Guía práctica de ciberseguridad

PROTEGE TU NEGOCIO

TECTECO
SECURITY SYSTEMS

Indice

1

¿Por qué necesitas leer esta guía?

INTRODUCCIÓN

Quizás no seas consciente de la importancia que tiene la seguridad digital en tu negocio o pienses que tú no estás en el punto de mira de los atacantes porque eres desconocido o pequeño, pero fíjate en estos datos:

A nivel mundial el

43%

de los ataques están dirigidos a pymes y en España esa cifra asciende al

70%

75.000€

coste medio de un ciberataque para una pyme

60%

de las pequeñas empresas y autónomos que sufren un ciberataque no son capaces de superar las pérdidas y tras el ataque cierran a los

6 meses

Por tanto, tu negocio puede estar en peligro si no tomas conciencia de los riegos a los que te expones y conoces las medidas adecuadas.

¡EMPEZAMOS!

2 ¿QUÉ ES EL CIBERCRIMEN Y CÓMO ACTÚA?

La realidad del cibercrimen

Quizás la imagen que tengas de un "hacker" sea ese freaky solitario que desde una habitación oscura y llena de tecnología trata de colarse en un sistema ajeno. Y ciertamente, de esos sigue habiendo, trabajando con la misma filosofía que antaño y con distintos grados de malignidad: desde el gracioso hasta el dañino.

Sin embargo, esto ha cambiado radicalmente. Ahora nos encontramos con distintas tipologías de cibercrimen:

- Existe la **ciberguerra**, promovida por gobiernos donde la guerra convencional se ha trasladado a la arena digital. De hecho, muchas de las rencillas internacionales actuales se dirimen en este entorno.
- Tenemos, por ejemplo, el **hacktivismo** que utilizan estos ataques con fines reivindicativos, ya sean políticos o sociales.
- O el **ciberterrorismo**, que utiliza medios y herramientas digitales para llevar a cabo ataques de índole terrorista con fines políticos, religiosos o económicos.

Pero, como ciudadano o empresario, fundamentalmente lo que te debe preocupar son las **mafias organizadas dedicadas al cibercrimen.**

Las mafias no son individuos que en su tiempo libre hacen trastadas, que se divierten haciendo que tu pantalla se convierta en barrotes, son profesionales que **emplean el 100% de su tiempo a obtener beneficios económicos de sus acciones delictivas**. Estas mafias han creado una verdadera **industria del cibercrimen** dedicadas exclusivamente a robar, donde coexisten distintos tipos de modelos de negocio:

- Empresas que desarrollan productos ad-hoc tales como malware o software que, bajo apariencia legítima, sirve para otros fines (por ejemplo, falsos antivirus).
- Empresas que alquilan infraestructura o capacidad de proceso ajena (manejada por botnets) para dedicarlos a realizar ataques.
- Empresas o individuos que prestan servicios de cibercrimen, conocidos también como "Crime as a Service", y que cualquier persona puede contratar.

Y es ante estas mafias ante las cuales debes protegerte adecuadamente, porque no importa el tamaño que tengas, todos somos objetivos de estas mafias.

> **"El cibercrimen ya es la actividad delictiva que mueve más dinero, por encima de la venta de armas y el narcotráfico"**

3 EN EL PUNTO DE MIRA DE LOS CIBERATAQUES

El desconocimiento y la falta de concienciación son el caldo de cultivo de los ciberataques. Existen, además, dos falsas creencias acerca de la ciberseguridad que ponen en riesgo tu negocio:

Falsa creencia #1
Los ataques vienen de fuera

Hay una tendencia a pensar que los ataques vienen casi siempre de fuera de tu red y que medidas como la instalación de un firewall perimetral son suficientes. Sin embargo, según un informe de IBM de 2018, **el 60% de los ciberataques se producen por amenazas internas.** El mismo informe pero de 2020 apunta a que el 86% de las brechas de datos fueron provocados por la acción de usuarios internos.

No obstante, no todas las amenazas internas vienen de usuarios maliciosos, que actúan intencionadamente por venganza o despecho. **Una gran parte de los ataques internos se producen por negligencia o error humano**. Por ejemplo, cuando dejas la contraseña apuntada en un post-it en la pantalla del ordenador, o si configuras mal un servidor por falta de conocimientos, dejando puertas abiertas por las que entran atacantes.

Se consideran también ataques internos los que realizan los infiltrados. Éstos son usuarios externos que obtienen acceso a la empresa gracias a credenciales legítimas sin autorización (por ejemplo, rompiendo la contraseña de la red WiFi). En estos casos el verdadero ataque se produce desde dentro de la red, aun siendo un usuario externo.

Por eso es crítico que **tu red corporativa quede securizada desde dentro**.

Algunos ejemplos muy conocidos de ataques insider son:

- Tesla (junio 2018), reportó que un empleado saboteó los sistemas de control del sistema de producción y envió información altamente confidencial a otras compañías. El motivo fue el enfado por una promoción que no llegó a recibir.

- Otro ataque con pérdidas millonarias fue el que sufrió el Punjab National Bank, con un fraude de unos 1.800 millones obtenidos de transacciones que permanecieron sin detectar durante siete años, como parte de una trama para la compra de diamantes en bruto.

Falsa creencia #2
¿Para qué me van a atacar a mí?

La mayoría de las pymes y de la gente en general cree que, al ser objetivos pequeños, los ciberdelincuentes no se van a interesar en ellos dado que tienen poco que robar o que sus datos no tienen valor.

Sin embargo, según Verizon, el 58% de las brechas de datos provienen precisamente de empresas pequeñas.

Esto se debe a que la mayoría de los ataques no se producen de forma dirigida, sino que **forman parte de campañas masivas en las que se buscan accesos de manera automatizada y aleatoria.**

Probablemente los ciberdelincuentes ni siquiera sepan a quién están atacando. Es como si accedieran a un aparcamiento y del modo más rápido posible se dedicarán a comprobar qué puertas de coches están abiertas. No importa el coche o su contenido, lo importante es acceder al mayor número de coches con el menor coste posible. Los ciberatacantes hacen **barridos automatizados de direcciones IP** hasta dar con una puerta abierta que les permite acceder a una red o dispositivo.

Como se menciona anteriormente, los ciberdelincuentes han seguido un proceso de profesionalización, y aunque algunos se dedican a las "grandes cuentas", muchos otros prefieren mantener **un modelo de negocio basado en un margen de beneficio menor pero multiplicado por un mayor número de objetivos.**

Todos los ciberataques tienen una motivación económica. Si reducen el coste yendo a por presas más fáciles, aunque la ganancia sea menor por cada una de esas empresas, lo compensan a base de volumen.

4 TÉCNICAS Y ATAQUES MÁS HABITUALES

Ingenieria social, phishing y timo del CEO

El eslabón más débil en la cadena de ciberseguridad es el factor humano. Por ello, los ciberdelincuentes utilizan técnicas **de ingeniería social para atacar.**
Estas técnicas buscan manipular a las personas para que actúen de determinada forma, apoyándose en comportamientos tales como la tendencia a agradar, el gusto por ser alabados, la codicia o la dificultad de dar un NO por respuesta.

Muchos de los ataques basados en ingeniería social no son más que una **evolución de las clásicas estafas de toda la vida** que buscan aprovecharse de la ingenuidad, el desconocimiento y, en muchos casos, la avaricia de las víctimas.
En la ingeniería social interviene más la psicología que la tecnología y, por tanto, **no existe ningún sistema informático que nos pueda proteger de un ataque de este estilo**, por lo que la mejor manera de no caer en estos ataques es **aprender a detectarlos para evitar picar en el anzuelo.**

Los cibercriminales siempre se aprovechan de vulnerabilidades, ya sean técnicas o humanas.

Entre los ataques más habituales que utilizan la ingeniería social están el phishing y el timo o fraude del CEO.

Phishing

Por ejemplo, el phishing utiliza una **combinación de ingeniería social y suplantación de identidad** para llevar sus ataques.

Estos ataques llegan habitualmente por email, pero también por sms o por aplicaciones de mensajería.

Lo que caracteriza a este tipo de mensajes es que **simulan ser de procedencia legítima**, imitando los colores corporativos e incluso una dirección de email que parece correcta. Suelen contener enlaces a webs fraudulentas donde, con la apariencia de la web real, te solicitan tus credenciales de acceso que, una vez tecleadas, quedan almacenadas para ser utilizadas posteriormente.

Otros pueden **contener archivos maliciosos o enlaces a webs fraudulentas** que instalan distintos tipos de malware en tus dispositivos para llevar a cabo ataques posteriores.

Ataque del CEO

Dentro de estos ataques, uno de los más peligrosos y dañinos y que más está creciendo es el denominado **timo o fraude del CEO.**

En él, el atacante suplanta la identidad de una persona con poder dentro de la organización y solicita al empleado víctima que le entregue información confidencial, o que haga una transferencia urgente. Estas peticiones se revisten de confidencialidad y secretismo para evitar que la víctima haga las consultas o comprobaciones pertinentes.

Malware. Tipos

El malware, abreviatura de "malicious software", es cualquier tipo de programa o código malicioso o malintencionado cuyo objetivo es infiltrarse en un dispositivo sin el consentimiento del usuario, para extraer información personal o confidencial, provocar un daño, bloquear el dispositivo, robar dinero o utilizarlo para atacar otros dispositivos.

En el acervo popular se suele utilizar de forma general el término virus, pero en realidad **el malware engloba distintas tipologías de software malicioso**, algunos de las cuales son más dañinos que otras. Por ejemplo, está el **Adware**, programas que suelen descargarse junto al software de carácter gratuito y que se instalan de forma inadvertida. Este tipo de software muestra publicidad pero también puede mostrar resultados alterados de las búsquedas del usuario redirigiendo a páginas fraudulentas. Muchas veces instala barras en el navegador que son muy difíciles de eliminar y, en general, son más molestos que dañinos.

Otro ejemplo, sería el **Spyware**: software espía que puede recabar todo tipo de información sobre una persona u organización sin su conocimiento ni consentimiento a través del equipo de la víctima.

También están los **troyanos**, un tipo de malware que se camufla en forma de programa legítimo para pasar inadvertido, como por ejemplo, software gratuito, juegos, películas o cracks de piratear programas. Una vez se instala actúa con efecto retardado dejando puertas abiertas que permiten infiltrarse en los dispositivos.

Bots: son programas pensados para desarrollar botnets, **redes de equipos infectados por códigos maliciosos, que son controlados por un atacante,** el cual dispone de sus recursos para que trabajen de forma conjunta y distribuida. Sería el caso mencionado anteriormente en el cual se alquila infraestructura y capacidad de proceso ajena para llevar a cabo ataques de diverso tipo.

Gusanos: malware que se **auto-replica y distribuye copias de sí mismo** a la red para infectar más dispositivos con algún otro tipo de malware como spyware o troyanos.

Por último, está el **ransomware:** un tipo de malware especialmente peligroso y dañino. Su nombre viene del inglés "ransom" que significa "rescate". Es capaz de **bloquear el acceso a un equipo usurpando el control, para cifrar todos los archivos** y solicitar un **rescate económico para liberarlos.**

Ataques contra redes WiFi

Es una realidad innegable que nuestra vida diaria cada vez depende más de tener conexión a Internet, por lo que la demanda de conectarse a una "WiFi" es cada vez mayor.

Sin embargo, la mayor parte de las redes WiFi a las que accedes son muy vulnerables e inseguras:

La clave de esta vulnerabilidad deriva de la forma habitual de **conexión mediante contraseñas compartidas o PSK (Pre-Shared Key)**.

Igual te estarás preguntando por qué, si son tan inseguras, se siguen utilizando. Para la respuesta hay que remontarse al origen de la propia tecnología WiFi.

Básicamente, debido a las limitaciones de los antiguos procesadores, cuando se concibió y diseñó esta tecnología se optó por **primar la sencillez y la velocidad, sacrificando los elementos relacionados con la seguridad.**

Y aunque se avanza en mejorar estos protocolos de seguridad se continua usando **el mismo sistema de autenticación, la PSK o clave precompartida,** que presenta muchas deficiencias:

- En muchos sitios la **clave es pública y compartida de manera masiva**, no teniendo ningún control de quién la tiene.
- Conectándonos con una clave compartida y sin identificación de los usuarios, **no es posible saber precisamente quién está conectado**, sólo puedes saber la MAC del dispositivo y esto es algo fácilmente suplantable.
- La propia naturaleza de una red implica que t**odos los que están conectados tienen capacidad de ver qué dispositivos están conectados y acceder a ellos**.
- Los usuarios dentro de la red tienen **capacidad de capturar el tráfico que circula por esa red y conocer información confidencial** como credenciales, capturar grabaciones de videocámaras, etc...

Pero, ¿qué tipo de ataques puedes sufrir por utilizar **redes WiFi no seguras**?

Ataques **Man in the middle**: un atacante se interpone entre dos elementos de la red, por ejemplo, tu PC y el router WiFi, y tiene la capacidad de desviar o controlar las comunicaciones entre las dos partes. Si estás en una WiFi pública con usuarios que desconoces, uno de ellos puede interponerse en mitad de tus comunicaciones y espiar una transacción bancaria, por ejemplo. Mira 3 ejemplos de ataques Man in the Middle

MAC e IP spoofing: La MAC es el código que identifica tu dispositivo, la IP es la dirección que se te asigna dentro de una red y el término "spoofing" significa falsificación. Por tanto, este tipo de ataques se basa en **falsificar la MAC o la IP para suplantar la identidad de un dispositivo** y poder, por ejemplo, elevar sus privilegios de acceso a determinadas áreas de la red.

Ataques de diccionario, los cuales se utilizan para descifrar las claves de las redes WiFi a las que no se tiene acceso. Para hacer esto, cualquiera que se sitúe cerca de una red WiFi, puede capturar los paquetes de información que se transmiten sin cifrar. Una vez capturado ese tráfico se procesa offline utilizando palabras de un diccionario o incluso combinaciones frecuentes hasta dar con la clave.

Propagación de malware: cuando un dispositivo infectado se conecta a una red WiFi sin suficientes controles de acceso, es más que probable que la infección se extienda a todos los dispositivos conectados a la misma red.

Como has podido comprobar **hay una gran variedad de ataques y ni todos son de carácter destructivo ni todos son detectados de forma inmediata.** De hecho, muchos pasan inadvertidos. Por ejemplo, tus equipos pueden estar formando parte de una botnet, sin que lo sepas. Puedes detectar síntomas como que te va más lento, que tu consumo en luz se ha incrementado o que el ancho de banda se reduce. **Si no te han robado datos o no hayas sufrido un ataque evidente como un ramsonware, no significa que no hayas sido atacado.**

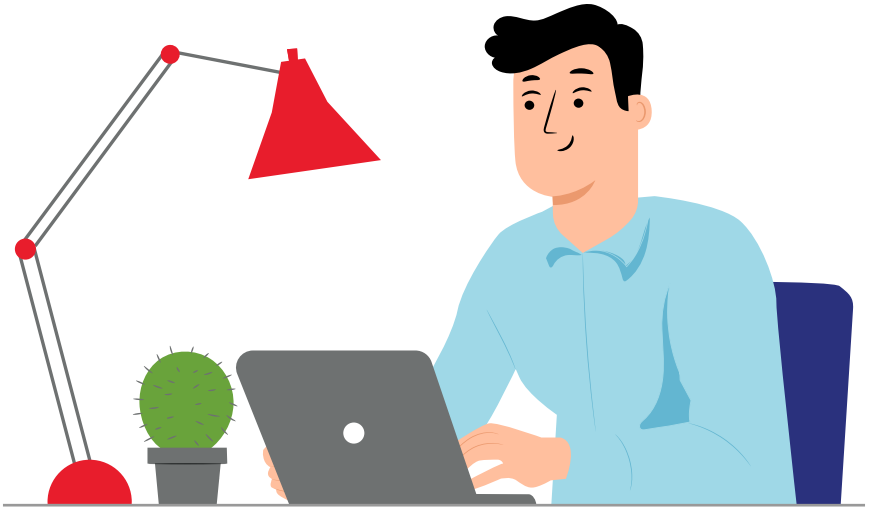
Media de tiempo que se suele tardar en descubrir que has sido atacado.

Es, por tanto, absolutamente crítico que tomes medidas orientadas a prevenir cualquier tipo de ataque con consecuencias nefastas para tu negocio.

Dos amenazas recientes sobre las redes WiFi:

EMOTET: troyano que se propaga a través de redes WiFi. Es peligroso, entre otras cosas, porque se extiende de forma silenciosa. Más información en

Agent Tesla: en un malware que roba las contraseñas de las redes WiFi en los dispositivos infectados. De esta forma pueden conectarse a todas las WiFi a las que dicho dispositivo tenga acceso. Más información en



5 TRES PILARES DE LA CIBERSEGURIDAD

La ciberseguridad se sustenta en tres pilares básicos: confidencialidad, integridad y disponibilidad.

Confidencialidad

Cuando hablamos de confidencialidad nos referimos a **garantizar la privacidad de los datos**, de modo que sólo sean accesibles por personas autorizadas. Por ejemplo, correos, información bancaria, datos de clientes, etc.

Para garantizar la confidencialidad de los datos debes aplicar medidas restrictivas tanto de tipo físico como lógico.

Integridad

La integridad de datos se refiere a la **imposibilidad de que puedan ser modificados o manipulados antes de llegar a su destinatario**. En este sentido, se trata de un concepto que está muy relacionado con la firma digital con el que seguramente estés familiarizado. Garantizar la integridad de las comunicaciones supone tener la tranquilidad de que los datos no se han manipulado en el tránsito, para lo cual es necesario poder verificar que un usuario es quien dice ser que es mediante **procesos de autenticación robustos**.

Disponibilidad

La disponibilidad es la característica que **garantiza que tanto los datos como los servicios sean accesibles**, lo cual es especialmente crítico para cualquier empresa.

Por ejemplo, la disponibilidad puede verse comprometida con los ataques de denegación de servicio o DDoS, uno de los ataques más habituales por su sencillez y bajo coste.

Que una empresa no disponga de su infraestructura para prestar sus servicios a sus clientes supone una gran pérdida económica.

Amplia información en nuestro blog:

6 ¿QUÉ PUEDO HACER?

MEDIDAS PARA PREVENIR UN CIBERATAQUE

Sistema SGSI, medidas técnicas y humanas para aplicar en tu negocio.

Implantación de un sistema SGSI

La primera medida a considerar sería la implantación de un **Sistema de Gestión de la Seguridad de la Información**, el cual consiste en una serie de **políticas, procedimientos y tareas**, enfocadas principalmente en la **gestión del riesgo**.

Hay una cosa a tener en cuenta: **la seguridad 100% no existe**, de hecho no podemos hablar de seguridad, sino de nivel de inseguridad.

Debes ser consciente de que las probabilidades de que intenten atacarte son altísimas y aún con protección puedes ser víctima de un ataque.

Por tanto, a la hora de implantar un Sistema de Gestión de la Seguridad de la Información lo que se busca son dos objetivos:

- **Reducir los riesgos** de ser atacados.
- **Minimizar los daños** en caso de no poder evitar el ataque.

Disponer de un SGSI además **ayuda al cumplimiento de la normativa legal**, como por ejemplo, la ley de protección de datos personales (RGPD y LOPD - GDD).

Para la implantación de dicho sistema es necesaria la **implicación de toda la empresa**, puesto que gran parte de las tareas se van a apoyar en cada uno de los empleados.

Por ello este cambio tiene que estar **liderado por la dirección de la empresa**, demostrando compromiso con los objetivos establecidos.

Campaña de concienciación interna

En cualquier caso, el primer paso siempre debe contemplar una **campaña de concienciación interna** entre los empleados de la empresa. Siempre se dice que un sistema es tan robusto como el más débil de sus componentes. Aunque, por supuesto, es necesario implantar medidas técnicas, estas no son suficientes si no **se considera el sistema en su conjunto**, incluyendo el personal.

Por eso resulta crítico el **establecimiento de una cultura de ciberseguridad** en la empresa, de modo que todos los empleados tengan al menos una formación básica al respecto.

A día de hoy, **la ingeniería social sigue siendo uno de los vectores de ataque más utilizados por los ciberdelincuentes** y el principal modo de defenderse ante ello, aunque haya medidas técnicas que ayuden, es con empleados capacitados para protegerse ante ello.

Es importante tener en cuenta que en las campañas de concienciación hay que diferenciar muy bien entre **la formación destinada al personal técnico y al resto de usuarios**.

En cualquier caso, la profundidad y el detalle en la formación siempre debe estar relacionado con el nivel de acceso del personal al sistema. Por ejemplo, un usuario con escasos privilegios no es tan peligroso como uno con acceso total y, por tanto, es este último al que habrá que exigir un mayor nivel de formación.

Recursos:

Visita la web del **INCIBE** (www.incibe.es) donde encontrará muchos recursos para formas y concienciar a tus empleados

También tienes el blog de **TECTECO** (www.tecteco.com) con muchos contenidos educativos y divulgativos.

Medidas técnicas

Además de la implantación del SGSI y de la campaña de formación interna, por supuesto son **necesarias medidas técnicas** que completen la estrategia de ciberseguridad de la empresa.

Estas medidas dependerán en gran medida de las características de la empresa, tales como tamaño, objetivo de la empresa, sistemas que emplee, etc., sin olvidar el presupuesto.

No existe el sistema invulnerable y cada empresa debe evaluar el coste que está dispuesta a asumir para aplicar el máximo nivel de ciberseguridad posible... y necesario.

A grandes rasgos podemos dividir las medidas de seguridad en dos categorías:

- Las que se aplican en los equipos (ordenadores personales y demás dispositivos).
- Las que afectan a la red en general.

Las medidas que se presentan a continuación no son completas ni exhaustivas, pero pensamos que son las más necesarias y habituales en un entorno de pequeña empresa o de un autónomo.

A nivel de equipo

1. Antivirus

La primera medida a considerar es la instalación de un antivirus. Si bien su utilidad está cada vez más en entredicho por la complejidad del malware actual, sigue siendo un requisito indispensable, aunque sólo sea para evitar el malware barato, que no por ello menos destructivo.

2. Usuarios y contraseñas individuales

En los equipos deben utilizarse **usuarios individuales, no genéricos,** y además protegidos siempre por contraseña. No se debe compartir el usuario salvo en casos muy justificados. Además, cada usuario debería tener ajustados los permisos estrictamente necesarios para realizar su labor. De este modo, si su cuenta resultara comprometida, se limitarían los daños.

3. Contraseñas seguras y actualizadas

Establece una política que obligue a utilizar contraseñas complejas y robustas (más de 8 caracteres, formada por números, letras mayúsculas, minúsculas y símbolos) y que sean renovadas periódicamente.

Es muy recomendable utilizar un gestor de contraseñas, donde se almacenen todas las contraseñas de forma segura y que ayude a generar contraseñas robustas sin necesidad de tener que recordar todas, únicamente la contraseña maestra.

4. No instalar NUNCA software pirata o de fuentes no confiables

Además de por imperativos legales y las posibles multas, esta recomendación es porque un **software pirata** o que provenga de una fuente desconocida, no oficial, **puede haber sido alterado por un ciberdelicuente**. En ese caso lo que el software haga, además de su funcionalidad oficial, escapa por completo a tu control, pudiendo crear una puerta trasera en tu equipo u otras cosas peores.

5. Actualiza todos los equipos y dispositivos

Es obligatorio **aplicar las actualizaciones de seguridad** lo antes posible. Si bien algunas actualizaciones a veces pueden producir resultados inesperados, la actual "carrera armamentística" con la publicación de zero days y demás, obliga a darle prioridad a mantener el equipo actualizado.

En el momento en el que una vulnerabilidad se hace pública, cualquiera podría explotarla.

Pero es que, además, puede que ya hubiera sido descubierta por delincuentes antes y que estuvieran haciendo uso de ella.

6. Cifrado de discos con información confidencial

Otra recomendación es el **cifrado de todos aquellos discos** que contengan información confidencial. De este modo, en caso de robo o extravío de dichos discos (incluso sacándolos de los ordenadores físicamente), los delincuentes no podrían acceder a los datos.

Esto es **especialmente crítico en portátiles o unidades extraíbles** como pendrives o discos duros externos.

7. Copias de seguridad

Por último, recalcar la importancia de hacer copias de seguridad. Pero copias de seguridad de verdad. Copiar datos a otra carpeta cuando te acuerdes (o tener los archivos duplicados en la misma carpeta) no es una copia de seguridad.

Una copia de seguridad en condiciones se hará de **manera automática y en un soporte diferente del que almacene los datos originales**. De este modo si el soporte original sufre un accidente o similar, se podrán recuperar dichos datos. La recomendación es que estén en **una ubicación física diferente como podría ser una nube**.

A nivel de red

Las recomendaciones a nivel de red son, en general, más complejas y **requieren más conocimientos técnicos.**

1. Bastionado del router

Bastionar es el proceso de **asegurar un sistema mediante la reducción de vulnerabilidades** en el mismo.

Es más que probable que el proveedor de internet te haya entregado un router con una configuración por defecto en la que, por ejemplo, el usuario y clave del administrador son Admin/1234 o algo muy similar, así como otra serie de características que los hace vulnerables. Por tanto, con el proceso de bastionado hay que modificar la configuración para conseguir un nivel de seguridad más alto.

Algunas de las cosas que hay que hacer obligatoriamente son **cambiar la contraseña de administrador, la contraseña de la red, y el nombre del SSID** para que no incluya datos sobre el proveedor ni datos identificativos, así como desactivar WPS.

Estos cambios de configuración se pueden hacer siguiendo la guía de usuario que se entrega con el router o buscando guías en internet para tu modelo concreto.

2. División de redes

Una buena práctica es dividir la red de la empresa en subredes más pequeñas con control de acceso entre dichas redes.

Esta división **debe hacerse en función de los tipos de dispositivos y los usuarios que los utilicen**, con lo que se crean conjuntos de dispositivos / usuarios aislados entre sí.

Por ejemplo, si tienes un servidor web, éste debería estar en una subred para él, completamente aislado de la red en la que se encuentren los equipos con acceso a la contabilidad de la empresa.

Del mismo modo habrá equipos que no requieran conexión con internet, que habrá que aislar de los que sí lo necesiten, etc.

Algunos routers permiten, por ejemplo, hacer una división básica, como es crear una red de invitados separada de los usuarios corporativos.

3. Bloquea el acceso a la red a equipos no corporativos

Otra medida, que se considera más una buena práctica, consistiría en **no permitir nunca el acceso a la red corporativa a equipos no corporativos.**

Con esto nos referimos tanto a **invitados** como a todos aquellos **equipos que no estén controlados por la organización**, como por ejemplo, los móviles personales de los empleados. Dado que estos equipos no están sometidos a una política de seguridad de la empresa, no se puede garantizar que no hayan sido previamente infectados por malware y que una vez dentro de la red tengan acceso indebido a recursos.

4. Autenticación robusta

Debes asegurarte de utilizar la autenticación de red más robusta posible permitida por tu router.

Bajo ningún concepto es aceptable un nivel de seguridad por debajo de WPA2 PSK, aunque preferiblemente debería ser superior, por ejemplo WPA2 enterprise con autenticación radius.

Por tanto, a nivel empresarial es inaceptable utilizar configuraciones WEP o WAP.

5. Instalar un firewall de red

Aunque su utilidad hoy en día no es tanta como hace años, debido a la evolución en las arquitecturas de red, la instalación de un firewall de red sigue siendo un requisito imprescindible.

De este modo podrás **controlar las conexiones de entrada a tu red y los flujos de comunicación entre las subredes** que hayas definido.

6. VPN

Por último, queda mencionar el uso de VPNs. Una VPN o red privada virtual permite **establecer una conexión privada y cifrada.** Más información sobre VPN en nuestro blog:

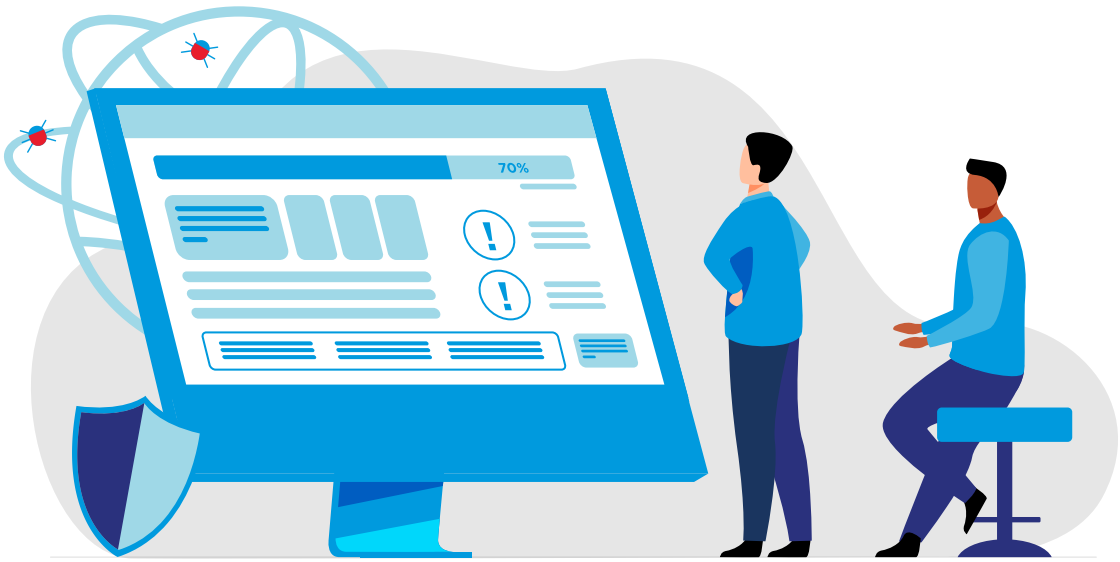
La solución Wefender de Tecteco protege tu red aunando todas estas funcionalidades en un sólo dispositivo. Infórmate aquí

7 CONCLUSIONES

La ciberseguridad se sustenta en tres pilares básicos: confidencialidad, integridad y disponibilidad.

Recuerda que **para los ciberdelincuentes no hay víctima pequeña**, siempre sacan una rentabilidad de cada ataque: datos para el mercado negro, dinero en forma de rescate o capacidad de proceso para llevar a cabo otros ataques.

Si quieres proteger tu negocio debes **tomarte en serio su seguridad digital y adoptar hábitos de ciberhigiene y medidas preventivas** que minimicen tu exposición a los riesgos más habituales que hemos revisado en este documento.



Acerca de TECTECO

TECTECO es una empresa de tecnología 100% española que nace con vocación I+D y especializada en ciberseguridad. Ha desarrollado y patentado la solución WEFENDER y la comercializa en modo de pago por uso (Secure WiFi as a Service – SwaaS) con el objetivo de cambiar el paradigma de la seguridad WiFi, acercando a pymes y hogares los niveles de seguridad de las grandes empresas.

Información

+34 91 756 92 64 | contact@tecteco.com
www.tecteco.com | www.wefender.es