DECÁLOGO

DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD PARA PYMES

estamos seguros

cepreven

CEPYME
CONFEDERACIÓN ESPAÑOLA DE LA PEQUEÑA Y MEDIANA EMPRESA

unespa ASOCIACIÓN EMPRESARIAL DEL SEGURO

DECÁLOGO

DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD PARA PYMES

Uno de los principales errores que cometen las pymes en materia de ciberseguridad es pensar que son demasiado pequeñas como para constituir un objetivo rentable y, en consecuencia, que no están expuestas a sufrir ataques cibernéticos.

Sin embargo, la realidad actual muestra exactamente lo contrario. Son precisamente las pequeñas empresas, o los particulares, las víctimas de una gran parte de los ataques. Las razones son muchas:

- Son más fáciles de acceder.
- No están suficientemente protegidas.
- Se pueden utilizar posteriormente como plataformas o vehículos para lanzar ataques a objetivos de mayor importancia.
- Son repositorios de información que se puede aprovechar para otros fines delictivos.

Todo esto hace que las pymes estén, hoy por hoy, muy expuestas a incidentes o ataques informáticos. Sin embargo, muchas no son conscientes de que las consecuencias de estos percances pueden ser muy graves e, incluso, amenazar su propia supervivencia.

Para evitar ser víctima de un ataque o, si se produce, tener capacidad de reacción, minimizar su impacto, garantizar la recuperación y, fundamentalmente, asegurar la continuidad del negocio, es preciso implantar en las pymes una serie de buenas prácticas en materia informática.

En este documento se presenta un decálogo de unas buenas prácticas sencillas, que se pueden aplicar por parte de pequeñas y medianas empresas sin experiencia en ciberseguridad. Estas indicaciones sirven de ayuda para proteger un negocio de ataques e incidentes cibernéticos, sin tener que realizar grandes inversiones ni contratar técnicos especializados.

1 DEFINA Y APLIQUE UNA POLÍTICA DE CIBERSEGURIDAD

- **Defina y documente** una política corporativa de seguridad cibernética.
- **Elabore** la política en base a un análisis de riesgos (activos, vulnerabilidades y amenazas).
- **Incluya** en la política un plan de ciberseguridad, que contemple un presupuesto específico, los riesgos identificados y las medidas a adoptar como, por ejemplo, la contratación de un seguro de riesgos cibernéticos.
- **Desarrolle** la política por medio de un plan de protección y reacción en caso de incidentes o ataques cibernéticos (Plan de ciberseguridad o de respuesta a incidentes).
- **Documente** esta política y difunda y haga cumplir el plan por parte de todo el personal de la compañía.
- **Asegure** que no se utilizan procedimientos informales o no establecidos en la política de seguridad cibernética.
- **Diseñe** un plan sencillo, en el que se detalle de forma simple y clara los activos a proteger y las normas o procedimientos a cumplir por todo el personal, así como los roles y responsabilidades de cada uno de ellos.
- **El plan** puede elaborarse tomando como base las actividades y acciones a adoptar en cada uno de los otros apartados de este decálogo.
- **Haga** un seguimiento periódico de la implantación del plan y actualícelo en consecuencia.

2 ASEGURE Y PROTEJA SUS DATOS E INFORMACIÓN

- **Documente y mantenga** operativo y actualizado un plan de *back-up* (respaldo o copia de seguridad) de sus datos e información, incluyendo la configuración de los sistemas y de las aplicaciones. El plan debe incluir:
  - **Relación** de activos que deben respaldarse obligatoriamente, por su importancia o carácter crítico, detallando su ubicación física o virtual.
  - **Periodicidad** o frecuencia de realización de la copia de respaldo.
  - **Periodo** de tiempo en que deben conservarse las copias efectuadas.
- **De acuerdo** con lo establecido en el plan de *back-up*, haga copias de seguridad de sus datos e información con periodicidad, manual o automáticamente, incluyendo la que se ha almacenado en la nube.
- **Realice** las copias de respaldo en unidades de almacenamiento físico independientes (disco duro, servidor, etc.) y guárdelas en lugar seguro distinto de aquel donde se encuentran los equipos cuyos datos e información se han resguardado.
- **Verifique** periódicamente que la copia de seguridad puede restaurarse sin fallos ni pérdidas, y asegúrese de que la aplicación o *software* de respaldo funciona.
- **Mantenga** actualizado y disponible el *software* de arranque de los sistemas.
- **Documente y mantenga** un plan de clasificación, protección y utilización de la información sensible, donde se identifique:
  - **Qué** información es crítica para la empresa y dónde se encuentra almacenada.
  - **Cuál** es su nivel de clasificación (libre o pública, confidencial, secreta...) y como se distinguirá cada nivel.
  - **Quién** tiene acceso a cada uno de los niveles y en qué condiciones.
  - **Normas** de uso de esta información, borrado y destrucción incluidos, conocidas por todo el personal de la empresa, incluyendo las posibles consecuencias de su incumplimiento.
- **En caso** de almacenamiento virtual o en la nube:
  - **Utilice** servicios que aseguren el almacenamiento seguro de datos e información y la disponibilidad para recuperar (restaurar) los datos copiados.
  - **Cifre o proteja** de alguna otra forma la información sensible durante su transmisión y almacenamiento y utilice servicios que envíen notificaciones cuando se produzcan eventos (cambios, borrado, almacenado, descarga, etc.).
  - **Asegure** la confidencialidad, integridad y disponibilidad de datos e información alojados en la nube mediante contrato con el proveedor donde se especifiquen las responsabilidades de cada parte.

3 UTILICE LAS REDES DE FORMA SEGURA

- **Utilice** un cortafuegos (*firewall*) para proteger la red, bien habilitando el propio del sistema operativo o instalando uno de los disponibles en el mercado (libre o con licencia).
- **Si la empresa** dispone de una red *wifi*, asegúrese de que esté oculta configurando el punto de acceso inalámbrico para que no transmita el nombre de la red (SSID; *Service Set IDentifier* o identificador del conjunto de servicios).
- **Asegúrese** de igual forma de proteger con contraseña (cambiando la que viene preinstalada) de modo que solo pueda acceder a ella el personal autorizado.
- **Si es posible**, configure la red *wifi* de manera que sus usuarios autorizados no conozcan la contraseña.
- **Si utiliza** una red *wifi* abierta, para uso de invitados o clientes, debe configurarse de forma separada a la de la empresa.
- **Establezca** políticas de descarga e instalación de aplicaciones por medio de la red de forma que solamente pueda hacerlo el personal debidamente autorizado.
- **Defina** una política de navegación segura por la web que incluya aspectos tales como los siguientes:
  - **Utilizar** contraseñas fuertes y cambiarlas periódicamente. Una contraseña fuerte es aquella que combina letras, números y otros caracteres, junto con mayúsculas y minúsculas.
  - **No descargar** archivos y aplicaciones *online* o hacerlo solamente de sitios web certificados.
  - **No hacer clic** sobre enlaces desconocidos o sospechosos o en todo caso sin antes verificar la dirección web completa.
  - **No utilizar** las redes sociales personales en la red corporativa.
  - **Al realizar** transacciones *online*, verificar que se utiliza una conexión segura (https en lugar de http).
  - **Efectuar** regularmente un borrado de *cookies* y rastros de navegación.

4 PROTÉJASE CONTRA EL MALWARE (CÓDIGO MALICIOSO)

- **Asegúrese** de que todos los equipos de la empresa están equipados con *software* antivirus y *antispyware* y que se actualizan regularmente.
- **Asegúrese** de que todos los equipos que puedan ser utilizados para correo electrónico están equipados con filtros *antispam*.
- **Configure** sus aplicaciones para que instalen las actualizaciones automáticamente.
- **En caso contrario**, instale los parches de seguridad proporcionados por los proveedores en cuanto los reciban.
- **Si utiliza** servicios en la nube, asegúrese de que dispone de protección contra el *malware*, actualice los parches y mantenga el *software* de seguridad.

5 UTILICE EL CORREO ELECTRÓNICO DE FORMA SEGURA

- **Defina** una política de utilización segura del correo electrónico que incluya aspectos tales como los siguientes:
  - **No abrir** mensajes si no se conoce al remitente o si son inesperados.
  - **Sospechar** de los mensajes que no están dirigidos directamente a la persona destinataria o no utilizan su nombre correcto.
  - **No responder** ni reenviar correos del tipo cadena (pidiendo que se reenvíe a los contactos).
  - **Ser** muy cuidadoso y precavido al hacer clic en cualquier enlace o abrir un archivo adjunto.
  - **Utilizar** un filtro *antispam* para correo electrónico no deseado.
  - **Eliminar** mensajes de *spam* sin abrirlos.
  - **No compartir** la dirección de correo electrónico en línea a menos que sea necesario.
  - **Configurar**, si es posible, una dirección de correo electrónico diferente para utilizarla en formularios *online* o para transacciones.
  - **Disponer**, en la medida de lo posible, de cuentas de correo diferentes para uso personal y empresarial o comercial.
  - **Verificar** la autenticidad de los mensajes sospechosos por otros medios (teléfono, etc.) utilizando datos de contacto de una fuente segura (no los del correo).
  - **Asegúrese** de tener instalado un *software* antivirus actualizado en cualquier dispositivo utilizado para acceder al correo electrónico.
  - **Si es posible**, proteja sus cuentas de correo electrónico con la autenticación multifactor (más de una contraseña).

6 ASEGURE EL ACCESO REMOTO Y FÍSICO A SISTEMAS Y EQUIPOS

- **Defina** una política de acceso remoto seguro a sistemas y equipos que incluya aspectos tales como los siguientes:
  - **Impedir** el acceso o el uso de equipos por parte de personas no autorizadas.
  - **Utilizar** contraseñas fuertes, diferentes para cada equipo o persona.
  - **Actualizar** (cambiar) las contraseñas periódicamente.
  - **Asegurar** que no se almacenan o mantienen las contraseñas en los equipos y sistemas (de forma especial en la navegación web).
  - **Proporcionar** a todo el personal acceso individual, con cuenta de usuario y perfil diferentes, no compartido.
  - **Proporcionar** acceso exclusivamente a los sistemas, equipos y funciones imprescindibles para desarrollar su labor.
  - **Otorgar** privilegios de administración solamente al personal estrictamente necesario.
  - **Limite o restrinja** el acceso físico al *hardware* de equipos y sistemas.
  - **No sitúe o proteja** conexiones de red en zonas de acceso público de la empresa.
  - **Almacene** los dispositivos portátiles no utilizados en lugares seguros.
  - **Asegurar** que todo el personal usa contraseñas seguras en los dispositivos móviles.
  - **Asegurar** que los dispositivos móviles no se configuran para iniciar sesión automáticamente.
  - **Utilizar**, si es posible, para el acceso a sistemas y equipos la autenticación multifactor (solicitar más de una contraseña).
  - **Suprimir** los privilegios de acceso remoto al personal que ya no los necesita o no sigue en la empresa.
  - **En caso de utilización** de servicios en la nube, debe conocerse su capacidad de asegurar un acceso protegido, a ser posible con autenticación multifactor, y con privilegios diferentes, limitando al máximo posible el número de usuarios permitidos.
  - **Siempre que** sea posible utilizar aplicaciones *software* del tipo VPN (red privada virtual) para acceder de forma remota.

7 PROTEJA LOS DISPOSITIVOS MÓVILES Y LA INFORMACIÓN QUE CONTIENEN

- **Evite** en lo posible que los dispositivos móviles contengan información de la compañía o tengan acceso a la red.
- **En caso** contrario, protéjalos con contraseña, cifre los datos e instale en ellos aplicaciones de seguridad (contraseñas y antivirus) que eviten el robo de información.
- **Asegúrese** de que tengan actualizado el último *firmware*, descargado del sitio web o de la aplicación del fabricante.
- **No utilice** dispositivos móviles que no permitan protección. En caso de hacerlo, evite conectarlos a la red.
- **Asegúrese** de configurar y cambiar las contraseñas preinstaladas al utilizar un nuevo dispositivo móvil.
- **No utilice** dispositivos móviles con información de la empresa en redes *wifi* o con equipos públicos.
- **Mantenga** al día un sistema de registro de seguimiento de utilización o préstamo de dispositivos móviles de la empresa.
- **Establezca** una política de utilización segura de medios de pago electrónicos (tarjetas, teléfonos, etc.).
- **Establezca** procedimientos de actuación en caso de pérdida o robo de un dispositivo móvil.

8 MANTENGA SUS APLICACIONES ACTUALIZADAS

- **Asegúrese** de tener actualizado todo el *software* de la compañía, lo que incluye:
  - **Actualice** periódicamente sistemas y equipos, fijos y móviles, configurando actualizaciones automáticas o de forma manual.
  - **Mantenga** y actualice las protecciones de seguridad utilizadas por su empresa. Esto puede incluir crear copias de seguridad, actualizar el *software* de seguridad, cambiar las contraseñas regularmente, etc.
  - **Asegúrese** de que los sistemas operativos están actualizados, incluyendo los parches proporcionados por el proveedor.
  - **Actualice** los navegadores web.
  - **Verifique** regularmente, e instale en su caso, el *software* de seguridad (antivirus, cortafuegos...).
  - **Asegúrese** que los proveedores de servicios en la nube mantienen actualizados las aplicaciones contratadas.
  - **Si el personal** de la empresa utiliza sus propios dispositivos móviles para desarrollar su labor, asegúrese de que tiene actualizadas sus aplicaciones, de forma especial la de seguridad.
  - **Asegúrese** de que los dispositivos tengan el último *firmware*, descargado del sitio web o la aplicación del fabricante.
  - **Asegure** los equipos y dispositivos de red (puntos de acceso inalámbrico, servidores, etc.) con parches de seguridad actualizados.

9 DISEÑE Y PONGA EN PRÁCTICA UN PLAN DE RESPUESTA A INCIDENTES

- **Diseñe, aplique y mantenga** un plan de respuesta a incidentes, no solamente ataques, para reaccionar y responder en caso de que se produzcan, minimizar el impacto y asegurar la continuidad del negocio. Incluye normalmente puntos como:
  - **Identificación** de activos críticos (datos, información, equipos, etc.).
  - **Distribución** de roles y responsabilidades entre el personal de la empresa.
  - **Información** necesaria (listados de contactos, teléfonos, alarmas, etc.).
  - **Forma de proceder** ante un incidente o ataque.
  - **Forma de proceder** ante el robo o pérdida de información.
  - **Forma de proceder** ante el robo o pérdida de un equipo.
  - **Forma de proceder** ante un bloqueo o parada de un sistema o equipo.
  - **Procedimientos** para informar después de un incidente o ataque.
  - **Disponibilidad** de potencia redundante para fallos de energía.

10 CONCIENCIE, INFORME Y FORME A TODO EL PERSONAL DE LA COMPAÑÍA

- **Asegúrese** de que todo el personal conoce sus responsabilidades en materia de ciberseguridad, así como la forma de proceder en caso de incidente o ataque cibernético.
- **Organice** regularmente campañas de información y concienciación del personal de la compañía en materia de ciberseguridad:
  - **Utilización** de equipos y dispositivos.
  - **Políticas** de contraseñas, correo electrónico, técnicas de ingeniería social (*phishing*, etc.).
  - **Uso** de redes sociales y navegación web.
  - **Tipos** de ataques más comunes (*phishing, ransomware*, etc.).
- **Forme** sobre las políticas de seguridad en red a todo el personal que tenga acceso a Internet o a la red interna.