo de pruebas de vulnerabilidad con un largo historial y actualizaciones diarias. Por ejemplo, este feed comunitario de Greenbone incluye más de 50,000 pruebas de vulnerabilidad.

El escáner se desarrolla y mantiene por Greenbone Networks desde 2009. Los trabajos son provisionados como Código Abierto a la comunidad bajo la Licencia Pública General de GNU (GNU GPL).

Greenbone desarrolla OpenVAS como parte de una familia de productos de gestión de vulnerabilidad comercial conocido como "Greenbone Security Manager" (GSM). OpenVAS es solo una parte de un elemento en una arquitectura más grande. En

combinación con módulos adicionales de código abierto, forma la solución Greenbone Vulnerability Management .



9. CONTINUIDAD DE NEGOCIO

Es fácil relacionar el término continuidad de negocio con el ámbito tecnológico o con las grandes corporaciones. Pero, por una parte la continuidad de negocio no es exclusiva de las TIC, aunque sí sean una parte de la misma.

Por otra parte, los desastres afectan igualmente a las pymes y a los autónomos. Todas las empresas deben tener en cuenta cuáles podrían ser las consecuencias de una parada en la producción o en la actividad diaria.

Cualquier empresa, con independencia de su tamaño o su sector, debe estar preparada para prevenir, protegerse y reaccionar ante incidentes de seguridad que puedan afectar e impactar directamente a su negocio.

Cada organización tendrá que analizar distintos aspectos relacionados con su funcionamiento, incluidos los vinculados a las TIC, priorizar y determinar los límites de funcionamiento aceptable y establecer las medidas necesarias que garanticen la continuidad de la actividad en caso de incidente o desastre, minimizando las consecuencias del mismo.

Por este motivo os proponemos diseñar un Plan de Continuidad de Negocio que comprenda planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía. El proceso y puesta en marcha se debe realizar atendiendo a las siguientes fases.

Fase 0. Determinación del alcance

Se trata de la fase con menor duración y presenta una necesidad de recursos baja. No obstante, su ejecución es imprescindible ya que aquí se determinarán qué activos, sistemas o procesos son críticos, es decir, aquellos cuya indisponibilidad impactaría directamente sobre nuestra organización, causando un cese imprevisto de la actividad.

Fase 1. Análisis de la organización

Esta fase basa su actividad en obtener, elaborar o comprender las circunstancias que rodean a nuestra organización, analizando tanto procesos, como tecnologías o recursos. Para conseguir esta panorámica, deberemos llevar a cabo un conjunto de tareas.

Mantener reuniones

En primer lugar, será necesario reunirse con los usuarios finales de los procesos seleccionados como críticos o que entran dentro de nuestro alcance, recopilando toda la información sobre el funcionamiento de dichos proceso. Por ejemplo, conocer si se realizan copias de seguridad, tanto de datos como de aplicaciones, cada cuánto tiempo, tiempos de respuesta en caso de tener subcontratado este servicio, etc.

Análisis de impacto sobre el Negocio.

A partir de la información recopilada, realizaremos un Análisis de Impacto sobre el Negocio, también conocido como BIA, por sus siglas en inglés, Business Impact Analysis. Este documento contendrá los requerimientos, tanto temporales como de recursos, de los procesos que se encuentren dentro del alcance del proyecto:

- *Tiempo de recuperación*, RTO (Recovery Time Objective), o tiempo que un proceso permanece detenido hasta ser restaurado.
- *Recursos humanos y tecnologías empleadas*, para que un proceso funcione en una situación de contingencia.
- *Tiempo máximo tolerable de caída del servicio* o MTD (Maximun Tolerable Downtime). Es decir, el tiempo que un proceso puede permanecer caído antes de que se produzcan consecuencias desastrosas para la organización.
- *Niveles mínimos de recuperación del servicio* o ROL (Revised Operating Level). Este sería el nivel mínimo de recuperación que debe tener una actividad para que se considere recuperada.

- *Dependencias con otros procesos*, ya sean internos o con proveedores externos. Se trata de saber si una situación de contingencia en otros procesos o en un proveedor externo se trasladaría a nuestra empresa.
- *Grado de dependencia de la actualidad de los datos* o RPO (Recovery Point Objetive). Se determina el impacto que tendría sobre nuestra actividad la pérdida de datos.

Con esta información, podremos determinar qué procesos y aplicaciones son prioritarios a la hora de ser recuperados, así como la necesidad de contar, por ejemplo, con copias de seguridad.

Análisis de riesgos.

Consiste en estudiar y determinar las posibles amenazas a las que está expuesta la organización, así como las posibilidades de materializarse en cada caso, y el impacto que causarían si llegaran a producirse.

Una vez extraídas las conclusiones, se realizará un plan de tratamiento de riesgos en el que se describan medidas, riesgo que mitiga, responsables de implantación, recursos necesarios, etc.

Fase 2. Determinación de la Estrategia de Continuidad

Esta fase se basa en determinar qué estrategias de recuperación se deberán implementar para cada uno de los elementos identificados como críticos o que pudieran verse afectados en una contingencia. Es decir, cómo recuperar un sistema o un proceso para evitar que la contingencia lo degrade de manera irreversible para la organización. Hay que tener en cuenta que algunos procesos podrán requerir varias estrategias de recuperación.

Fase 3. Repuesta a la contingencia

En esta fase se comienza con la implantación de las iniciativas que se han puesto de manifiesto en la fase anterior. Además, se deberá abordar toda la documentación relacionada con la respuesta a la contingencia, a través de los siguientes documentos:

- *Plan de crisis* cuyo objetivo es evitar una toma de decisiones improvisada que pueda empeorar la situación o bien que simplemente no se tomen decisiones.
- *Planes operativos de recuperación de entornos*, que deberán especificar sobre qué entorno se aplican. Hay que tener en cuenta que estos documentos podrán abarcar uno o varios entornos, y contendrán información específica de cada uno de ellos. Por ejemplo, un entorno puede ser un ERP, otro el correo electrónico, etc.
- *Procedimientos técnicos de trabajo*, donde se describen las acciones que se han de llevar a la práctica para la gestión y recuperación de un sistema, infraestructura o entorno.

Fase 4. Prueba, mantenimiento y revisión

Para que un Plan de Continuidad sea eficaz, deberemos comprobar que realmente funciona y mantenerlo actualizado. Para ello, habrá que ejecutar una serie de pruebas sobre los entornos identificados, tras las cuales elaboraremos unos informes que recojan los resultados obtenidos.

Además, deberán quedar reflejados todas las incidencias surgidas en este proceso, algo indispensable para poder establecer medidas correctoras.

Fase 5. Concienciación

Que la concienciación forme parte de la última fase no implica que sea menos importante que las predecesoras. En esta fase se pondrán en marcha todo tipo de medidas que fomenten la concienciación del personal en materia de continuidad y el conocimiento de los planes elaborados. El público objetivo será tanto personal técnico como de negocios, si tienen algún tipo de relación con el alcance.

Con independencia del sector o del tamaño, cualquier organización debe estar preparada para afrontar con garantías un incidente de seguridad que pueda afectar al desarrollo de sus actividades.

Establecer una serie de medidas dirigidas a minimizar el impacto que pueda tener cualquier tipo de contingencia sobre el negocio proporcionará mayor seguridad y capacidad de respuesta ante cualquier eventualidad.

10. CUMPLIMIENTO LEGAL

Para abordar la ciberseguridad o la seguridad de la información es importante considerar la legislación vigente en la materia, es decir, los requisitos legales de ciberseguridad.

La norma "ISO/IEC 27001. Sistema de gestión de la seguridad de la información (SGSI)" alude expresamente a considerar los citados requisitos legales en los siguientes apartados:

- *Apartado 2*. Comprensión de las necesidades y expectativas de las partes interesadas
- *Apartado 8.2.1.* Clasificación de la información
- *Apartado 18.1.* Cumplimiento de los requisitos legales y contractuales

Código de Derecho de la Ciberseguridad

¿Pero cuáles son estos requisitos legales de ciberseguridad? ¿Y cuáles aplican a mi organización? ¿Y si cambian?

En España es recomendable basarse en el *"Código de Derecho de la Ciberseguridad"*.

Los códigos electrónicos contienen compilaciones de las principales normas vigentes del ordenamiento jurídico, permanentemente actualizadas, presentadas por ramas del Derecho. Se complementan con un sistema de alertas de actualización cuya suscripción se puede realizar a través de los servicios de Mi BOE.

Con Mi BOE, puede suscribirse de manera gratuita a nuestros servicios de alerta y recibir puntualmente información por correo electrónico sobre las novedades publicadas en materias de su interés.

El pasado 12 de noviembre de 2020 fue actualizado el "Código de Derecho de la Ciberseguridad".

Los cambios en los requisitos legales de ciberseguridad fueron los siguientes:

- Modificaciones en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- La inclusión de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- La derogación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Requisitos legales de ciberseguridad

El "Código de Derecho de la Ciberseguridad" está formado por esta legislación o requisitos legales de ciberseguridad:

CONSTITUCIÓN ESPAÑOLA

Constitución Española (parcial)

NORMATIVA DE SEGURIDAD NACIONAL

- Ley de Seguridad Nacional
- Consejo Nacional de Ciberseguridad
- Mecanismos para garantizar funcionamiento integrado Sistema de Seguridad Nacional
- Estrategia de Seguridad Nacional
- Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Reglamento de Evaluación y Certificación de Seguridad de Tecnologías de la Información
- Comité de Seguridad de los Sistemas de Información de la Seguridad Social
- Comité de Seguridad de las Tecnologías de la Información
- Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
- Real Decreto-ley de seguridad de las redes y sistemas de información
- Ley reguladora del Centro Nacional de Inteligencia
- Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia
- Ley sobre secretos oficiales
- Desarrollo de las disposiciones de la Ley sobre Secretos Oficiales
- Ley Orgánica de los estados de alarma, excepción y sitio
- Ley de Secretos Empresariales
- Estrategia Nacional de Ciberseguridad 2019

INFRAESTRUCTURAS CRÍTICAS

- Ley que establece medidas para la protección de las infraestructuras críticas
- Reglamento de protección de las infraestructuras críticas

- Contenidos de Planes de Seguridad del Operador y de Planes de Protección Específicos

NORMATIVA DE SEGURIDAD

- Servicios Centrales y Periféricos de la Dirección General de la Policía (parcial)
- Ley Orgánica de protección de la seguridad ciudadana
- Ley de Seguridad Privada
- Reglamento de Seguridad Privada

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD

- Ley de servicios de la sociedad de la información y de comercio electrónico (parcial)
- Centro Criptológico Nacional
- Organización básica de las Fuerzas Armadas (parcial)
- Desarrollo de la organización básica del Estado Mayor de la Defensa (parcial)

TELECOMUNICACIONES Y USUARIOS

- Ley de servicios de la sociedad de la información y de comercio electrónico
- Medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos
- Distintivo público de confianza en los servicios de la sociedad de la información
- Ley de acceso electrónico de los ciudadanos a los Servicios Públicos
- Desarrollo parcial de la Ley de acceso electrónico de los ciudadanos a los servicios públicos
- Ley reguladora de determinados aspectos de los servicios electrónicos de confianza

- Expedición del documento nacional de identidad y sus certificados de firma electrónica
- Ley General de Telecomunicaciones
- Reglamento sobre el uso del dominio público radioeléctrico
- Protección del dominio público radioeléctrico
- Ley de conservación de datos relativos a comunicaciones electrónicas y redes públicas
- Formato de entrega datos conservados por los operadores

CIBERDELINCUENCIA

- Ley Orgánica del Código Penal (parcial)
- Ley Orgánica reguladora de la responsabilidad penal de los menores (parcial)
- Ley de Enjuiciamiento Criminal (parcial)

PROTECCIÓN DE DATOS

- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Reglamento de la Ley Orgánica de protección de datos de carácter personal
- Reglamento Europeo relativo a protección en el tratamiento de datos personales

RELACIONES CON LA ADMINISTRACIÓN

- Ley del Procedimiento Administrativo Común de las Administraciones Públicas (parcial)
- Ley de Régimen Jurídico del Sector Público (parcial)

¿Cómo procederemos ante un incidente?

Como hemos visto, existe una multitud de leyes, reglamentos, esquemas y medidas relativas a los incidentes de seguridad. Para ello vamos a resumir brevemente cómo actuar.

Cuando sucede un incidente de este tipo, se ha de activar el plan de actuación, mediante el despliegue preciso y ágil de acciones y tareas específicas dirigidas a la resolución o minimización de la brecha, a la mitigación de las consecuencias negativas a personas y sistemas de información y datos personales y a la evitación futura de situaciones de riesgo o impacto.

El plan de actuación ante brechas de seguridad recoge un contenido necesario y útil para decidir las medidas a adoptar y las acciones a desplegar, así como para la importante valoración de la necesidad de notificar a las autoridades de control y personas afectadas.

Entre las medidas y las acciones a desplegar, de acuerdo con las principales autoridades y expertos, destacamos las siguientes:

SUJETOS IMPLICADOS

Responsable del tratamiento (la persona física o jurídica que decide fines y medios del tratamiento de datos personales):

- Para aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD.
- Para valorar notificar la brecha de seguridad a la autoridad de control competente, sin dilación indebida, y en su caso la comunicación con los afectados.

Expertos en seguridad:

- Para la gestión técnica, tecnológica o informática del incidente.
- Para facilitar toda aquella información mínima y necesaria para la posible comunicación de la brecha de seguridad a la autoridad de control.

Delegado de Protección de Datos (DPD), sea obligatorio o voluntario. Ocupará un papel muy relevante para liderar el plan de actuación en todos sus aspectos.

Autoridad de control competente*:* se encargará de verificar que se cumple con el RGPD, y particularmente respecto a la gestión de la brecha de seguridad.

ACCIONES Y MEDIDAS

- Recopilación y análisis de la información relativa al incidente de seguridad (en particular, las dimensiones de integridad, disponibilidad, seguridad y privacidad).
- Clasificación del incidente de seguridad.

- Determinación objetiva de si efectivamente se está ante una brecha de seguridad.
- Investigación, comunicación y coordinación de los medios internos/externos implicados.
- Puesta en marcha del plan de respuesta (medidas de contención y de limitación de daños).
- Puesta en marcha del proceso de notificación, previa valoración de notificación temprana a la autoridad de control competente, a afectados y en caso necesario a fuerzas de seguridad.
- Proceso de respuesta: contención, solución/erradicación, recolección y custodia de evidencias, terminación y recuperación; comunicación/Informe de resolución (interna/externa).
- Proceso de notificación: valoración, gestión, notificación a autoridad de control y comunicación a afectados.

SEGUIMIENTO Y CIERRE

- Valoración de contratación de un análisis forense digital experto.
- Valoración de adopción de medidas jurídicas y procesales.
- Realización de un informe final sobre la brecha de seguridad.
- Cierre del incidente de seguridad.

NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

El RGPD establece la obligación de notificación de la violación de la seguridad de los datos personales a la autoridad de control competente (art. 33). En consecuencia, de ser efectiva una violación de la seguridad de los datos personales, el responsable del tratamiento (su empresa, fundación, asociación o administración pública) tiene la obligación de notificarla a la autoridad de control competente.

Y lo hará sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de la brecha de seguridad. No obstante, si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos en los que se funde la dilación.
Como excepción a dicha obligación se contempla el caso de escasa o nula probabilidad de dicha violación de seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Sin embargo, adicionalmente el RGPD obliga a que, cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida (art. 34).

También existe una herramienta de la Agencia Española de Portección de Datos (AEPD) en la que podemos ver si realmente debemos comunicar una brecha de seguridad sufrida en nuestra empresa o negocio.

Está disponible en la siguiente dirección web:

https://servicios.aepd.es/Comunica

La AEPD destaca que la política de notificaciones de brechas de seguridad se debe tener en cuenta con el fin de disponer de un criterio común a todos los tratamientos de datos personales que consten en el registro de actividades de tratamiento de una organización.

Guía para la notificación de brechas de datos personales

Enlace a la GUIA

Para facilitar una visión de conjunto del contenido y procedimiento ante la autoridad de control española, la notificación de la violación de la seguridad ha de contener los siguientes extremos:

1. Identificación del proveedor
2. Identidad y datos de contacto del responsable de protección de datos u otro punto de contacto en el que pueda obtenerse información
3. Indicación de si se trata de una primera o segunda comunicación

4. Fecha del incidente
5. Circunstancias en que se ha producido la quiebra
6. Naturaleza y contenido de los datos personales afectados
7. Medidas técnicas y de organización
8. Otros proveedores que intervienen en los servicios afectados
9. Resumen del incidente
10. Número exacto o estimado de abonados o particulares afectados
11. Posibles consecuencias y efectos negativos en los abonados o particulares
12. Medidas técnicas y organizativas adoptadas para paliar los posibles efectos negativos
13. Posible notificación adicional a los abonados o particulares
14. Medios de comunicación utilizados para la notificación
15. Número de abonados o particulares destinatarios de la notificación
16. Quiebra que afecta a abonados o particulares de otros estados miembros
17. Notificación a otras autoridades nacionales competentes

Además de tener en cuenta las obligaciones de notificación establecidas por la AEPD para las brechas de seguridad, en función de que la entidad haya designado o no Delegado de Protección de Datos (DPD), será recomendable contar con la opinión experta de especialistas jurídicos para valorar la necesidad de efectuar la notificación de la violación de seguridad, así como planificar las acciones y medidas a adoptar por el Responsable de Tratamiento.

CINCO MEDIDAS PRÁCTICAS DE SEGURIDAD

El Reglamento General de Protección de Datos y, en España, la Ley Orgánica 3/2018 promueven una cultura de gestión diligente de los datos personales por los responsables y encargados del tratamiento, a fin de minimizar el impacto sobre los afectados de los incidentes de seguridad y, en virtud del principio de responsabilidad

proactiva, "aprender de las brechas" mediante la determinación de los fallos en los procedimientos de gestión de la información.

Así, dado que la privacidad puede verse afectada por incidentes de confidencialidad, integridad y disponibilidad, deben aplicarse medidas de seguridad básicas para hacer frente a estos desafíos. De acuerdo con la AEPD, destacamos cinco:

1. Uso de contraseñas seguras y segundo factor de autenticación.
2. Copias de seguridad, para hacer frente al secuestro de información y datos personales.
3. Sistemas actualizados, para la aplicación de las medidas de seguridad.
4. Política estricta de servicios expuestos en Internet, para evitar o minimizar accesos remotos no autorizados.
5. Cifrados de dispositivos portátiles, frente al acceso por extravío o robo.

11. PLAN DIRECTOR DE SEGURIDAD.

Detección

Es un hecho que a pesar de las medidas que implantemos, siempre existe el riesgo de que ocurra un incidente de ciberseguridad. Por ello, debemos preparar un plan de acción que nos indique cómo actuar de la manera más eficaz posible en estos casos.

Existen muchos tipos de incidentes de ciberseguridad, algunos son más habituales que otros que podrían encajar en una de las siguientes tipologías:

- incidentes no intencionados o involuntarios
- daños físicos
- incumplimiento o violación de requisitos y regulaciones legales
- fallos en las configuraciones
- denegación de servicio
- acceso no autorizado, espionaje y robo de información
- borrado o pérdida de información
- infección por código malicioso

Para ejecutar correctamente el plan y evitar que el daño se extienda se deben detallar las acciones a realizar en cada momento, la lista de las personas involucradas y sus responsabilidades, los canales de comunicación oportunos, etc.

Tras un incidente, si hemos aplicado el plan, tendremos una valiosa información para conocer y valorar los riesgos existentes, y así evitar incidentes similares en el futuro.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

En caso de que ocurran incidentes graves o desastres que paralicen nuestra actividad principal, aplicaremos el plan de contingencia y continuidad del negocio.
El objetivo principal será asegurarnos de que todos los miembros de la organización conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información.

Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la empresa. También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

Análisis de riesgos

Al considerar si una situación es un incidente o un desastre, una buena regla es evaluar la gravedad del evento y la probabilidad de que termine rápidamente. Un incidente es un evento que puede ser, o puede llevar a, una interrupción, trastorno, pérdida o crisis de negocios.

Por ejemplo, un incidente podría ser algo tan simple como una tubería con fugas, pero si la tubería explota, la situación puede convertirse rápidamente en un desastre. La introducción de un virus en una red se trataría inicialmente como un incidente de ciberseguridad, ya que se supone que puede abordarse rápidamente con varias herramientas de software y técnicas de seguridad. Sin embargo, si el virus demuestra ser un ataque importante de denegación de servicio, el incidente puede convertirse rápidamente en un desastre si se interrumpe el negocio.

El análisis de riesgos es uno de los trabajos más importantes a la hora de definir proyectos e iniciativas para la mejora de la seguridad de la información. Si consideramos que las herramientas tecnológicas y la información que manejamos son de gran valor para nuestra organización debemos empezar a pensar en poner en práctica un *Plan Director de Seguridad*.

El *Plan Director de Seguridad (PDS)* se puede simplificar como la definición y priorización de un conjunto de proyectos en materia de seguridad de la información, dirigido a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables a partir de un análisis de la situación inicial.

Llevar a cabo un buen análisis nos permitirá centrar nuestro foco de atención en los riesgos asociados a los sistemas, procesos y elementos dentro del alcance del PDS. De esta forma mitigaremos la posibilidad de tener algún tipo de incidente de ciberseguridad. Por otra parte, también podemos obtener beneficios si realizamos un análisis de riesgos de forma aislada en lugar de llevarlo a cabo dentro de un contexto mayor como es el del desarrollo de un PDS.

A continuación, veremos de forma sencilla las principales tareas del análisis de riesgos, aportando recomendaciones prácticas sobre cómo llevarlo a cabo, y considerando algunas particularidades a tener en cuenta para que aporte el máximo valor al PDS.

Cabe señalar que las fases o etapas que componen un análisis de riesgos dependen de la metodología escogida. En el caso que nos ocupa, hemos seleccionado un conjunto de fases que son comunes en la mayor parte de las metodologías para el análisis de riesgos.

Fase 1. Definir el alcance

El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio. Vamos a considerar que este análisis de riesgos forma parte del Plan Director de Seguridad.

Por lo tanto, recomendamos que el análisis de riesgos cubra la totalidad del alcance del PDS, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad.

Por otra parte, también es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas.

Por ejemplo, análisis de riesgos sobre los procesos del departamento Administración, análisis de riesgos sobre los procesos de producción y gestión de almacén o análisis de riesgos sobre los sistemas TIC relacionados con la página web de la empresa, etc.

En este caso práctico consideramos que el alcance escogido para el análisis de riesgos es “Los servicios y sistemas del Departamento Informática”.

Fase 2. Identificar los activos

Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. Para mantener un inventario de activos sencillo puede ser suficiente con hacer uso de una hoja de cálculo o tabla como la que se muestra a continuación a modo de ejemplo:

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
1	SERVER1	Servidor datos	Dpto. Informática	Servidor físico	CPD	Sí
2	ROUTERWIFI	Router wifi clientes	Dpto. Informática	Router Físico	Sala Reuniones	No
3	SERVER2	Servidor Web	Dpto. Marketing	Servidor virtual	CPD Externo	Si
…						

Fase 3. Identificar / seleccionar las amenazas

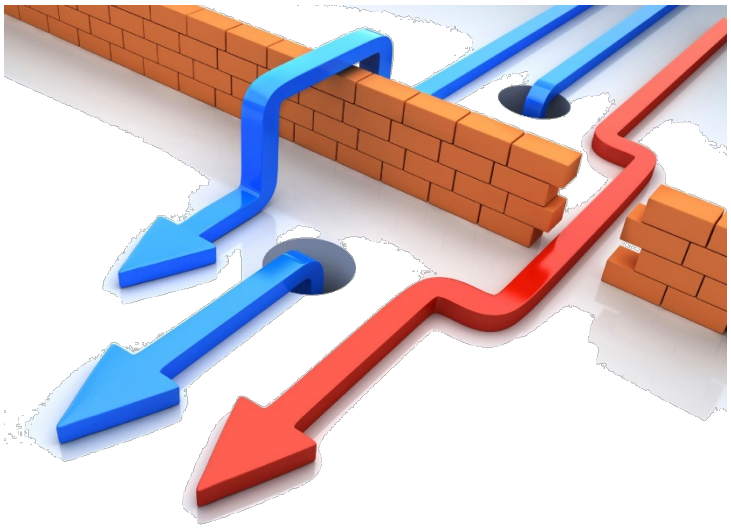
Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado.

Por ejemplo, si nuestra intención es evaluar el riesgo que corremos frente a la destrucción de nuestro servidor de ficheros, es conveniente, considerar las averías del servidor, la posibilidad de daños por agua (rotura de una cañería) o los daños por fuego, en lugar de plantearnos el riesgo de que el CPD sea destruido por un meteorito.

Fase 4. Identificar vulnerabilidades y salvaguardas

La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser identificar un conjunto de ordenadores o servidores cuyos sistemas antivirus no están actualizados o una serie de activos para los que no existe soporte ni mantenimiento por parte del fabricante. Posteriormente, a la hora de evaluar el riesgo aplicaremos penalizaciones para reflejar las vulnerabilidades identificadas.

Por otra parte, también analizaremos y documentaremos las medidas de seguridad implantadas en nuestra organización. Por ejemplo, es posible que hayamos instalado un sistema SAI (Sistema de Alimentación Ininterrumpida) o un grupo electrógeno para abastecer de electricidad a los equipos del CPD. Ambas medidas de seguridad (también conocidas como salvaguardas) contribuyen a reducir el riesgo de las amenazas relacionadas con el corte de suministro eléctrico.



Estas consideraciones (vulnerabilidades y salvaguardas), debemos tenerlas en cuenta cuando vayamos a estimar la probabilidad y el impacto como veremos en la siguiente fase.

Fase 5. Evaluar el riesgo

Llegado a este punto disponemos de los siguientes elementos:

- Inventario de activos.
- Conjunto de amenazas a las que está expuesta cada activo.
- Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).
- Conjunto de medidas de seguridad implantadas

Con esta información, nos encontramos en condiciones de calcular el riesgo. Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos. Pero para entenderlo mejor, veremos a modo de ejemplo las tablas para estimar los factores probabilidad e impacto.

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Tabla para el cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Media	2	El daño derivado de la materialización de la amenaza tiene consecuencias relevantes para la organización.
Alta	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.

Tabla para el cálculo del impacto

Cálculo del riesgo

A la hora de calcular el riesgo, si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto:

RIESGO = PROBABILIDAD x IMPACTO

Si por el contrario hemos optado por el análisis cualitativo, haremos uso de una matriz de riesgo como la que se muestra a continuación:

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy Bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy Alto

Tal y como indicábamos en el apartado anterior, cuando vayamos a estimar la probabilidad y el impacto debemos tener en cuenta las vulnerabilidades y salvaguardas existentes.

Por ejemplo, la caída del servidor principal podría tener un impacto alto para el negocio. Sin embargo, si existe una solución de alta disponibilidad (Ej. Servidores redundados), podemos considerar que el impacto será medio ya que estas medidas de seguridad harán que los procesos de negocio no se vean gravemente afectados por la caída del servidor.

Si por el contrario hemos identificado vulnerabilidades asociadas al activo, aplicaremos una penalización a la hora de estimar el impacto.

Por ejemplo, si los equipos de climatización del CPD no han recibido el mantenimiento recomendado por el fabricante, incrementaremos el impacto de amenazas como *"condiciones ambientales inadecuadas"* o *"malfuncionamiento de los equipos debido a altas temperaturas"*.

Fase 6. Tratar el riesgo

Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido.

Por ejemplo, trataremos aquellos riesgos cuyo valor sea superior a "4" o superior a "Medio" en caso de que hayamos hecho el cálculo en términos cualitativos.

A la hora de tratar el riesgo, existen cuatro estrategias principales:

- *Transferir el riesgo a un tercero*. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
- *Eliminar el riesgo*. Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
- *Asumir el riesgo*, siempre justificadamente. Por ejemplo, el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
- *Implantar medidas para mitigarlo*. Por ejemplo, contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.

Por último, cabe señalar que como realizamos este análisis de riesgos en el contexto de un PDS, las acciones e iniciativas para tratar los riesgos pasarán a formar parte del mismo.

Por lo tanto, deberemos clasificarlas y priorizarlas considerando el resto de proyectos que forman parte del PDS. Asimismo, tal y como indicábamos en la introducción, llevar a cabo un análisis de riesgos nos proporciona información de gran valor y contribuye en gran medida a mejorar la seguridad de nuestra organización.

Análisis

El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis, que debe ser realizado por un perito informático, puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad.

¿En qué consiste un análisis forense?

El análisis forense tiene como objetivo la adquisición de datos y el aseguramiento de prueba electrónica. Se debe obtener el elemento que se quiere analizar manteniendo una cadena de custodia y garantizando la posibilidad de comprobar los requisitos por cualquiera de las partes de un proceso judicial.

Del análisis de datos se extraen una serie de conclusiones que serán entregados al cliente y, si fuese necesario, defendidos ante un juzgado.

Tanto desde el punto de vista teórico, como desde el práctico, nos podemos encontrar con diferentes tipos de análisis:

- ***Sistemas***. En este análisis se tratarán los incidentes de seguridad acaecidos en servidores y estaciones de trabajo con los sistemas operativos.
- ***Redes***. En este tipo se engloba el análisis de diferentes redes: cableadas, wireless, bluetooth, etc.
- ***Sistemas embebidos***. En dicho tipo se analizarán incidentes acaecidos en dispositivos móviles como smarphones, tablets, PDA, etc.

El análisis forense digital nos brinda las técnicas y los principios imprescindibles para desarrollar una investigación que nos posibilite identificar, recuperar, reconstruir y analizar las evidencias de lo sucedido.
Todo ello, una vez se ha producido el delito relacionado con las tecnologías de la información y las comunicaciones.

Fases del análisis forense digital

En un análisis forense digital pueden identificarse las siguientes fases:

1. Adquisición.

En esta fase se obtienen copias de la información que se sospecha que puede estar vinculada con algún incidente. De este modo, hay que evitar modificar cualquier tipo de dato utilizando siempre copias bite a bite con las herramientas y dispositivos adecuados. Cabe aclarar este tipo de copia es imprescindible, debido a que nos dejara recuperar archivos borrados o particiones ocultas, arrojando como resultado una imagen de igual tamaño al disco estudiado.

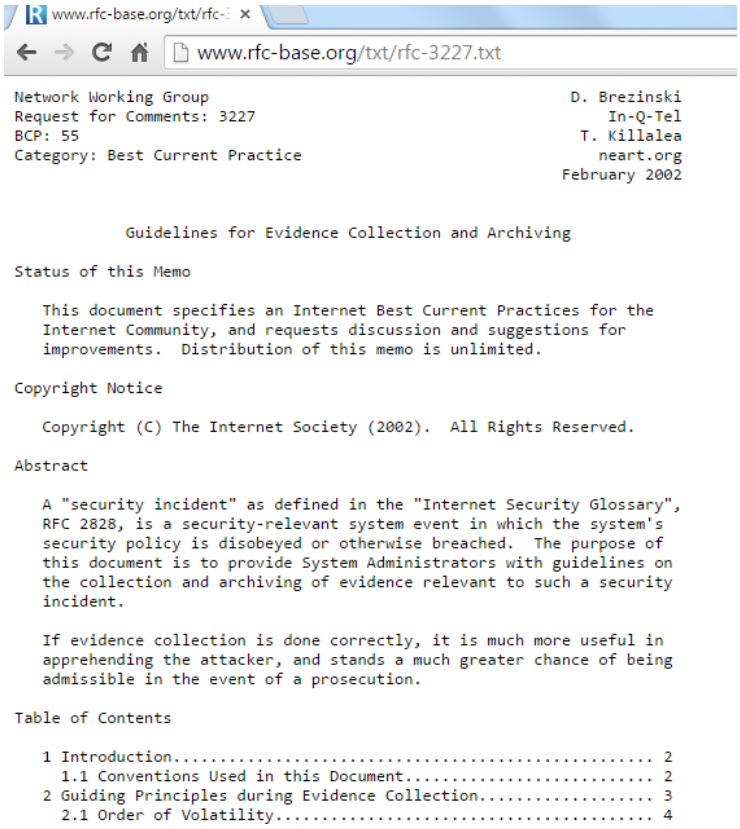
Rotulando con fecha y hora acompañado del uso horario, las muestras deberán ser aisladas en recipientes que no permitan el deterioro ni el contacto con el medio. En muchos casos, esta etapa es complementada con el uso de fotografías con el objetivo de plasmar el estado de los equipos y sus componentes electrónicos.

Recomendamos la utilización de guantes, bolsas antiestáticas y jaulas de Faraday para depositar dispositivos que puedan interaccionar con ondas electromagnéticas como son los celulares.

La adquisición de muestras debe respetar una regla fundamental que está ligada a la volatilidad de las muestras, por lo que se deberán recolectar en el orden de la más volátil en primera instancia a la de menos, sobre el final. A modo de ejemplo, podríamos indicar que primero deberíamos recolectar datos relevantes a la memoria, contenidos del caché y como último paso recolectar el contenido de documentos o información que esté disponible en el soporte de almacenamiento.

Para darle mayor relevancia, podemos consultar las Request for Comments, más conocidos por sus siglas RFC, son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento

de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. De esta forma consultando la RFC 3227, podremos apreciar con mayor profundidad todo lo relativo a esta etapa.



www.rfc-base.org/txt/rfc-3227.txt

Network Working Group — D. Brezinski
Request for Comments: 3227 — In-Q-Tel
BCP: 55 — T. Killalea
Category: Best Current Practice — neart.org
February 2002

Guidelines for Evidence Collection and Archiving

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

Table of Contents

1 Introduction..... 2
1.1 Conventions Used in this Document..... 2
2 Guiding Principles during Evidence Collection..... 3
2.1 Order of Volatility..... 4

2. Preservación

En esta etapa se debe garantizar la información recopilada con el fin de que no se destruya o sea transformada. Es decir que nunca debe realizarse un análisis sobre la muestra incautada, sino que deberá ser copiada y sobre la copia se deberá realizar la pericia.

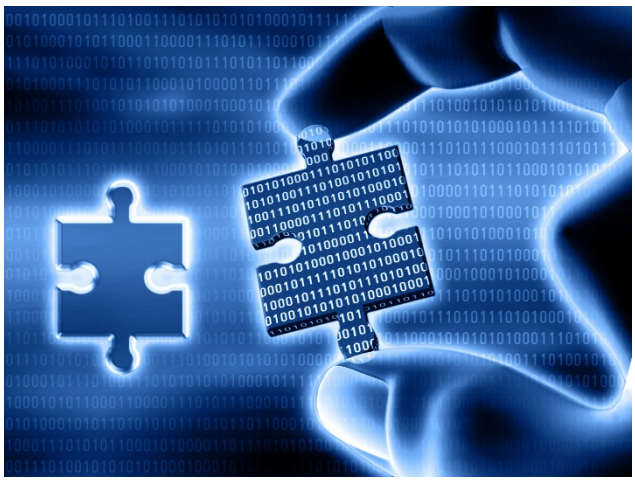
De este modo, aparece el concepto de cadena de custodia, la cual es un acta en donde se registra el lugar, fecha, analista y demás actores que manipularon la muestra.

En muchos casos deberemos utilizar las técnicas de Hashes para identificar de forma unívoca determinados archivos que podrían ser de gran utilidad para la investigación.

Al intervenir una evidencia digital, el procedimiento habitual consiste en obtener la firma hash del fichero o disco duro intervenido, realizar una copia de la evidencia mediante los diversos métodos conocidos, obtener la firma hash de la copia de la evidencia y cotejarla con la original. Si ambas firmas digitales coinciden, la cadena de custodia queda preservada y el perito informático podrá comenzar a estudiar la copia de la evidencia digital intervenida.

3. Análisis

Finalmente, una vez obtenida la información y preservada, se pasa a la parte más compleja. Sin duda, es la fase más técnica, donde se utilizan tanto hardware como software específicamente diseñados para el análisis forense.



Si bien existen métricas y metodologías que ayudan a estructurar el trabajo de campo, se podrán obtener grandes diferencias dependiendo de las herramientas que se utilicen, las capacidades y experiencia del analista.

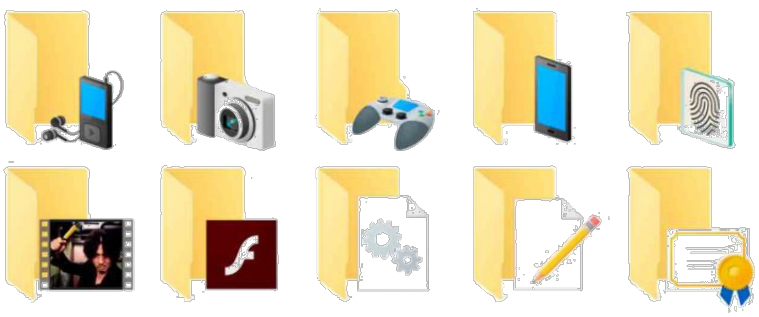
Además, es muy importante tener en claro qué es lo que estamos buscando, debido a que esto dará un enfoque más preciso a la hora de ir a buscar pruebas. Sin embargo, el estudio de la línea de tiempo (timeline),

logs de accesos y una descarga de la memora RAM será muy útil para la mayoría de las pericias.

Es muy importante en esta instancia la evaluación de criticidad del incidente encontrado y los actores involucrados en él.

4. Documentación

Si bien esta es una etapa final, recomendamos ir documentando todas las acciones, en lo posible, a medida que vayan ocurriendo. Aquí ya debemos tener claro por nuestro análisis qué fue lo sucedido, e intentar poner énfasis en cuestiones críticas y relevantes a la causa.



Debemos citar y adjuntar toda la información obtenida, estableciendo una relación lógica entre las pruebas obtenidas y las tareas realizadas, asegurando la repetición de la investigación.

5. Presentación

Normalmente se suelen usar varios modelos para la presentación de esta documentación. Por un lado, se entrega un informe ejecutivo mostrando los rasgos más importantes de forma resumida y ponderando por criticidad en la investigación

sin entrar en detalles técnicos. Este informe debe ser muy claro, certero y conciso, dejando afuera cualquier cuestión que genere algún tipo de duda.

Un segundo informe llamado "Informe Técnico" es una exposición que nos detalla en mayor grado y precisión todo el análisis realizado, resaltando técnicas y resultados encontrados, poniendo énfasis en modo de observación y dejando de lado las opiniones personales.

Conclusiones

A la hora de auditar un incidente de seguridad, hay que tener muy en claro su naturaleza, ser meticulosos, estructurados, muy claros en las observaciones y detallar con la mayor precisión posible.

Asegurando preservar la muestra en estado original y siempre trabajando sobre copias realizadas bit a bit, lograremos ir alineados a las metodologías estandarizadas internacionales, las cuales nos darán pie a presentar nuestros resultados con un soporte legal ante alguna Institución que lo requiera.

Evaluación

La fase de análisis no termina hasta que no se puede determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en el sistema, etc. Es decir, es el núcleo duro de la investigación y tiene que concluir con el máximo de información posible para poder proceder a elaborar unos informes con todo el suceso bien documentado.

Antes de empezar el análisis, es importante recordar unas premisas básicas que todo investigador debe tener presente en el momento de enfrontarse al incidente. Como ya se ha explicado nunca se debe trabajar con datos originales y se debe respetar cada una de las previamente habremos creado la imagen a partir de las copias que se

hicieron para el análisis. En este caso podremos trabajar con la imagen, ejecutar archivos y realizar otras tareas sin tanto cuidado, pues siempre cabe la opción de volver a montar la imagen desde cero en caso de problemas.

La opción del análisis en frío resulta muy atractiva pues en caso de malwares se podrán ejecutar sin miedo, reproducir lo que ocurre y desmontar la imagen sin que la copia original resulte afectada. De este modo tal vez se pueda ir un poco más allá en la investigación y ser un poco más agresivo.
Existen varios programas gratuitos para crear y gestionar máquinas virtuales, por ejemplo, Oracle VM VirtualBox (45), que ofrecen muy buenas prestaciones.

Creación de la línea temporal

Sea cual sea el tipo de análisis que se va a llevar a cabo, el primer paso suele ser crear una línea temporal dónde ubicar los acontecimientos que han tenido lugar en el equipo desde su primera instalación.

Para crear la línea temporal, lo más sencillo es referirnos a los tiempos MACD de los archivos, es decir, las fechas de modificación, acceso, cambio y borrado, en los casos que aplique. Es importante, como ya se ha indicado en alguna ocasión tener en cuenta los husos horarios y que la fecha y hora del sistema no tienen por qué coincidir con los reales. Este dato es muy importante para poder dar crédito a las pruebas y a la investigación en general.

Para empezar, lo mejor es determinar la fecha de instalación del sistema operativo, para ello se puede buscar en los datos de registro. Además la mayoría de ficheros del sistema compartirán esa fecha. A partir de aquí puede ser interesante ver qué usuarios se crearon al principio, para ver si hay discrepancias o usuarios fuera de lo común en

últimos instantes del equipo. Para ver esta información también es útil acudir al registro del sistema operativo.

Teniendo ya los datos iniciales del sistema, ahora se puede proceder a buscar más información en los ficheros que se ven "a simple vista". Lo importante es localizar que programas fueron los últimos en ser instalados y qué cambios repercutieron en el sistema.

Lo más habitual es que estos programas no se instalen en los lugares habituales, sino que se localicen en rutas poco habituales, por ejemplo en archivos temporales o mezclados con los archivos y librerías del sistema operativo. Aquí se puede ir creando la línea temporal con esos datos.

Alternativamente es útil pensar que no todos los archivos están a la vista. Se puede encontrar información en archivos normales, pero también en temporales, ocultos, borrados o usando técnicas como la esteganografía, no se puede obviar ninguna posibilidad.

Habitualmente los sistemas operativos ofrecen la opción de visualizar los archivos ocultos y también las extensiones. Es útil activar estas opciones para detectar posibles elementos ocultos y extensiones poco habituales que nos resulten extrañas.

Para los archivos borrados se utilizaran programas especiales capaces de recuperar aquellos datos que se hayan eliminado del disco pero sobre los cuales aún no se haya sobrescrito nada. Es posible que el atacante elimine archivos o registros varios en afán de esconder lo que ha ocurrido, si estos no han sido sobrescritos se podrán recuperar y se podrán situar en la línea temporal relacionándolos con el conjunto de sucesos.

Para recuperar información oculta mediante esteganografía también se deberán usar programas concretos. Es posible que el atacante ocultara información sobre otros archivos, tales como imágenes o audio para enviarlos posteriormente o tenerlos almacenados sin llamar la atención. Habitualmente hallaremos más información en ubicaciones ocultas que en los lugares más habituales.

Con todos estos datos se debería poder crear un esbozo de los puntos clave en el tiempo tales como la instalación del sistema, el borrado de determinados archivos, la instalación de los últimos programas, etcétera.

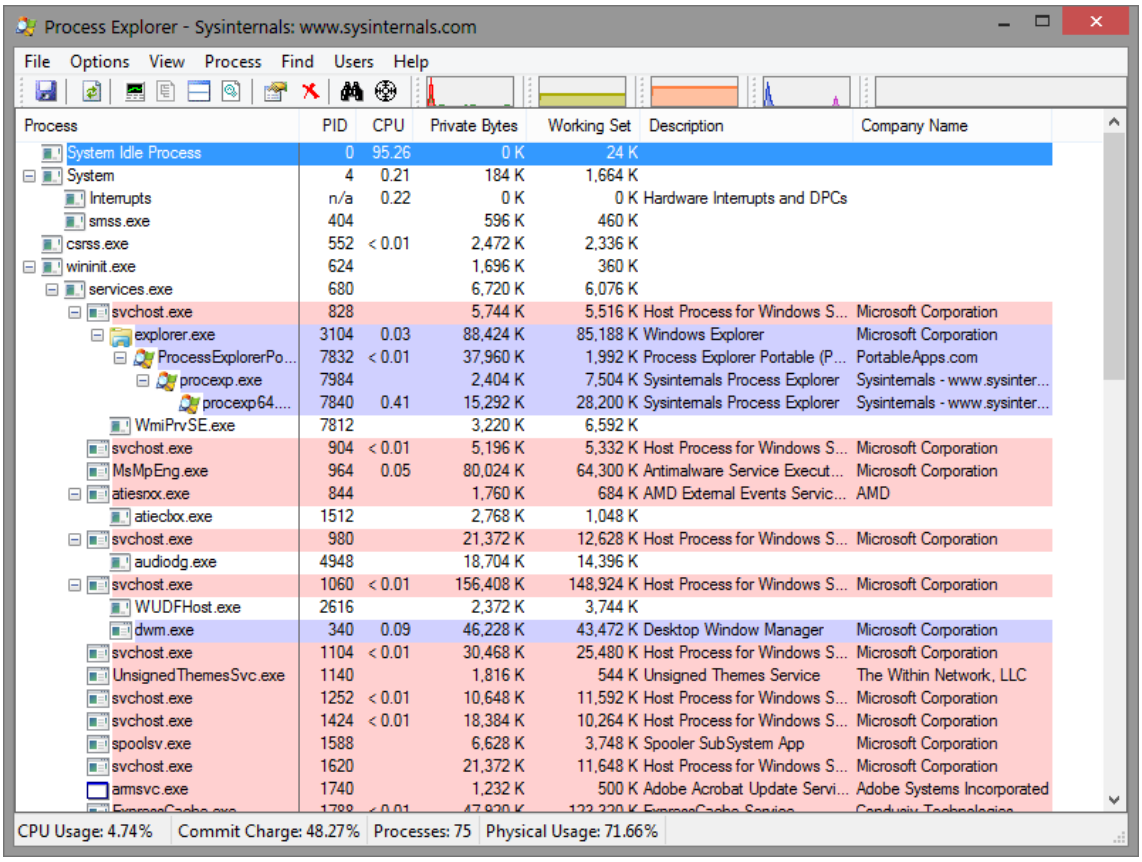
Determinar cómo se actuó

Para determinar cómo se actuó es importante llevar a cabo una investigación sobre la memoria del equipo. Es interesante realizar un volcado de memoria para la obtención de cierta información. Con programas destinados a tal fin podremos ver que procesos se están ejecutando en el momento concreto y también aquellos que hayan sido ocultados para no levantar sospechas.

Con esta información podremos saber qué ejecutables inician los procesos en ejecución y qué librerías se ven involucradas. Llegados aquí se puede proceder a realizar volcados de los ejecutables y de dichas librerías para poder analizar si contienen cadenas sospechosas o si, por lo contrario, son archivos legítimos. Sabiendo los procesos que se ejecutan y su naturaleza podemos obtener pistas de cómo se actuó para comprometer el equipo.

A menudo nos deberemos fijar en procesos en ejecución aparentemente inofensivos, habituales y legítimos en los sistemas operativos. No es extraño que determinados procesos con fines malintencionados se camuflen con procesos legítimos.

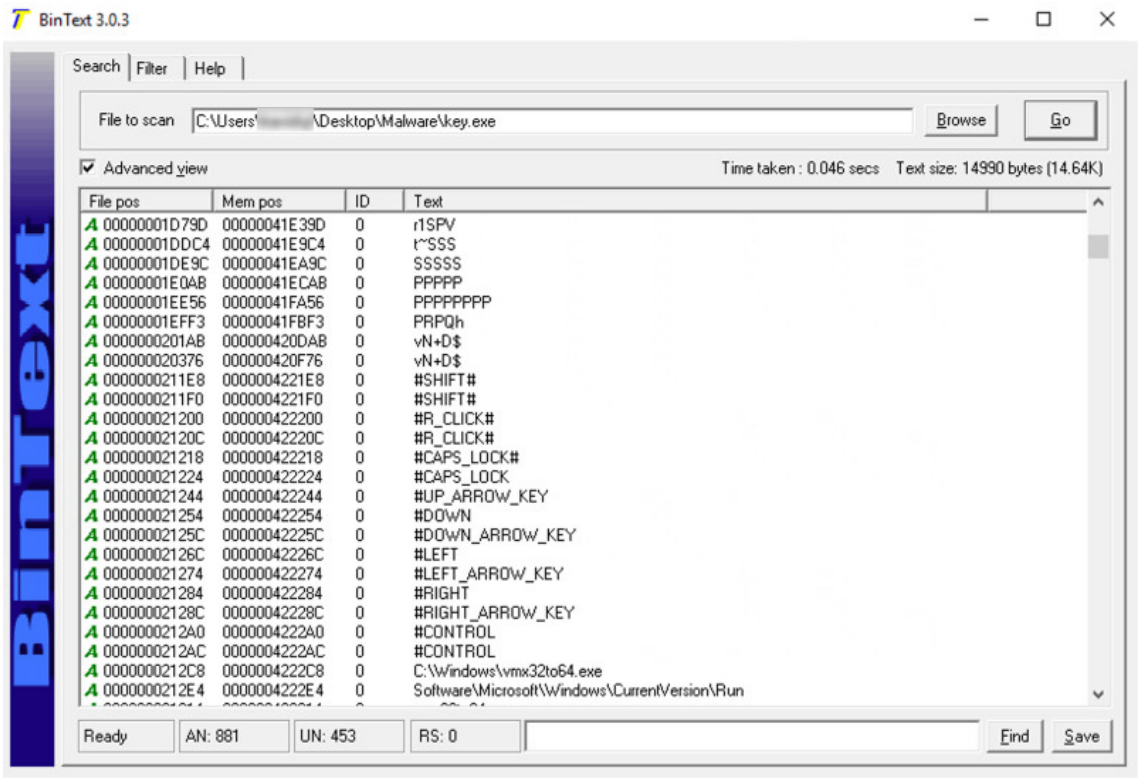
Para ello deberemos observar que muchas veces estos se encuentran sin un proceso padre, cuando lo más habitual es que dependan de otros. En otras ocasiones simplemente se camuflan con nombres muy parecidos a otros para pasar desapercibidos.



Ciertos programas también nos darán información sobre las cadenas del ejecutable en cuestión. Con ellas podremos ver si mutan su contenido cuando se ejecutan en memoria y cuál es su contenido.

En ocasiones, cierta información de las cadenas nos puede dar pistas muy valiosas, como por ejemplo, cadenas dónde encontrar logs, o enlaces a direcciones de Internet. También nos puede dar pistas sobre el tipo de malware al que nos enfrentamos.

Si por ejemplo encontramos cadenas con alfabetos o teclas concretas del teclado, es probable que nos encontremos ante un keylogger.



Finalmente, otra práctica interesante para determinar cómo se actuó es leer la secuencia de comandos escrita por consola. Para ello procederemos con el volcado de memoria y podremos obtener dicha información.

De este modo podremos leer que comandos se hicieron por consola y sabremos si se ejecutó algún proceso de este modo. Debemos excluir nuestras propias instrucciones pues seguramente aparecerán los comandos del volcado de memoria que se hicieron en su momento.

Identificación de autores

Para poder realizar una identificación del autor o autores del incidente, otra información importante que nos puede dar el volcado de memoria son las conexiones

de red abiertas y las que están preparadas para enviar o recibir datos. Con esto podremos relacionar el posible origen del ataque buscando datos como la dirección IP en Internet.

Hay que actuar con prudencia puesto que en ocasiones se utilizan técnicas para distribuir los ataques o falsear la dirección IP. Hay que ser crítico con la información que se obtiene y contrastarla correctamente. No siempre se obtendrá la respuesta al primer intento y posiblemente en ocasiones sea muy difícil averiguar el origen de un incidente.

Es interesante recapacitar en los distintos perfiles de atacantes que se pueden dar hoy día en este ámbito para intentar mimetizarse y entender quién pudo ser el autor.

Por un lado podemos encontrar organizaciones y criminales que actúan por motivaciones económicas. Su finalidad es robar cierta información, ya sea empresarial o personal, para una vez obtenida venderla o sacar un rendimiento oneroso de la información.

Por otro lado está quién sólo busca acceder a sistemas por mero prestigio y reconocimiento en su ambiente cibernético. Accediendo a sistemas mal configurados y publicando datos que prueben su fechoría incrementará su notoriedad y se dará a conocer más en las redes.

En este punto es importante analizar dos vertientes. En caso que se esté realizando un peritaje con fines inculpatorios, o sea, judiciales, se deberá intentar resolver quién es el autor o al menos aportar pistas fiables para que otros investigadores puedan llevar a cabo otras investigaciones de otros ámbitos.

En cambio, si es con fines correctivos lo más interesante seguramente será obviar esta fase y proceder con el estudio del impacto causado y estudiar las mejoras que se pueden implantar para evitar episodios similares.

Impacto causado

El impacto causado se puede calcular en base a distintos factores y no hay un método único para su cálculo, ni una fórmula que nos dé un importe económico. Aun así para estos cálculos puede servir ayudarse de métodos como BIA (Business Impact Analysis) que determinan el impacto de ciertos eventos ayudando a valorar los daños económicamente.

A la larga cualquier incidente ocurrido devengará en unos gastos económicos que habrá que cuantificar en función de los ítems afectados tras el suceso. En ocasiones el coste económico resultará de tener que reemplazar una máquina o dispositivo que ha quedado inservible tras un ataque o bien las horas de empleado de tener que reinstalar el sistema. En este caso, el cálculo no supone mayor dificultad y se resuelve fácilmente.

En otras ocasiones, por ejemplo, los daños pueden deberse al robo de una información de secreto industrial en el que habrá que cuantificar no sólo qué supone reponer el sistema sino, a la larga, en qué se verá afectada la empresa.

Los datos robados pueden ser para publicar cierta información sobre la empresa y poner en la opinión pública datos con intenciones de crear mala imagen, lo cual supone un daño incalculable y muy elevado para la empresa.

El **impacto** no sólo se puede **calcular en base económica**. Como ya se ha comentado al inicio de esta sección también existen otros factores, es el caso del **tiempo de inactividad**. Si el incidente ha supuesto paralizar la producción de una planta

automatizada de fabricación esto supone muchas horas en que la producción es nula, por lo tanto no se trabajará.

Evidentemente, a la larga también supondrá un problema económico pues no se podrán servir los pedidos pendientes de los clientes. Si la paralización afecta a una oficina, tal vez no se pare la producción de bienes pero sí el trabajo de los empleados que verán retrasado todo su trabajo.

Clasificación de los incidentes de seguridad

El siguiente 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.

También 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.

Priorización

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

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

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 siguiente a la detección

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 pérdida 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

Reacción

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 mi negocio relacionada con mis clientes, proveedores, etc.., que pueden incluir datos de carácter persona de acuerdo con la LOPD
- **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)

La solución es disponer de un **Plan de Respuesta ante Incidentes de Seguridad**. Si bien la respuesta es sencilla, la elaboración de un *Plan de Respuesta ante Incidentes* no es trivial. No obstante, estas serían las pautas a seguir para la creación de un *Plan de Respuesta ante Incidentes*:

- **Disponer de un protocolo interno de gestión de incidentes**. Establecer un comité de crisis con el personal adecuado para definir y establecer las medidas que se van a adoptar frente al incidente de seguridad.
- **Analizar el incidente de seguridad.** Es importante disponer de las herramientas necesarias para analizar, por ejemplo, a través de sistemas de monitorización y de logs de los sistemas, cómo y cuándo se ha producido el incidente, determinar la información que ha podido ser sustraída y averiguar dónde se ha hecho pública, etc.
- **Evaluación inicial y toma de decisiones**. Una vez se ha analizado el incidente y se ha determinado como ha sucedido, es de vital importancia aplicar los controles y las medidas necesarias para resolver el incidente de seguridad y establecer las acciones destinadas a cerrar la filtración y evitar nuevas fugas de información. En esta fase, se establecen los posibles planes de comunicación tanto a nivel interno, como a los clientes afectados y a las autoridades correspondientes.
- **Seguimiento de las medidas aplicadas**. Es de vital importancia monitorizar y realizar una mejora contínua en base las lecciones aprendidas para asegurar que las medidas de protección y prevención impulsadas son adecuadas para que no se vuelva a producir un incidente de seguridad con las mismas características.

Nunca estaremos 100% seguros frente a una brecha de seguridad, pero es importante en base las buenas prácticas y gracias a la tecnología, disponer de medidas de seguridad que minimicen los ataques y los riesgos en los que una organización está expuesta y, sobre todo, saber actuar una vez la empresa ha sido atacada o es susceptible de que se haya producido una fuga de información.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Una vez que tengamos un plan de respuesta ante incidentes, deberemos ensayarlo y hacer todas las simulaciones. Realizar pruebas de manera anual para asegurar que el plan funciona es una medida recomendable.

12. RELACIÓN CON PROVEEDORES

La externalización de ciertos servicios puede tener muchas ventajas para nuestra empresa suponiendo un ahorro de personal y recursos propios al contratarse un tercero como proveedor para desempeñar una o varias tareas específicas por un período de tiempo determinado.

Es habitual la subcontratación de profesionales especializados que pueden tener acceso a información confidencial siendo nuestra obligación implementar las medidas técnicas necesarias para limitar los permisos y los accesos a la información, para que los proveedores accedan únicamente a la información estrictamente necesaria para realizar su trabajo

Podemos agrupar estos proveedores en tres grupos:

- **Proveedores de servicios tecnológicos**. Son aquellos que nos prestan servicios como: Mantenimiento informático de hardware o software, alojamiento web, servicios cloud, consultoría tecnológica, etc.
- **Proveedores de servicios no tecnológicos** pero con acceso a datos personales y/o confidenciales de nuestra empresa; Asesores laborales, fiscales, jurídicos, agencias de viajes, etc.
- **Proveedores de equipamiento y productos tecnológicos**. Nos suministran dispositivos de hardware; como ordenadores o teléfonos móviles y software, como aplicaciones de gestión, recursos humanos o videoconferencia.

En la actualidad antes de contratar un proveedor, además de los criterios económico y de prestación de servicio que nos puedan prestar, es fundamental valorar si la empresa o profesional que seleccionemos ofrece las garantías legales que la norma requiere ya que en caso contrario, nosotros como contratantes responderemos como responsables

ante una infracción de la Ley Orgánica de Protección de Datos Personales y Garantia de Derechos Digitales (LOPDGDD) o el Reglamento General de Protección de Datos RGPD.

La gestión de proveedores y el RGPD

El Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, es de aplicación efectiva desde el 25 de mayo de 2018, supone un cambio muy importante en la gestión de los datos personales de las empresas.

Además de la puesta en marcha de una serie de medidas de seguridad, tanto tecnológicas como procedimentales, el RGPD crea una nueva serie de derechos y obligaciones para los tratantes de datos.

Un aspecto que tendrá mayor consideración a partir de la fecha mencionada, será la relación con aquellos proveedores que traten datos personales.

Con el RGPD, se establecen nuevas exigencias a la hora de establecer relaciones con los proveedores en cuanto a gestión de la privacidad ya sean en procesos de licitación como en contratación directa.

Algunos de los requisitos a tener en cuenta serían:

- **Contratos**: los proveedores deben tener un contrato escrito (o cualquier otro tipo de acto legal) con los responsables donde se detalle la duración, la naturaleza y el objeto del tratamiento, el tipo y las categorías de datos personales, así como las obligaciones y los derechos del responsable del tratamiento.

- **Seguridad de los datos:** los proveedores deberán garantizar la implantación de las medidas de seguridad suficientes y las señaladas por el contratista, a fin de que se establezca un marco de seguridad adecuado.
- **Control por parte de las autoridades:** los encargados de tratamiento, podrán estar sujetos al control por parte de las autoridades de protección de datos (nacionales o europeas) en tanto son responsables de la gestión de datos personales.
- **Brechas de seguridad:** tendrán la obligación de informar al contratante y al usuario, si es el caso, de las brechas de seguridad que hayan podido sufrir, dentro del plazo legalmente establecido de 72 horas.
- **Transferencias internacionales de datos:** si el tratamiento de los datos o parte del mismo se va a llevar a cabo por parte del proveedor, fuera del ámbito de la UE, tendrá la obligación de informar del hecho al contratante y reflejarlo en el contrato que les vincule.
- **Privacy by default:** cualquier tratamiento de datos deberá llevarse a cabo mediante la premisa de Privacy by default, es decir, teniendo en cuenta desde el momento mismo del diseño del tratamiento, los aspectos relacionados con la privacidad. Por tanto, el contratante tendrá que tener en cuenta lo previsto en la normativa relacionada con la privacidad, lo previsto en cuanto la seguridad que los proveedores le puedan ofrecer, valorando bajo su propia responsabilidad, el proveedor más adecuado.

Destrucción de información confidencial

La Ley Orgánica de Protección de Datos y Garantia de Derechos Digitales (LOPDGDD) y la Agencia Española de Protección de Datos (AEPD) exigen que cualquier empresa o institución que trabaje con información a nombre de terceros, debe cumplir con la normativa y los procedimientos adecuados con el proceso de destrucción de estos datos confidenciales.

Esta normativa hace que la destrucción de información confidencial se realice de forma segura y sea tan importante como su almacenamiento y el acceso limitado a esta.

Si esta normativa se incumpliera, los datos confidenciales incorrectamente destruidos podrían llegar a manos malintencionadas.

El cumplimiento de estas normas y procedimientos es de gran importancia pues en caso de incumplirlos o vulnéralos podría incurrirse en un delito contra la protección de datos.

Pueden verse en la prensa múltiples casos de empresas y entidades que vulneran los derechos de sus clientes al no destruir de forma segura sus archivos confidenciales una vez finalizada su vida útil.

Este tipo de acciones son severamente castigadas por la ley, y la audiencia Nacional ya ha firmado varias sentencias por el incumplimiento de las normativas: LOPD y el Real Decreto 1720/2007, imponiendo sanciones de hasta 60.000 €.

Además de la sanción económica, estas sentencias causan un grave deterioro de la imagen y la reputación de la entidad sancionada, lo que repercute en una pérdida de confianza por parte de sus clientes.

Teniendo todo esto en cuenta, es importante conocer las opciones de borrado y destrucción segura de datos que existen en el mercado.

Con la colaboración de: Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Destrucción Segura de Datos

Para la información en soporte digital, podemos encontrar una gran variedad de desmagnetizadores que además de realizar el borrado de los dispositivos generan un pulso muy potente y enérgico para garantizar un borrado óptimo y eficaz, pues se crea un campo de borrado mucho más potente que el de los cabezales de lectura y escritura habituales. Este sistema garantiza que los datos no se puedan recuperar por medios informáticos o de laboratorio.

La documentación impresa en papel o soportes ópticos como CDs y DVDs, deben ser destruidos mediante sistemas mecánicos que realicen cortes en estos materiales. De manera que se garantice un tamaño y forma adecuado de los restos acorde con los diferentes grados de seguridad y necesidades de la empresa.

En este tipo de destructoras de documentos de papel existe una gran variedad de tamaños y niveles de seguridad, comprendiendo desde las destructoras más básicas para oficina y empresas pequeñas, hasta las máquinas más profesionales para empresas que deben gestionar gran cantidad de información confidencial.

Es un hecho que a pesar de las medidas que implantemos, siempre existe el riesgo de que ocurra un incidente de ciberseguridad. Por ello, debemos preparar un plan de acción que nos indique cómo actuar de la manera más eficaz posible en estos casos.
Existen muchos tipos de incidentes de ciberseguridad, algunos son más habituales que otros que podrían encajar en una de las siguientes tipologías:

- incidentes no intencionados o involuntarios
- daños físicos
- incumplimiento o violación de requisitos y regulaciones legales
- fallos en las configuraciones
- denegación de servicio
- acceso no autorizado, espionaje y robo de información
- borrado o pérdida de información
- infección por código malicioso

Para ejecutar correctamente el plan y evitar que el daño se extienda se deben detallar las acciones a realizar en cada momento, la lista de las personas involucradas y sus responsabilidades, los canales de comunicación oportunos, etc.

Tras un incidente, si hemos aplicado el plan, tendremos una valiosa información para conocer y valorar los riesgos existentes, y así evitar incidentes similares en el futuro.

En caso de que ocurran incidentes graves o desastres que paralicen nuestra actividad principal, aplicaremos el plan de contingencia y continuidad del negocio.

El objetivo principal será asegurarnos de que todos los miembros de la organización conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la empresa. También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

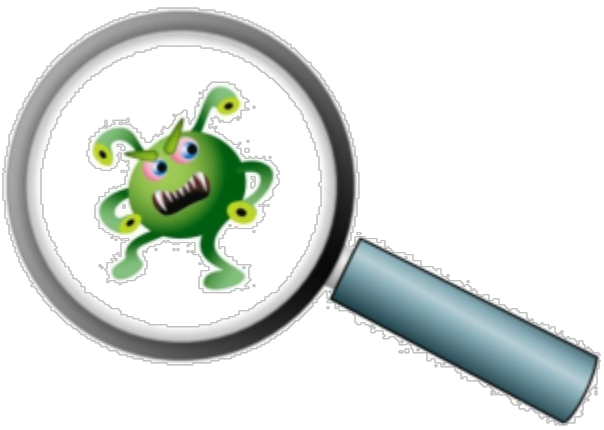
Resumen

¿Cómo podemos saber si nuestro ordenador está infectado por algún tipo de malware? ¿Cuáles son los síntomas que pueden hacernos sospechar que nuestros sistemas de información están en peligro? Realmente no son menos diferentes que cuando nos cogemos un buen constipado.

En cualquier momento, cualquier equipo, de cualquier empresa, por pequeña que esta sea, es susceptible de sufrir un ataque informático o de ser infectado con un virus. Si bien es cierto que al igual que si no nos abrigamos o no nos alimentamos adecuadamente, las probabilidades de agarrarnos un constipado son más altas, en una infección por malware o en cualquier tipo de ataque, tendremos una probabilidad mayor si no tomamos ciertas medidas.

Un ataque puede consistir desde el acceso a información de la empresa (robar información confidencial, credenciales de acceso, datos bancarios, etc. que luego venderán en el mercado negro o utilizarán para actividades fraudulentas), a tomar el control de nuestros dispositivos tecnológicos: ordenadores, servidores, móviles para otras actividades delictivas, como por ejemplo convertirlos en zombis bajo el control del ciberdelincuente y realizar desde él envíos de spam o ataques de denegación de servicio. Todo esto sin que nos demos cuenta.

La principal vía de entrada suele ser a través de la instalación de algún tipo de malware tras haber visitado una página web dudosa o haber abierto algún fichero adjunto infectado desde el correo electrónico.



Nada es más importante que implicar a nuestros empleados, concienciando y formándolos sobre ciberseguridad y cómo identificar los comportamientos sospechosos en los equipos de trabajo. Estos son diez de los principales síntomas, que deben hacernos sospechar que nuestro sistema pueda estar infectado:

- **El sistema funciona más lento de lo normal**. Si bien puede tratarse de algún error de configuración u optimización en el equipo por alguna herramienta

mal instalada o configurada; también podría tratarse de algún tipo de malware, como un troyano, que esté consumiendo los recursos del sistema al infectarlo.

- **La conexión a internet va muy lenta**. El malware puede estar haciendo uso de la conexión a internet para robar información y mandarla al exterior, realizar ataques de denegación de servicio, enviar correos masivos, etc. Esto hace que se reduzca el ancho de banda.
- **Algunos programas no arrancan correctamente**. Programas que no se ejecutan o que piden la instalación de librerías u otros programas para poder ejecutarse. Puede ser un problema de configuración, pero también un síntoma de infección.
- **Se está enviando spam desde tu equipo**. Los contactos de la agenda de contactos de tu correo electrónico reciben correos que no has enviado con adjuntos extraños y enlaces a páginas sospechosas. Este es un claro síntoma de que el sistema puede estar comprometido por algún tipo de malware que se esté intentando propagar por medio de tu correo electrónico.
- **El antivirus y el cortafuegos de tu equipo están desactivados**. El primer paso para la infección de un equipo por parte de un virus, suele ser desactivar los programas de protección de tu sistema.
- **El navegador de internet tiene un comportamiento extraño**. Al navegar, se abren ventanas con publicidad o páginas web no solicitadas de contenido «dudoso», la página de inicio se cambia sola, etc. Esto suele ser un claro síntoma de infección por un tipo de malware, que aprovecha los anuncios publicitarios, llamado adware.
- **El espacio de almacenamiento de información está lleno sin motivo**. Un repentino y anormal descenso del espacio dedicado al almacenamiento de la información en el equipo, servidor de datos, nube, etc. puede hacernos sospechar que estos puedan estar comprometidos y siendo utilizados para

actividades maliciosas, como el almacenamiento de contenidos e información ilícita.

- **El sistema presenta actividad sin estar utilizándose**. Se escuchan sonidos y parpadean las luces indicativas de lecturas en el disco duro del sistema cuando nadie está trabajando en él. Esto puede ser producido por algún programa en ejecución, como actualizaciones programadas o escaneos del antivirus, pero puede ser también un síntoma de la actividad de algún tipo de malware.
- **Hay credenciales de acceso que no funcionan**. Puede ser que un atacante haya conseguido acceder al sistema y cambiar las contraseñas.
- **Mi equipo tiene un comportamiento extraño, no puedo acceder a mi información o su contenido a aparecido cifrado de repente**. Hay malware diseñado para robar, mover, eliminar o cifrar la información almacenada en los equipos. Entre ellos está el ransomware, que cifra la información y pide un rescate a cambio de su devolución.

Estos son solo un ejemplo de las «pistas» que puede darnos nuestro sistema para «avisarnos» que tenemos un problema de seguridad. Hay que estar atentos a los síntomas o «pequeñas señales» que muestran nuestros sistemas, que puedan hacernos sospechar de un problema de este tipo.

Muchas veces serán falsas alarmas causadas por un funcionamiento irregular del hardware del equipo o por una configuración incorrecta de algún programa. También tendremos que prestarles atención ya que pueden suponer un riesgo de cara a proteger la confidencialidad, integridad y disponibilidad de nuestro principal activo: la información.