aplimedia
software ERP en la Nube

GUÍA DE CIBERSEGURIDAD PARA PYMES

TODO LO QUE NECESITAS SABER PARA MANTENER TU EMPRESA SEGURA

94 453 57 25
info@aplimedia.com
www.aplimedia.com

Paseo del Arenal, nº5
Oficina 501
48005 Bilbao

¡Gracias por entrar en el mundo de la seguridad cibernética!

No te arrepentirás, seguro que sacas alguna conclusión interesante de este curso.

Soy Jon, de Aplimedia, y seré tu guía para este mini curso. No se trata de un curso técnico, tampoco te voy a meter miedo (¡eso lo dejamos para Halloween!). Lo haré tan sencillo y fácil de entender como sea posible.

En este breve curso, aprenderás los **conceptos básicos de la seguridad cibernética**, y, lo más importante, cómo tomar medidas realmente fáciles y prácticas para proteger todo tu contenido digital.

Puede ser que estés aquí porque ya has sido atacado o pirateado - tal vez tu página web o correo electrónico han sido atacados - pero espero que estés aquí antes de que eso suceda.

Explicaré los conceptos básicos y los pasos que puedes seguir para detener futuros ataques, y al final de este mini curso, sabrás perfectamente qué pasos tomar para reducir tus posibilidades de ser atacado.

¿Qué veremos a lo largo de esta guía?

Tendencias en ciberataques ..... pág. 4
Mitos sobre ciberseguridad ..... pág. 5
Tipos de ataques informáticos ..... pág. 7
- Phishing ..... pág. 7
- Malware ..... pág. 10
- Ataques de contraseña ..... pág. 13
- Ataques de denegación de servicio (DoS) ..... pág. 17

Uso de Internet en lugares públicos ..... pág. 18
VPN: ¿por qué utilizarla? ..... pág. 20
Teletrabajar con seguridad ..... pág. 22
Invierte en un hosting de calidad para tu web ..... pág. 23
Plugins y seguridad ..... pág. 25
Copias de seguridad ..... pag. 27
Plan de recuperación anti-desastres ..... pág. 29

Tendencias en ciberataques

Quiero comenzar esta guía ofreciéndote algunos datos que te ayuden a entender la importancia de la ciberseguridad en tu vida personal pero, especialmente, en tu empresa.

- Cada vez se sufren **más ataques informáticos** y muchos de ellos tienen éxito.
- Han aumentado las **víctimas de ransomware**, tanto personas físicas como empresas, muchas de las cuales terminan pagando por recuperar sus datos.
- El principal **problema** somos **las personas**: invertimos poco en formar y concenciar a los empleados sobre ciberseguridad y amenazas online.
- Las empresas cada vez más **se interesan en la seguridad** de sus plataformas informáticas y aumentan sus presupuestos.
- Las plataformas **analíticas y de machine learning** se empiezan a utilizar para detección de virus, ransomware…

¿Qué países son más vulnerables?

Los datos muestran que México y España son los países donde los ataques informáticos tienen más porcentaje de éxito.

**Porcentaje comprometido por, al menos, un ataque exitoso en los últimos 12 meses y por país.

Antes de continuar, analicemos algunos mitos:

1. Los ataques cibernéticos únicamente tienen como objetivo las grandes empresas.

INCORRECTO

Si bien atacar a grandes empresas tiene un mayor atractivo, en realidad, las PYMES se han convertido en el último sector en caer en las listas de éxitos de los atacantes.

¿Por qué? Porque las pequeñas empresas tienen muchos activos digitales que proteger, pero recursos limitados y pocos conocimientos de cómo protegerlos de manera efectiva.

2. "No recopilo ni guardo ningún detalle de mis clientes en mi web y uso software de CRM o automatización de correo electrónico de terceros, por lo que no soy un objetivo".

INCORRECTO

Tu sitio web no es objetivo de ataques informáticos únicamente por la información de tus clientes, ese es solo un tipo de ataque. Tu web puede usarse como host para ataques en otras webs, convirtiéndose en un robot que trabaja para un ciberdelincuente. También es posible que el objetivo del ataque sea dañar tu reputación profesional.

3. "Cuando navego en lugares públicos solo uso redes seguras o los datos de mi proveedor de telefonía, así que estoy bastante seguro".

INCORRECTO

El uso generalizado de dispositivos móviles y el acceso a Internet en lugares públicos ha provocado que los ciberdelincuentes adapten sus técnicas de ataque para explotar las vulnerabilidades en el software del teléfono o la conexión wifi / datos en espacios públicos.

4 “Trabajo con equipos y dispositivos iOS, que no pueden infectarse”

INCORRECTO

Si bien los Mac tienen un sistema operativo diferente, no son inmunes y pueden transmitir virus a otros ordenadores.

Si has entrado en pánico y no tienes claro qué hacer para protegerte ante ataques informáticos... ¡no te preocupes! Estoy para ayudarte.

¡Sigue, sigue leyendo los siguientes capítulos y serás un usuario informático más seguro!

En el próximo capítulo vamos a comenzar a analizar algunos ataques comunes de seguridad cibernética que afectan a las PYMES.

¡SIGUE LEYENDO!

Tipos de ataques informáticos: PHISHING

La suplantación de identidad se da cuando recibimos correos electrónicos, llamadas telefónicas o llegamos a sitios web que pretenden ser una persona u organización en la que confíamos. El objetivo es obtener tu información personal: contraseñas, detalles de tu cuenta bancaria o números de tarjetas de crédito.

Esencialmente, el **phishing es ingeniería social**, donde se crea un sentimiento de confianza a través de la manipulación psicológica y la explotación de la debilidad humana para robar su información personal.

La mayoría de **estos ataques son sutiles**: un mensaje de correo electrónico que te alerta de una factura no pagada o una violación de seguridad y te pide que sigas el enlace en el correo electrónico para resolver el problema de inmediato.

Otros tipos de ataques de phishing son **más agresivos**, ya que los ciberdelincuentes obtienen información personal que, accidentalmente, has puesto a disposición del público a través de las redes sociales.

El *spear phishing* también es un tipo de ataque común contra las PYMES. Hay varios tipos:

- *Spear phishing links*: se utilizan enlaces dentro del e-mail y, si pinchamos en ellos, nos descargamos malware.
- *Spear phishing attachments*: se adjunta un archivo malicioso en el mismo e-mail con el objetivo de que descarguemos directamente el malware.
- *Spear phishing via service*: para evitar la detección del malware se utilizan otros medios de comunicación, por ejemplo redes sociales o servicios externos a la empresa. También puede ser por webmail, ya que algunos servicios webmail no incorporan sistemas de detección de malware.

Algunos ejemplos de Phishing...

¿Tu también tienes unas mascota de la que te encanta subir fotos a redes sociales? Los ciberdelincuentes podrían estar observándote, dado que el uso del nombre de la mascota es bastante habitual en contraseñas, tanto personales como profesionales.

Recibes una llamada telefónica que te informa que el firewall de tu PC está desactualizado o caduca y te ofrecen un precio con un descuento increíble para instalar un nuevo software de seguridad.

Recibes un e-mail en tu correo empresarial, supuestamente de tu banco o cualquier otra fuente de confianza, y dicho correo te insta a hacer clic en un enlace sospechoso.

Un empleado publica datos en las redes sociales que proporcionan información confidencial de la compañía como parte de una estafa de ingeniería social.

¿Cómo detectar y prevenir ataques de Phishing?

- La **mala gramática** o los **errores ortográficos** son comunes en los correos electrónicos que son parte de una estafa de phishing.

- Los **enlaces sospechosos** en los correos electrónicos se pueden verificar al pasar el puntero del ratón, sin necesidad de hacer clic sobre el enlace. Puedes ver a dónde conduce el enlace, y la mayoría de las veces no coincidirá con el texto en el enlace dentro del correo electrónico. ¡No hagas clic!

- Si el mensaje en el correo electrónico crea una **sensación de amenaza y urgencia**, existe una buena posibilidad de que sea una estafa de phishing.

- Inspecciona las **direcciones de e-mails sospechosas**, aunque parezcan de un remitente de confianza. Si las inspeccionas detalladamente y detectas diferencias (una letra de más u ortografía alterada) es muy probable que sea phishing.

- Trata todas las llamadas telefónicas no solicitadas con escepticismo y sospecha. La mayoría de grandes empresas no llaman en frío.

- Si las llamadas telefónicas no solicitadas tienen un elemento de amenaza y urgencia, cuelga de inmediato.

- La herramienta más potente contra el phishing es la educación de los empleados: dedica tiempo y recursos para formarlos en ciberseguridad.

Tipos de ataques informáticos: MALWARE

Este es principalmente un término colectivo utilizado para referirse a una variedad de formas de software hostil o intrusivo, incluidos virus informáticos, gusanos, troyanos, ransomware, spyware y otros programas maliciosos. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

Estos son los tipos de malware más habituales:

- Los **virus, gusanos y troyanos**, en términos simples, son piezas de código malicioso que se utilizan para infectar tu PC o portátil. Los virus generalmente se adjuntan a un archivo (por ejemplo, un archivo ejecutable .exe) y se pasan entre las computadoras por correo electrónico, pero solo dañan los archivos si se ejecutan. Los gusanos son códigos maliciosos que pueden viajar sin interacción humana a través del intercambio de información en su sistema. Los troyanos parecen bastante inocentes, pueden disfrazarse de software útil, pero una vez descargados, pueden eliminar archivos o dañar tu sistema operativo.

- El **ransomware** retiene tus datos digitales o acceso como rehén hasta que se realice un pago al criminal.

- Las **botnets** utilizan tu PC o portátil como parte de un grupo de computadoras para bombardear otro sitio web con correos electrónicos no deseados o grandes cantidades de datos con la intención de poner el sitio web temporalmente fuera de servicio o robar información personal a gran escala.

- El **spyware** es un software que registra las actividades del usuario del PC o portátil, como las pulsaciones de teclas utilizadas para el acceso y el acceso con contraseña.

¿Cómo protegerte frente al malware?

Mantén actualizado tu sistema operativo

Sí, sé que puede ser molesto cuando estás trabajando, tienes una fecha límite que cumplir, y sabes que, si haces clic en “actualizar ahora” puedes quedarte parado entre 10 minutos y 24 horas. Sin embargo, si continúas posponiendo actualizaciones, cada minuto que no se ejecutan es otro minuto en el que algo puede salir realmente mal y causar daños permanentes (o al menos durante un período de inactividad muchísimo más largo que la propia actualización). Si no cuentas con mantenimiento informático, ¡este punto es todavía más importante!

Instala un firewall en tu sistema

Esto te protegerá de intentos externos de acceder o controlar tu ordenador. También puedes instalar firewalls de hardware en tu router para proteger la red, ya que un firewall de software solo protegerá el PC en la que está instalado.

Mantén actualizado tu software de firewall

Al igual que el sistema operativo, es importante mantener actualizado tu firewall para asegurarte de que estás cubierto/a ante todas las amenazas actuales. Los desarrolladores de firewall actualizan sus software continuamente, es por ello por lo que también debes mantenerlo actualizado.

Elimina o actualiza softwares antiguos

Si tienes un software antiguo en tu sistema que ya no utilizas o actualizas, elimínalo; de lo contrario, crearíamos una vulnerabilidad, una ruta para que los atacantes la exploten. Si dispones de actualizaciones que todavías no has instalado... ¡ejecuta la actualización!

Instala software antivirus en tu PC

Existen muchas versiones gratuitas de software antivirus con la opción de comprar actualizaciones para fines específicos. Ejecútalos regularmente o permite que se actualicen automáticamente para la protección antivirus en curso en tu sistema.

Tipos de ataques informáticos: ATAQUES DE CONTRASEÑA

Esto es exactamente lo que crees: un ataque que tiene como **objetivo obtener tus contraseñas** o las de tus empleados para poder acceder libremente a tus sistemas.

Estos tipos de ataques generalmente se clasifican como ataques de fuerza bruta: el atacante usa un software que prueba una y otra vez distintas contraseñas aleatorias con un enfoque de prueba y error para descifrar tu código e ingresar a tu sistema.

Los ataques de fuerza bruta son comunes en páginas web, donde los atacantes intentan obtener acceso al back-end o panel de administrador de la web para eliminar archivos, corromperlos, redirigir tu página a otro destino o usarla como un robot con fines maliciosos.

Si un atacante obtiene acceso a tu página web, incluso si no guardas datos de clientes en ella, los **daños que se pueden causar a tu reputación** pueden ser irrecuperables. Seguro que más de una vez te ha pasado que has intentado acceder a una página web de una empresa y se te ha redirigido a otra página con contenido pornográfico.

Incluso si recuperas el control de tu web y tu dominio... ¿crees que los clientes potenciales que experimentaron la redirección volverán a tu página?

El impacto y el coste de cambiar tu marca, dominio y, en general, arreglar tu reputación, no tienen precio.

¿Puedes permitirte no ser proactivo en la protección de tu información digital?

¿Cómo lograr contraseñas a prueba de ataques?

Opta por contraseñas largas

Los símbolos, números, mayúsculas, minúsculas... son elementos que nos pueden ayudar a construir una contraseña segura y potente, pero sin duda, el elemento más importante a la hora de escoger una contraseña a prueba de hackers es la **longitud**. Se ha desmostrado que es mucho más seguro utilizar una contraseña larga y simple (por ejemplo “lacasadelpueblodemitiapaca”) que una contraseña corta con mayúsculas, símbolos, números... (por ejemplo “c4rLo$”).

Comprueba cómo de segura es tu contraseña en https://howsecureismypassword.net/

Duración de las contraseñas

Es interesante aplicar un tiempo de expiración a las contraseñas para obligar a los usuarios a cambiarlas periódicamente, evitando siempre el utilizar contraseñas que ya han sido utilizadas previamente.

Autenticación en dos pasos

La autenticación en dos pasos reduce muchísimo las posibilidades de que los atacantes puedan acceder a información privada o sensible, ya que no basta con que descifren tu contraseña.

¿Cómo puedes evitar que te roben la contraseña?

Crea contraseñas seguras

Evita el uso de contraseñas que usen palabras demasiado cortas o demasiado simples. Sigue los consejos que te hemos dado acerca de cómo crear contraseñas seguras, utilizando contraseñas largas.

Cambia las contraseñas regularmente

Cambiar las contraseñas regularmente es una buena práctica para garantizar un mayor nivel de seguridad para tu información digital. Sé que es muy difícil recordar cada contraseña para cada programa o aplicación a la que accedes, pero el coste de no llevar a cabo esta práctica es mucho más alto.

Usa un administrador de contraseñas

Una buena manera de evitar tener que recordar cientos de contraseñas (y evitar la tentación de reutilizar las mismas contraseñas débiles) es usar un administrador de contraseñas.

Hay muchas opciones, yo te recomiendo LastPass. Solo necesitas recordar una contraseña maestra. Te permite realizar comprobaciones de seguridad de vez en cuando para detectar vulnerabilidades y programar recordatorios para cambiar de contraseña.

Cuidado con los empleados descontentos

Asegúrate de tener unos protocolos para eliminar los derechos de acceso y las contraseñas de cualquier empleado que deje de trabajar en tu empresa.

He visto a muchos empleados descontentos cambiar todas las contraseñas de las cuentas de redes sociales de una empresa y luego seguir publicando bajo el nombre de la organización...

Y te puedes imaginar que las consecuencias no son buenas.

Una vez más, un administrador de contraseñas puede ser muy útil para pequeñas y medianas empresas, pudiendo eliminar automáticamente todos los derechos de acceso de un empleados.

Tipos de ataques informáticos: ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)

Un ataque de denegación de servicio tiene como **objetivo interrumpir toda una red**: los atacantes envían un gran volumen de tráfico y datos a una web o sistema con el único propósito de sobrecargarlo con una gran cantidad de solicitudes de conexión.

Es como tratar de introducir más y más agua en un globo hasta que no cabe más y explota.

Para que esto funcione de manera efectiva, el atacante tendrá que haber "reclutado" una gran cantidad de ordenadores (¡sin que los usuarios lo sepan) para contribuir al ataque. Esto convierte tu PC en un zombie que trabaja en nombre del atacante.

¡Tu propio ordenador puede haber contribuido a un ataque DoS sin que lo supieras!

¿Cómo protegerte de ataques DoS?

- Audita tu tráfico de internet: ¿hay picos inusuales en el tráfico que no puedes explicar? Esto podría apuntar a un ataque DoS.
- El foco de los ataques DoS suele tener como objetivo cerrar sitios web comerciales, generalmente solicitando un rescate para que el sitio vuelva a funcionar.
- Mantén actualizados tus antivirus, cortafuegos y softwares. Cualquier grieta en tu armadura puede ser explotada.

Uso de Internet en lugares públicos

Estamos en una era en la que podemos trabajar literalmente desde cualquier parte del mundo. Tener un ordenador portátil, smartphone y conexión WiFi significa que podemos estar conectados en todo el mundo.

Las cafeterías están repletas de usuarios con portátiles que beben café con leche o tienen conversaciones en voz alta en sus teléfonos sin pensar ni preocuparse por la información confidencial que potencialmente están compartiendo públicamente.

Para una PYME es liberador no tener que depender de conexión a Internet por cable para realizar su trabajo. Simplemente basta con coger un equipo inalámbrico y trabajar: en trenes, aeropuertos, cafeterías o donde puedan obtener una conexión WiFi medio decente.

El problema es que hay algunas personas en este mundo dispuestas a usar estas **conexiones WiFi públicas** para **explotar y robar información privada** con fines maliciosos.

Todos los usuarios que utilizan su smartphone, tablet o portátil en un espacio público están sometiendo su información personal a un riesgo considerable porque sus datos pueden ser interceptados a través de redes WiFi públicas.

Si utilizas antivirus y cortafuegos ya vas un paso por delante, pero, ¿estás considerando los riesgos que entraña el simple hecho de acceder a Facebook o revisar tu e-mail desde una red WiFi pública? Probablemente no.

No sé qué opinas tú, pero yo no quiero renunciar a la conveniencia de conectarme a una red WiFi pública en centros comerciales, aeropuertos o cafés solo porque hay personas sin escrúpulos en el mundo al acecho para robar mis datos personales.

Entonces, ¿qué puedes hacer para proteger tu información digital en un espacio público?

El WiFi público es inseguro

En el momento en que inicias sesión en una red WiFi pública, ya te estás exponiendo a una amenaza. Asegúrate de estar conectándote a una conexión correcta y legítima. Muchos atacantes establecen conexiones falsas que se parecen a la de esa cafeterías, centro comercial, aeropuerto... y cuyo objetivo es que hagas clic.

Todos tus dispositivos están en riesgo

Tu teléfono y tu tablet son dispositivos potentes que almacenan una gran cantidad de datos. No los trates de forma distinta a un ordenador: los riesgos son los mismos. Instala y actualiza regularmente el antivirus de tu teléfono para escanear y limpiar potenciales amenazas.

No te conectes a páginas web sensibles en espacios públicos

Si estás navegando en un espacio público, no te conectes a la banca online ni a sitios donde se hayan almacenado datos de tu tarjeta de crédito. Son sitios web con mayor riesgo de exposición y ataque.

Comprueba tu configuración de red

Si bien tu ordenador puede estar libre de virus, al conectarte a una red pública podría infectarse o comprometerse debido a que otros dispositivos infectados están conectados a esa red pública.

VPN (red privada virtual): ¿por qué utilizarla?

En términos simples, una VPN es una tecnología que crea una **conexión encriptada** al navegar a través de una red insegura.

Se configura y se conecta a través de una red privada que impide que alguien vea lo que estás haciendo online. Un atacante podría ver que estás conectado a una red privada pero no podría monitorizar tu actividad.

Es como tener tu propia burbuja protectora que protege tus datos cuando navegas o accedes a Internet en espacios públicos.

Hay varias VPNs entre las que escoger. Una buena manera de comenzar a evaluar qué tipo de VPN necesitas es comparar los beneficios y las características con tus propios requisitos personales y de la empresa. ¿La necesitas solo para ti o tienes comerciales qe trabajan en la calle? Esto puede suponer una diferencia importante en el coste.

Estos son algunos de los beneficios de utilizar una VPN:

- Se puede instalar y usar una VPN en **varios dispositivos**, lo que garantiza el estar protegido en todo momento.
- Algunas VPN usan **encriptación de grado bancario**, lo que te mantiene súper seguro cuando navegas por la red.
- **Navegar de forma anónima** mantendrá tu actividad a salvo de miradas indiscretas.

- Algunas VPN ofrecen **eludir el contenido geo-restringido**, por lo que puedes falsear tu dirección IP (dirección única que identifica tu ordenador) para que parezca que estás navegando desde otro país .

- **Bloquea e intercepta datos de cookies** molestos que normalmente te siguen por Internet (¿harto de ese anuncio que aparece después de navegar en Amazon? Algunas VPN pueden bloquear esta actividad).

- Eso sí, como consejo, asegúrate de verificar que el proveedor de VPN no está registrando tu información en su sistema.

Recomendaciones para teletrabajar con seguridad

A la hora de teletrabajar, es importante tomar determinadas precauciones que nos permitan controlar el acceso a nuestros servidores por parte de los empleados.

Las medidas de seguridad variarán en función de tu infraestructra.

¿**No utilizas una VPN** para el acceso a tu servidor? Deberías limitar las conexiones estableciendo cuáles son las IPs de confianza. Esto puede ser un trabajo árduo dado que tienes que recopilar muchos datos y las IPs pueden ser dinámicas.

¿**Utilizas VPNs**? Recuerda tener una fuerte política de contraseñas y métodos de doble autenticación.

¿Cómo detectar comportamientos inusuales?

- Monitoriza si algún usuario se conecta a un servidor o servicio **fuera del horario de trabajo o en fin de semana**. Plantea la posibilidad de restringir los horarios de conexión.

- Establece una base de datos con la información de las **IPs públicas desde las cuales se conectan los usuarios**. Si detectas un cambio de IP que no concuerda, toma medidas. Por ejemplo, si ves que la IP de un usuario cambia, pero su proveedor sigue siendo el mismo, es posible que simplemente haya reiniciado el router y su IP haya cambiado. Si, por ejemplo, la IP cambia a una IP de China, deberías tomar medidas para verificar que tu sistema no se está viendo comprometido.

- **Monitoriza por recursos** directamente en los dispositivos: en los ordenadores, escritorios virtuales… Te ayudará a detectar si puede haber malware o bots comprometiendo tus sistemas y consumiendo recursos.

Invierte en el hosting de tu página web

No puedes permitirte el lujo de **ignorar la seguridad de tu página web**.

A lo largo de las páginas anteriores hemos visto cómo las páginas web pueden verse comprometidas por ataques de fuerza bruta, redireccionándolos a páginas web no confiables que pueden dañar permanentemente la reputación de tu empresa, tu marca y el funcionamiento interno de tu web.

Uno de los puntos clave a la hora de configurar y dar de alta una página web es escoger un **buen provedor de alojamiento o hosting web**, que te de ciertas garantías en cuanto a la seguridad de tus datos e infraestructura.

La tentación de escoger la opción de alojamiento más barata puede ser fuerte, sobre todo para una PYME. Puede ser que, si tienes una web, basaras tu decisión respecto al alojamiento en función de la cuota, si incluía o no el dominio, si incluía un maquetador web... Ignorando el apartado más importante: la seguridad. Pero lo cierto es que el impacto de no escoger bien y escoger alojamientos con seguridad pobre puede ser realmente desastroso.

¿Qué preguntarle a un proveedor de hosting para asegurarte de que estás tomando la decisión correcta?

¿Tiene una política de seguridad?
Muchos proveedores incluyen diversas prestaciones en su servicio de alojamiento web, pero dejan en tus manos la seguridad. A menos que cuentes con informáticos experimentados que sepan proteger tu sitio, este tipo de opciones no son adecudas.

¿Cómo protege el proveedor de hosting su propia red?
Al fin y al cabo, si su seguridad se ve comprometida, también la tuya se verá comprometida.

Si algo sale mal, ¿qué medidas toman para proteger tus datos y hacer que tu web vuelva a funcionar?¿en qué plazos?
Esto es particularmente importante para los propietarios de PYMES que se dedican al comercio electrónico: si tu web está caída, no puedes vender.

¿Tu proveedor ofrece un certificado SSL como parte de su paquete?
Esto es importante para la seguridad de los clientes que compran a través de tu web. Las transacciones de datos en tu web deben ser seguras y estar encriptadas.

¿Quién es responsable de actualizar el software y otras aplicaciones?
Si el proveedor dice ser responsable, asegúrate de que te lo dice por escrito. De lo contrario, busca un desarrollador web o experto en seguridad web que pueda mantener tu sitio actualizado. Todos tenemos un fontanero o un electricista en nuestra agenda, es hora de añadir un desarrollador web.

¿Cuál es su política de monitorazación de seguridad en tiempo real?
Hablo de verificaciones regulares de malware, verificaciones de firewall o listas negras de direcciones o actividades sospechosas.

Estos son buenos puntos de partida para empezar a considerar opciones de alojamiento realmente seguras. No importa si tienes un e-commerce o tu web es un simple escaparate de tus servicios... ¡la seguridad es lo primero!

Plugins y seguridad web

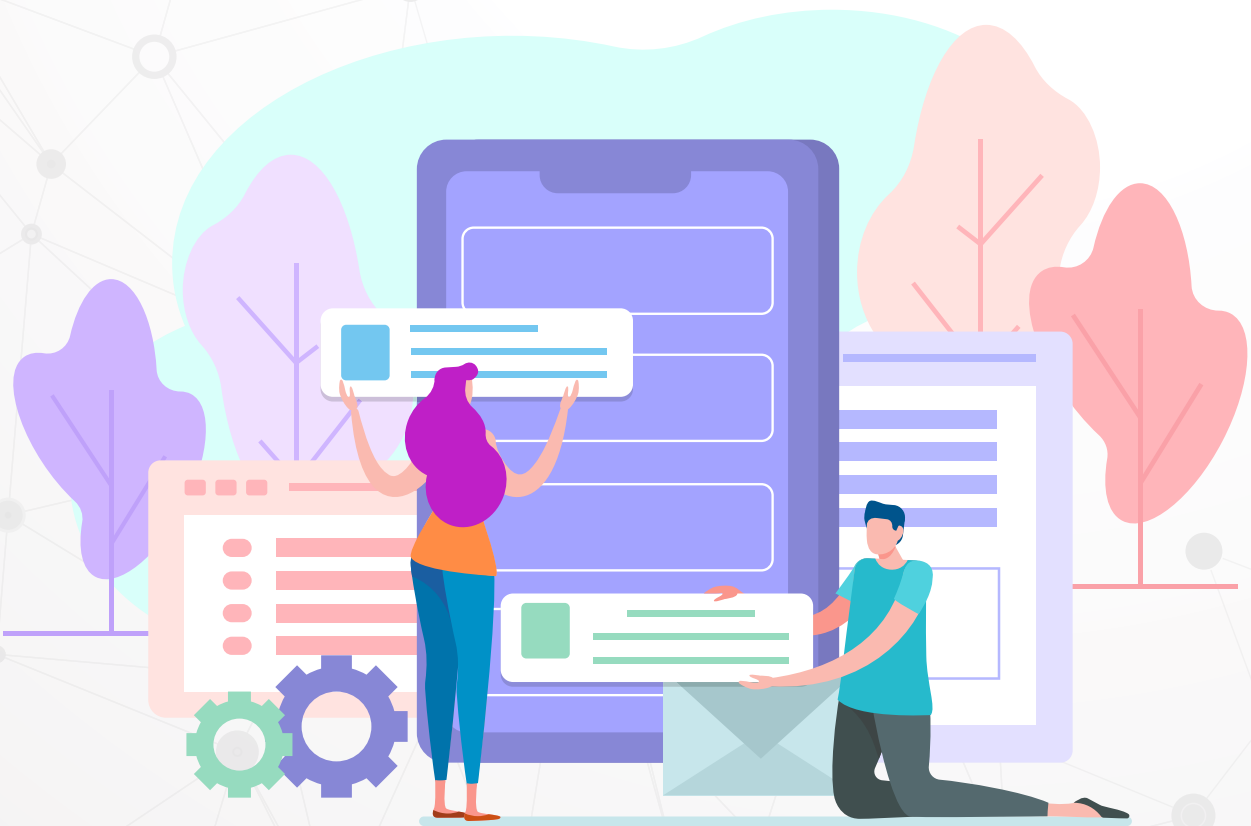
WordPress

Si eres usuario de WordPress, sabrás que hay literalmente cientos de plugins o complementos entre los que elegir para tu web.

Los plugins son pequeños “programas” que puedes instalar en tu página web para extender sus funcionalidades. Y son realmente útiles. Pero antes de ponerte a comprar plugins sin pensarlo, párate a pensar acerca de la seguridad y potenciales problemas que pueden acarrear.

Una página web con demasiados plugins puede experimentar problemas en cuanto al rendimiento y velocidad de carga. El número máximo recomendado de plugins instalados es de 10 a 12.

Sin embargo, hay otras consideraciones. Sí, lo adivinaste: ¿cómo de seguro es ese nuevo plugin? Admito que no existe un método infalible para detectar un plugin inseguro, pero puedes mitigar el riesgo planteándote unas cuantas preguntas.



Lista de verificación de seguridad de un plugin

- ¿Qué necesitas en el plugin? En lugar de comprar dos o tres, ¿puedes comprar **uno que haga todo el trabajo**?

- **Revisa las reseñas** cuidadosamente. Si un plugin tiene una calificación de 4 o 5 estrellas pero solo hay dos reseñas, mejor buscar otra alternativa hasta que encuentres más información.

- **Busca en Google el nombre del plugin** más la palabra **"seguridad" o "vulnerabilidades"**. Si existen razones para desconfiar del plugin lo más probable es que lo descubras haciendo una búsqueda rápida en Google. Recuerda "[nombre del plugin] + seguridad".

- Comprueba cuándo fue **la última vez que el desarrollador actualizó** el plugin. Si ha sido dentro del último mes probablemente sea un plugin bastante seguro. La regla de oro es no instalar plugins para los que el desarrollador ya no realiza actualizaciones: garantizan agujeros de seguridad en tu código, que estará desprotegido ante posibles amenazas, además de poder causar potenciales incompatibilidades con futuras actualizaciones de WordPress.

- Tómate tu tiempo y **lee los comentarios**. Los usuarios suelen ser bastante honestos y expresar su descontento sin ningún tipo de reparo.

Copias de seguridad de tu página web

Todo va a las mil maravillas. Tienes una página web magnífica, que recibe tráfico constantemente y... de repente... ¡BOOM! Eliminas un poco de código por error, te pierdes una actualización crítica de WordPress, tu web se infecta por un malware o estás migrando tu página a otro alojamiento y de repente simplemente desaparece.

Pero no pasa nada, **haces copias de seguridad de tu web a menudo**... ¿no?

Las copias de seguridad regulares son un tema que a menudo se pasa por alto pero que es clave para operar una página web exitosa y segura. Son una parte esencial del mantenimiento de una web, ningún sitio web es inmune a un poco de drama técnico de vez en cuando. Así que, solo porque creas que no vas a necesitarlas (con suerte), no deberías dejar de hacerlas a menudo.

¿Mi recomendación? **Haz una copia de seguridad cada día**, especialmente si tu página recibe mucho tráfico diariamente o si haces cambios regularmente.

Como **mínimo**, esto debe hacerse **mensualmente** para los **archivos** del sitio y **semanalmente** para los archivos de la **base de datos**, pero, sin duda, lo

más recomendable, es que hagas una copia de seguridad **cada vez que hagas cambios importantes** en tu web, como publicar una entrada en el blog o hacer algún cambio en el código (si tienes conocimientos más avanzados de desarrollo web).

Las copias de seguridad también deben realizarse antes de instalar una nueva versión de WordPress para que, si algo sale mal, puedas volver a la versión anterior.

Hay muchas formas de realizar copias de seguridad. Si utilizas WordPress existen muchos plugins, algunos más técnicos que otros.

Algunas consideraciones al pensar cuál es el método de respaldo más adecuado para tu página:

- ¿Se puede automatizar la copia de seguridad de modo que puedas ajustarla a un horario y olvidarte?
- ¿La copia de seguridad se almacena automáticamente en Dropbox u otro proveedor de almacenamiento en la nube para facilitar el acceso? Si dejas las copias de seguridad únicamente en manos de tu proveedor y éste es víctima de un ataque, tú también te verás perjudicado. Es mejor almacenar las copias en otro lugar.
- ¿Se pueden restaurar fácilmente las copia de seguridad? Está muy bien hacer una copia de seguridad de los archivos, pero ¿se pueden volver a instalar fácilmente?
- Considera la contratación de algún servicio en línea que realice y almacene tus copias de seguridad a cambio de una tarifa mensual.

Plan de recuperación anti-desastre

En todo el mundo, todas las empresas, no importa el sector o la industria, todas están siendo objetivo de ataques ransomware cada minuto. España es, de hecho, uno de los países donde este tipo de ataque tiene un mayor porcentaje de efectividad.

La prevención es importante, pero no es el único punto a tener en cuenta: debemos tener un **plan en caso de que seamos víctimas de un ataque** y éste tenga éxito. Este plan debe incluir puntos como:

- **Copias de seguridad continuas**. Cuando más corto sea el rango de tiempo de recuperación mejor.
- **Movilidad de cargas**. Comprobar que podemos restaurar una copia de seguridad de forma fácil, rápida y sin errores.
- **Soluciones Multi-Cloud**.

El objetivo es buscar un equilibrio

Cuando hablamos de invertir presupuesto en algo que puede pasar o no, es difícil calcular cuánto invertir. Sobre todo cuando no tenemos cuantificados los riesgos. La cuestión es intentar organizarnos y medir, de algún modo.

Para ello podemos basarnos en el *Recovery Point Objective* (RPO) y el *Recovery Time Objective* (RTO).

El ***Recovery Point Objective* o RPO** es la cantidad de datos que consideramos admisible perder desde la última copia de seguridad. Por ejemplo, podríamos considerar admisible recuperar datos de hace 24 horas pero irnos a 2 o 3 días atrás ya sería demasiado.

El ***Recovery Time Objective* o RTO** es el tiempo entre que cae nuestra actividad y volvemos a levantarla totalmente.

El reto es más bien organizativo. Se trata de traducir este punto de recuperación y tiempo de recuperación en un valor económico y cotejarlo con el coste del despliegue y mantenimiento del plan de recuperación antidesastre.

Todo depende de tu negocio: por ejemplo el RPO y RTO será mucho más bajo si hablamos de e-commerce, pero si nuestra página web es simplemente un "escaparate" de nuestros servicios o productos probablemente podremos permitirnos un RTO y RPO algo más alto. Si hablamos de instituciones sanitarias o financieras, directamente es inadmisible perder cualquier tipo de dato.

Plantéate cuál sería la pérdida económica en distintos escenarios de pérdida de datos y tiempo de recuperación y escoge el plan que mejor se adapte a tus necesidades y presupuesto.

¡Y hasta aquí esta guía de ciberseguridad para PYMES!

Gracias por llegar hasta el final y gracias por tomarte el tiempo para investigar acerca de seguridad informática.

Espero que te haya resultado útil y que pongas en práctica todo lo aprendido para ponérselo realmente difícil a los hackers. ¡Invertir en aprender e implementar seguridad es invertir en tranquilidad!

aplimedia
software ERP en la nube

Sobre Aplimedia

Empresa de desarrollo de software con más de 25 años de experiencia en el desarrollo de soluciones ERP para PYMES de todo tipo de sectores y actividades.

www.aplimedia.com — info@aplimedia.com — 94 453 57 25 — Bilbao (España)