digitalPYMES: CIBERSEGURIDAD EN LA PYME

neo managing mobility

DIGITAL PYMES

neo managing mobility

NEO managing mobility S.L.

C/ Pollensa 2 Edificio Artemisa 17
28290 Las Rozas - Madrid
T. +34 91 575 18 06
neo@neo-si.com

DigitalPYME: Ciberseguridad en la PYME

Septiembre de 2018

INTRODUCCIÓN

NEO Managing Mobility *es una empresa de software dedicada al desarrollo e implantación de sistemas de información con un alto nivel de especialización en la transformación digital de empresas y organizaciones a través de la tecnología.*

Contamos con una amplia experiencia en proyectos de optimización y movilización de procesos empresariales para grandes compañías nacionales e internacionales en más de diez países.

Además de nuestra capacidad para participar en proyectos TI y de transformación digital, nuestra actividad orbita en torno a dos plataformas SaaS (*"Software as a Service"*) en las que hemos concentrado buena parte de nuestro conocimiento:

Work&Track Fleet GPS es una plataforma IoT destinada a la gestión de flotas y activos móviles (vehículos, personas, cargas, etc.). El sistema, además de la gerencia de los propios activos (control de coste, mantenimiento, auditoría, etc), permite su geolocalización, trazabilidad de toda su actividad, optimización del comportamiento y monitorización de otros aspectos que se consideren relevantes (consumo de combustible, modos de conducción, temperatura, tacógrafo digital, etc.).

Work&Track Mobile es una innovadora plataforma orientada a la movilización de procesos empresariales. El sistema está diseñado para que cualquier empresa, independientemente de su tamaño, pueda transformar sus procesos a través de la movilidad mejorando la gestión de personal desplazado. Entre otras funciones, con Work&Track Mobile se facilita la geolocalización del personal de campo, la organización de tareas de campo (despacho de órdenes inteligente, optimización de rutas, etc.) y el reporting de actividad (con formularios y procesos personalizados).

El ecosistema de **Work&Track,** comercializado como servicio con un coste mensual (10 €/usuario), elimina las barreras de coste y plazo que habitualmente acompañan a este tipo de tecnologías lo que nos ha permitido, en los últimos años, sumar más de 200 pequeñas y medianas empresas a nuestra cartera de cliente.

Esta realidad nos ha permitido darnos cuenta que son la PYMES las grandes olvidadas de la digitalización. Un olvido que, cada vez con más fuerza, está generando una brecha competitiva, y de niveles de servicio, entre pequeños y grandes que amenaza seriamente la viabilidad empresarial de algunas compañías.

Por ello, y más allá de nuestra apuesta de producto accesible para la PYME, desde NEO queremos contribuir a la transformación de las pequeñas empresas. Por ese motivo presentamos la iniciativa **DigitalPYME** donde, periódicamente, abordaremos, desde un punto de vista estrictamente práctico, cómo una pequeña empresa debe emprender su transformación digital.

Estamos convencidos de que, con la orientación necesaria, cualquier empresa puede acceder a la tecnología más avanzada compitiendo, de tú a tú, con los grandes actores de cualquier sector.

CIBERSEGURIDAD EN LA PYME

Recientemente un gran amigo y cliente de NEO nos contó que el sistema informático de su empresa, donde almacenaba todos los datos de clientes, contabilidad y todos los trabajos en curso, había sido infectado por un virus.

¡Menuda faena!

La jornada laboral previa al ciberataque transcurrió con normalidad, pero, al volver al día siguiente, todos los ordenadores de la empresa, el servidor donde tienen instalado su ERP (programa de gestión) e incluso la copia de seguridad habían sido infectados con un virus de tipo "Ramsonware" (de esos que bloquean toda la información del ordenador, cifrándola y exigiendo un pago por recuperarla).

Por desgracia, tras invertir varios días en un vano intento de recuperar la información, no tuvieron más remedio que darla por perdida. A pesar del tremendo coste que les ha supuesto, al menos les queda el consuelo de que, por su actividad, no han tenido que echar el cierre. Otros no tuvieron tanta suerte.

Todo esto nos ha hecho reflexionar sobre los peligros a los que están expuestas las pequeñas empresas y organizaciones que ven en la ***Ciberseguridad*** un concepto costoso, fuera de su alcance, y por el que tampoco deben preocuparse demasiado. Después de todo, ¿quién querría atacar a una Pyme? La realidad, como ha podido comprobar nuestro querido amigo, es muy diferente. Cualquier empresa u organización está expuesta a los peligros derivados de la *ciberdelincuencia*: virus, robo de datos, suplantación de identidades, etc.

Por ello queremos dedicar este primer **DigitalPYME** a la ciberseguridad. Estamos convencidos que tomando un conjunto de medidas básicas, y con un nivel de inversión mínimo, cualquier empresa puede alcanzar un nivel más que aceptable de protección para evitar este tipo de desastres.

MENTIRAS Y VERDADES

Si inviertes en tener la mejor alarma, la mejor cerradura o las mejores cámaras de seguridad ¿por qué no inviertes en el mejor antivirus?

La seguridad en Internet es una de las mayores preocupaciones del siglo XXI y parece que en las pequeñas empresas no queremos darnos cuenta de ello. Siempre pensamos que el ladrón se colará por la ventana, pero los asaltos que más dinero cuestan a cada vez más empresas se hacen a través de un cable de 5mm.

El INCIBE (Instituto Nacional de Seguridad) cifra en 14.000 millones de euros el coste de los ciberataques, sólo en España, durante 2017. Si lo comparamos, por ejemplo, con los 4.000 m€ que se roban o hurtan en tiendas, los 3.500 m€ en bancos y cajeros, los 1.500 m€ sustraídos por carteristas o los 3.900 m€ que se derivan de asaltos a viviendas nos podemos hacer una idea de la magnitud e importancia de la ciberdelincuencia.

“A mí nunca me pasará”, “No pasa hasta que pasa”, “Fíjate, pensaba que nunca me iba a pasar”: éstas son las frases que oirás y que marcan el antes y el después de un ataque o desastre informático.

Los *ciberdelincuentes* no diferencian entre empresas grandes o pequeñas, ni entre españolas o inglesas, ni tampoco entre las que tienen el edificio más grande que el resto. Quizá si analizamos los mitos que hay en torno a la seguridad nos podremos dar cuenta de su carácter global:

· *La ciberdelincuencia requiere un altísimo nivel de sofisticación:*

Esta es, quizá, la primera mentira vinculada a la ciberseguridad. Quizá influenciada por el cine, o las series de televisión, donde la figura del ciberdelincuente siempre encaja con el arquetipo de super-experto en informática, criptografía y programación.

La realidad es, desgraciadamente, mucho más mundana. Un ataque informático puede realizarlo cualquiera con unos conocimientos muy básicos. Para realizarlo no es necesario saber programar, ni tener demasiados conocimientos sobre seguridad o ser un experto en criptografía: basta con bajarse una aplicación de Internet y seguir un sencillo tutorial. Y hay miles de programas y tutoriales por toda la red así que un adolescente con algo de tiempo libre, un (ex)empleado desleal, un competidor resentido o un cliente enfadado pueden crearnos un problema en pocos minutos, sin gastarse un euro y sin tener que recurrir a ningún experto.

· *A las PYMES no nos afectan, ¿quién va a perder el tiempo atacándonos?*

Esta es la segunda mentira de la ciberseguridad. Creemos que, al ser una PYME con pocos trabajadores, nadie se tomará la molestia de atacarnos. Pues bien, el 95% de los ataques son realizados por ciberdelincuentes con herramientas que atacan a millones de ordenadores al mismo tiempo (las mismas que describíamos en el punto anterior y que no requieren de gran pericia para su uso).

Esto quiere decir que a los ciberdelincuentes (y ya hemos visto que para serlo no es necesario ser ningún experto) les interesa atacar a todos los ordenadores posibles y lo hacen de manera automática y casi simultánea. Tú eres un objetivo porque eres un número más de los miles que quieren conseguir.

· *Proteger una empresa es carísimo.* Mentira.

Como decíamos al principio, una empresa protege sus instalaciones con alarma, rejas o puertas de seguridad por el miedo a intrusiones no deseadas. A mayor escala, un banco, por ejemplo, se protege además con cámaras de seguridad, cristales blindados, puertas bloqueantes y unas alarmas carísimas. Esta similitud puede extrapolarse a los sistemas de seguridad informática: una pequeña empresa, como una carnicería, no necesita los mismos sistemas que un banco, por tanto, la inversión a realizar es mucho menor.

Una empresa con 10 ordenadores puede estar perfectamente protegida pagando unos 1.200 € al año.

PISHING, RANSOMWARE Y CORREO ELECTRÓNICO

Estas tres palabras son, en este momento, las tres principales amenazas para cualquier PYME.

El término ***phising*** corresponde a un ataque de suplantación de identidad. En ellos el atacante engaña al usuario para que acceda a su página web, su aplicación o su sistema haciéndole creer que realmente está accediendo a un sistema legítimo. El usuario introduce sus datos en el sistema falso facilitándoselos al delincuente. El ejemplo clásico de este tipo de ataques empieza con un correo electrónico donde nuestro banco nos indica que, por motivos de seguridad, debemos volver a darle algunos de nuestros datos. En el correo se adjunta el link que nos lleva a una página que, en apariencia, es igual que la del banco donde introducimos los datos requeridos (normalmente datos de acceso a la cuenta y tarjeta de crédito). En la realidad es una página falsa, igual que la del banco, pero controlada por un ciberdelincuente que se hace, en el momento, con los datos del incauto usuario.

Un ***ransomware*** es un virus que bloquea el equipo y cifra los archivos del mismo pidiendo un "rescate" económico para poder recuperarlos. Es uno de los virus más peligrosos que podemos encontrar.

El 60% de los virus tipo ***ransomware*** se instalan en el ordenador afectado a través de ficheros adjuntos en el correo electrónico.

Como puede verse, el correo es una fuente interminable de problemas si no se usa con las debidas precauciones (*Consultar el segundo apartado de este documento*). Aunque menos frecuentes, las infecciones también se producen en páginas fraudulentas, las cuales tienen un enlace que, al clicar, descarga y ejecuta el programa (siempre le pregunta al usuario antes si desea instalar de modo que con unas mínimas precauciones se puede evitar).

La mayoría de las veces las infecciones vienen por una mala acción de un usuario que inconscientemente pica en una trampa de ingeniería social o similar. Por eso tenemos que tener a nuestro personal formado bajo unas pautas muy sencillas (debes de ser igual de pesado que nosotros en este punto).

Por último, aquí tienes una lista con otros peligros que también acechan:

· ***Malware:*** Desde el principio de la informática hemos denominado a los archivos infecciosos como "virus". Actualmente, la definición ha cambiado a "*Malware*" ya que agrupa a todo tipo de programa o código malicioso diseñado para infectar un equipo y ejecutar acciones dañinas o fraudulentas.

· ***Troyano (o "caballo de troya"):*** Como en la mitología griega, este malware está incluido dentro de algún *software*, como aplicación o juego gratuito, y se oculta en nuestro permitiendo el acceso remoto de un usuario no autorizado al sistema.

· ***Spyware (o programa espía):*** Son minúsculas aplicaciones que recopilan la información de tu sistema para enviarla a través de Internet, como contraseñas, *logings*, nombres de usuario o direcciones de email.

· ***Phising:*** Son los métodos fraudulentos utilizados para conseguir, mediante correo electrónico o webs fraudulentas, y suplantando la identidad de grandes entidades la información de cuentas bancarias y credenciales.

· ***Cryptojacking:*** Es el malware de moda (a mediados de 2018). Son virus que utilizan recursos de nuestro sistema informático (Procesador y Memoria) para minar criptomonedas a nombre de otro. Si la infección llega a miles de ordenadores la capacidad de minado de criptomoneda puede llegar a ser muy alta generando grandes beneficios a los autores del ataque (además en moneda no rastreable por lo que el incentivo para generar este tipo de ataques es muy elevado).

EL ESLABÓN MÁS DÉBIL DE LA CADENA

Aquel slogan publicitario que decía *"La potencia sin control, no sirve de nada"* podría aplicarse a la situación de muchas pequeñas empresas: ordenadores de última generación, IPADS, la mejor conexión a Internet, el router con más luces del mercado... y al final todo se viene abajo porque un usuario, con su antivirus desactualizado, abre un correo con virus.

El sentido común, y la experiencia del usuario, es primordial para no caer en trampas de ciberdelincuentes. De hecho, se considera que la gran mayoría de ataques se inician gracias a la ingeniería social: un correo recibido "que parece de verdad", alguien que nos llama "diciendo que es del banco", una web "que parece buena" donde nos piden nuestros datos. Trampas en las que es fácil caer y en las que cualquier delincuente podría obtener los datos de tus clientes, el acceso a tu banco o cifrar tus ficheros para pedir una recompensa en bitcoins.

Por ello el eslabón más débil de la cadena son las personas. Nuestros empleados y los usuarios de nuestros sistemas. Para fortalecernos, la primera regla de la seguridad es formarles de forma continua y periódica. Hay que ser pesado y, constantemente, recordarles las reglas y peligros de la seguridad. Si eliminásemos el factor humano, los problemas de seguridad se reducirían por debajo de la mitad y, en una PYME, en más de 90%.

Seguro que todo le mundo en tu empresa sabe poner o quitar la alarma, sabe cómo abrir y cerrar las instalaciones, sabe cómo bloquear la caja o dónde están las medidas de seguridad de la oficina. Entonces, ¿cómo es posible que no sepan cómo comportarse con su correo electrónico o en Internet?

No importa cuan jóvenes o mayores sean o cuanto sepan de informática. A todo el mundo con acceso a un ordenador, teléfono o equipo conectado a Internet en una organización debe ser informado de algunas reglas básicas. Y estas hay que repetirlas hasta la saciedad. Una y otra vez.

Insistimos. En una PYME si conseguimos que la gente sepa lo que hace y se comporte con sentido común habremos conseguido el 90% de nuestros objetivos en materia de ciberseguridad.

A continuación, te damos las reglas básicas que debes transmitir a todas las personas de tu organización. Da igual cuanto sepan de informática, el puesto que ocupen o la labor que realicen.

La seguridad es cosa de todos y todos deben cumplir el siguiente decálogo:

UNO.

Piensa antes de abrir un correo electrónico de alguien que no conozcas. Pregúntate siempre: ¿Porqué me escribe esta persona? ¿Tiene sentido que me escriba a mí o al buzón que estoy leyendo? ¿Hay posibilidades de que sea un correo fraudulento? Y recuerda: ningún príncipe congoleño (ni su primo, el Director del Banco Nacional de Birmania) tiene ningún interés en ti (salvo pedirte dinero en uno de los timos más antiguos del sector).

DOS.

Nunca, bajo ningún concepto, abras o descargues un archivo adjunto en un correo de alguien que no conozcas, ni siquiera en vista previa. Nuevamente pregúntate ¿porqué me envían a mí este fichero adjunto?, ¿lo quiero para algo?, ¿necesito abrirlo (y no, en este caso la curiosidad NO es una necesidad)?

TRES.

Aunque conozcas al emisor, ten cuidado. Míralo bien antes de descargar nada. Por ejemplo, si el asunto o el cuerpo está mal redactado, con faltas de ortografía, en un idioma distinto e incluso si el contenido tiene algún sentido. Alguien puede estar haciéndose pasar por él (es algo mucho más común y sencillo de lo que parece).

CUATRO.

Ten cuidado al abrir archivos adjuntos comprimidos (da igual quién los envíe: ¡CUIDADO!), y más cuando el archivo no debería estar comprimido (como un Word o una simple imagen). Cualquiera con acceso a un correo electrónico debe saber distinguir un fichero por su tipología o saber qué es un fichero comprimido. Si alguien no tiene esos conocimientos entonces no es apto para el uso del correo o el acceso a Internet (¿dejarías a una persona sin cualificación manejar maquinaria pesada? ¿no? ¿entonces...?).

CINCO.

Si el archivo tiene una extensión diferente a la que debe de tener, bórralo inmediatamente. Una imagen no puede ser un fichero .exe. Si no sabes qué es un fichero .exe... ¡deja de utilizar el correo hasta que no sepas qué es una extensión de archivo, cómo se mira y cuáles son las más comunes!.

SEIS.

No introduzcas, bajo ningún concepto, tus datos personales, usuarios o contraseñas, a través de páginas que te llegan en un correo electrónico o en webs no seguras. Piensa, por ejemplo, que el banco nunca te dirá que accedas a tu cuenta a través de un email y si así fuera, cambia de compañía. ¡No deben ser dignos de tu confianza!

SIETE.

Hay muchas webs que intentan descargar un plugin (programa incrustado en la web) o similar cuando accedemos. Debemos tener mucho cuidado y, siempre que entres, ten por costumbre rechazar cualquier cosa que intente instalarse en tu ordenador. Salvo que expresamente sepas lo que es y lo necesites, nunca aceptes descargar e instalar nada. No le digas a todo que SÍ y, ¡por dios! Lee los mensajes antes de darle a "Aceptar".

OCHO.

Si no entiendes algún mensaje o no sabes a qué se refiere lo mejor es parar y buscar a alguien que te ayude. Lo más probable es que si llegas a esa situación estés a punto de generar un problema, así que, ante la duda, esperar un poco siempre va a ser más barato. Si alguien no entiende por qué lo has hecho.... Dale nuestro número de teléfono y que nos llame, si se atreve.

NUEVE.

Asegúrate que tienes un antivirus instalado, actualizado y funcionando. Puede que no sea cosa tuya instalarlo o actualizarlo, pero sí lo es comprobar que lo está. Cuando todo el contenido de tu ordenador se haya perdido, y a lo mejor tu empresa haya tenido que cerrar, será un poco tarde para decirte que revisar el antivirus era cosa del informático.

DIEZ.

Hacer copias de seguridad es vital. Asegúrate que tus datos son respaldados con cierta frecuencia y comprueba, al menos cada 6 meses, que esta copia se hace correctamente.

Nuevamente puede que no sea tu responsabilidad hacer la copia, pero sí lo es asegurarte que se hacen y, sobre todo, que la información copiada es correcta (puede restaurarse). Pide de vez en cuando algún fichero o simula una pérdida de datos, pero asegúrate que tus datos se copian. Nuevamente tu puesto de trabajo, y el futuro de tu compañía, pueden depender de ello.

ONCE.

Errar es de humanos así que, si crees que has cometido uno de los errores anteriores, no lo ocultes: apaga tu ordenador inmediatamente y contacta con el responsable de informática de tu empresa. La mayoría de los problemas tienen efectos muy limitados en los primeros minutos.

Recuerda que, si el problema se extiende, hay cientos de formas de detectar el origen, así que, si pretendes no decir nada porque crees que nadie va a enterarse, es muy posible que todo el mundo se entere cuando el problema sea mucho más serio.

NEO pone a tu disposición, un archivo en PDF para que puedas imprimirlo y entregarlo a todos los empleados de tu empresa. Anticiparse es lo os convertirá en una empresa segura.

No nos cansamos de decirlo. La formación a los empleados en esencial. Y, como consejo, te recomendamos que:

· Recuerdes estas reglas cada cierto tiempo. No está de menos hacer un refresco una vez al año (no importa lo que sepan los usuarios de informática, o el puesto que ocupen en la organización... estas reglas son absolutamente transversales y afectan a todos).

· Puedes poner trampas controladas para ver qué grado de seguridad tienen tus empleados: haz simulacros para recuperar copias de seguridad, utiliza herramientas para simular ataques por correo electrónico, etc.

· Las amenazas también se actualizan así que debemos estar atentos a las novedades.

SEGURIDAD PERMIETRAL: RED

Cuando hablamos de seguridad perimetral nos referimos a la forma de proteger nuestra red interna de la externa. Es decir, proteger la red donde están conectados nuestros ordenadores, de lo que queda al otro lado del router: Internet.

El objetivo es restringir y controlar el tráfico de datos que entran a nuestra organización y/o sale de ella.

El 99% de las empresas tienen una red interna, que suele usarse para la transferencia de archivos a un servidor, para conectarse con otros ordenadores, o para conectarse con una impresora o escáner. Para una red de este tipo, sólo necesitamos un switch, un aparato similar a un router pero sin conexión a internet y un antivirus.

¿Por qué necesitamos un antivirus si la red es interna y no está conectada a Internet?

Muy sencillo: los pendrives pueden contener algún archivo autoejecutable que funciona igual que los que descargamos de Internet y pueden fastidiarnos todos los ordenadores de la empresa.

Además de la red interna, si queremos conectar nuestros equipos también a Internet, necesitamos:

· **Un router** que conecte la red interna con Internet (normalmente los routers facilitados por las operadoras de telefonía cumple la doble funcione de "switch"y router).

· **Aislar tu red de Internet.** Cierra todos los puertos del router para evitar que un alguien se nos cuele. Dejar un puerto abierto es el equivalente digital a dejar la puerta abierta. Si tiene que estar abierta alguien tiene que vigilarla. En esta web, puedes ver el estado de todos los puertos de tu red:
www.internautas.org

· **Conecta** todos tus ordenadores por cable.

· **Debes tener una red wifi** para la red interna, sólo para temas relacionados con la empresa, y otra para invitados, donde se conecten los móviles o portátiles de las visitas.

· **Siempre hay que cambiar las contraseñas** de los routers wifi. Cuánto más compleja, mejor. El protocolo de seguridad debe ser WPA2-PSK. Recuerda que las contraseñas originales, que llegan desde la operadora, son obtenidas por medios automáticos conocidos y públicos. Cualquier puede obtener el password original de tu router en pocos minutos de búsqueda.

· **Si por algún motivo necesitas acceder a tu red interna desde fuera** de la oficina (desde casa por ejemplo), debes hacerlo configurando una VPN. Ni se te ocurra abrir directamente un puerto de escritorio remoto y acceder por ahí.

· **Si necesitas abrir un puerto,** asegúrate que tenga un cortafuegos que impida la entrada de personal no autorizado.

Crear una red básica y completa, como la que acabamos de explicar y con firewall incluido, puede costarte entre 700 y 900 euros. Además, deberíamos recordar que la red requiere de un mantenimiento básico y periódico para comprobar que todo funciona como deba (con dedicarle 1 o 2 horas mensuales es suficiente).

Si queremos un grado de seguridad adicional podemos añadir un gestor ***UTM*** (Gestión Unificada de Amenazas): un aparato que se conecta a la red, entre el router y el swicht. Su función es controlar el tráfico entrante y saliente, filtrar correos basura y bloquear webs con alto riesgo de infección o aquellas que no queremos que los empleados visiten en horas de trabajo (bien sea por su contenido o por ser susceptibles de contener malware), etc. Además, tiene la capacidad de analizar todos los archivos que entran a la red en busca de virus.

El precio de un UTM convencional puede rondar los 1200 €, con licencia del software durante un año. Si quieres mantener tu red a salvo, esta solución es la mejor elección (aunque su coste ya puede resultar excesivo para las organizaciones más pequeñas).

ANTIVIRUS

Disponemos de gran variedad de antivirus para proteger nuestros ordenadores. La protección es necesaria dadas las amenazas que existen en la red por lo que, aunque sean en versiones libres, es necesario tenerlas instaladas. Podríamos separarlos en 3 grupos:

· **Gratuitos:** Programas antivirus con ciertas limitaciones frente a sus hermanos de pago.

· **De pago:** Programa de instalación local. Suelen ser versiones avanzadas de las gratuitas.

· **Cloud:** Plataformas web desde las que administramos todos los antivirus. Nos avisa de cualquier evento desde que uno de nuestros ordenadores corporativos ha perdido una actualización a casos de infección. Son un complemento de las anteriores.

¿Cómo elegimos el mejor antivirus para nuestra empresa?

Evidentemente, y como casi todo, depende del presupuesto, pero desde NEO te aconsejamos que no escatimes e inviertas en lo que realmente necesites. Debemos saber que un antivirus gratuito cumplirá su función, pero de forma limitada. Si no queremos asumir el riesgo las opciones de pago de calidad rondan los 30 euros por licencia anual (para cada ordenador). Se comprar directamente “on-line”, se instalan en pocos segundos y las actualizaciones son automáticas.

Un antivirus actual, del que estemos pagando una licencia anual, no requiere mantenimiento, por lo que no tendremos que perder tiempos en actualizarlo en cada uno de los equipos de la empresa. El sólo se actualizará. Ahora bien es importante:

· **Auditar** una vez al año que los equipos de la empresa tienen los antivirus instalados y funcionando.

· **Asegura**r que los usuarios comprueben con frecuencia que su antivirus está actualizado o no le está dando mensajes relacionados con vulnerabilidades.

· **Realizar un escaneo** completo de los equipos cada tres meses.

COPIAS DE SEGURIDAD

Como definición una copia de seguridad es un respaldo de datos originales que se realiza con el objetivo de preservarlos y recuperarlos en caso de pérdida.

Tenemos muchas opciones para realizar una copia de seguridad. La forma más sencilla es utilizar la herramienta que viene por defecto en nuestro sistema operativo, pero te daremos unos consejos para que utilices los mejores programas BackUps del mercado sin invertir mucho dinero.

Las copias de seguridad se pueden realizar de 2 maneras:

· **Completas:** Cuando se realizan desde cero. Suelen ser las primeras que se hacen, ya que tardan bastante tiempo en realizarse.

· **Incrementales:** Añaden, a una copia existente, los últimos archivos que has creado o modificado. Se puede hacer a diario o semanalmente, no te llevará mucho tiempo y te asegurarás de que tienes todos tus archivos actualizados.

Una buena política sería realizar una copia completa cada mes, o semana, y copias incrementales todos los días. Además, mantener al menos dos copias en fuentes distintas: por ejemplo, si uso un disco duro externo usaré uno una semana y otro otra, para evitar que, en caso de rotura de cualquiera de ellos, siempre tengamos uno de repuesto.

En cuanto al soporte para las copias de seguridad: un USB, un disco duro externo, un ordenador o un soporte especializado (cintas) han sido los más actualizados en el pasado. En la actualidad, gracias a las velocidades de conexión, lo más habitual es utilizar un almacenamiento en la nube (que es lo que te recomendamos).

Si realizamos una copia de seguridad en un soporte físico tendremos que tener en cuenta algunos aspectos como: realizar copias en más de un disco, guardarlos a buen recaudo y fuera de la empresa (desconectado de la red). Además, los soportes externos hay que verificarlos periódicamente y renovarlos ya que con el tiempo pueden estropearse.

Elijas el sistema de almacenamiento que elijas, necesitarás un software adicional para gestionar cada cuánto tiempo se debe hacer la copia, de qué archivos y si es completa o incremental. Para ello, aquí hay 3 programas que te ayudarán a ello:

· **Cobian BackUp:** Permite realizar copias desde el propio ordenador, a través de una red local o FTP y restaurarla cuando lo necesites. Permite, además, el cifrado y compresión de las copias para mayor seguridad. Este software es gratuito, y lo debes descargar sólo y únicamente de su web.

· **Acronis:** Recomendable para las copias de seguridad completas. Con su propio software de gestión, podrás restaurar las copias en caso de fallo grave sin mucho inconveniente. Además, te protegerá de ransomware, el temido virus que encripta todos los datos de servidores y ordenadores. Su precio varía en función de las necesidades, pero desde 49,99 € al año, tendrás tu empresa protegida.

· **Norton Ghost:** Permite realizar copias completas o selectivas. Además, puedes programarlas para que se realicen en un momento en concreto o cada cierta frecuencia. Es de los más flexibles y configurables del mercado y su precio ronda unos 30 € al año por licencia.

Una vez que se están haciendo las copias de seguridad en un soporte físico, hay 3 elementos clave para tener en cuenta.

El medio (USB, Disco Externo o Servidor) en el que se realicen las copias de seguridad debe estar desconectado de Internet.

Si dejas un disco duro USB conectado a un servidor y programas ahí las copias de seguridad diarias es lo mismo que no tener copias. Si haces esto y tienes una infección, por ejemplo un Ransomware, lo que pasará es que se infectará el equipo y el disco donde se hacen las copias.

Si usas un disco externo o una unidad USB asegúrate de usar al menos dos unidades e ir alternándolas, teniendo dos copias completas y diferenciales duplicadas. Una buena idea es usar una semana una y otro otra. Si usas un servidor externo este debe estar fuera de la red y conectarse sólo para hacer la copia.

Volvemos a repetir nuestra recomendación: Usar un almacenamiento cloud de Azure o Amazon donde 1 TB podría costarnos en torno a 100 € Mensuales. La mayoría de los sistemas de copia de seguridad son compatibles con ellos y, además, el proveedor cloud nos ofrece su seguridad añadida: hace copias de las copias, limita su acceso, etc.

En todo caso si optamos por un disco externo USB, lo más barato, o un servidor debemos preguntarnos siempre por la seguridad de la copia: ¿Qué pasa si se pierde? ¿Qué pasa si se rompe? ¿Qué pasa si se infecta? Por eso en estos casos es recomendable tener dos fuentes y dos copias e ir alternándolas. Por ejemplo: una semana una, otra semana otra, un mes uno un mes otro, incluso un día una un día otra. Todo depende de la cantidad de información que generemos y el problema que nos pueda suponer la pérdida de un día o dos de trabajo.

La Ubicación. Una vez hecha la copia ésta debe estar físicamente fuera de la oficina. Preguntémonos ¿Qué pasaría si hay un robo, un incendio o un desastre similar? No podemos permitirnos que se pierdan al mismo tiempo el original y la copia. Por ello es importante tener la copia de seguridad fuera de la oficina.

Si utilizamos una unidad USB o Disco Duro externo tendremos que moverlo manualmente. En este caso también es importante que la información de la copia de seguridad esté cifrada. No serías el primero que la olvida en algún lugar por lo que es importante que los datos no sean accesibles.

Si utilizas un servidor externo asegúrate que éste se desconecta de tu oficina una vez realzada la copia y no es accesible automáticamente desde la misma (salvo que lo necesites).

Comprobar. Debemos estar seguros de que las copias de seguridad funcionarán en caso de necesitarlas. A veces, nos acostumbramos y automatizamos el trabajo sin comprobar realmente si se está haciendo bien, y cuando lo necesitamos nos damos cuenta de que hay archivos que no se han incluido y los hemos perdido.

La última regla de las copias se basa en comprobar su integridad. De forma periódica la información copiada debe ser restaurada, analizada y asegurar que:

· Está todo lo que queremos copiar. Prestar especial atención, por ejemplo, a carpetas de ficheros de datos de programas de gestión.

· Toda la información se está copiando bien. No hay ficheros corruptos o similares.

· Si se copian bases de datos, por ejemplo, de ERPs, hay que asegurarse de que se están realizando correctamente y pueden restaurarse sin problemas.

Lo más recomendable es restaurar los datos una vez al mes y hacer chequeos aleatorios. Eso sí, una vez al año hay que hacer un simulacro de desastre y verificar que tengo todo lo que necesito para recuperarme de un desastre.

No bajes la guardia y recuerda estas tres grandes claves:

· Prepárate para perder la información de tu oficina.

· Prepárate para que ese mismo día pierdas la información de una de tus copias de seguridad.

· Asegúrate que lo que te quede, aunque tenga dos o tres días de antigüedad, es rescatable al 100x100.

Si haces esto, nunca perderás la información.

CÓMO ACTUAR EN CASO DE DESASTRE

Si nos percatamos de que alguno de nuestros ordenadores tiene problemas de seguridad o ha sido infectado con un malware o virus, lo primero y más importante es **desconectarlo de la red y apagarlo.**

Una vez desconectado y apagado ya podemos proceder a comunicar con el responsable de informática para que nos dé instrucciones. Reiniciar el ordenador, ignorar el problema o dejar que cunda el pánico no van a resolver la situación. Desconectar de la red y apagarlo tampoco, pero evitará que empeore. Y, créenos, empeoraría.

No debemos hacer distinción del equipo o su dueño. Da igual que sea el portátil del gerente, el ordenador del director general , el servidor de la compañía o el que maneja el sistema de la caja. La desconexión y el apagado no es opcional aunque eso suponga paralizar la actividad. Si no lo haces, corres el riesgo de infectar todos los equipos de la red y la paralización costará mucho más.

Una vez realizada la desconexión y apagado debemos tener en cuenta las siguientes reglas:

1. Poner la copia de seguridad en cuarentena, desenchufándola de la red y haciendo una copia de seguridad offline en un ordenador fuera de la red que no tenga problemas. Después, escanéala para asegurarte que está libre de virus.

2. No utilices un equipo infectado para recibir instrucciones del servicio de soporte informático, incluso en caso de necesidad extrema. Utiliza otro, y si está conectado a otra red, mejor.

3. No formatees hasta que la crisis haya pasado (o tengas claro que has podido restaurar toda la información de una copia de seguridad). Da igual que la infección esté en el servidor y sea un equipo caro de reemplazar. Aunque es una solución válida, piensa que perderás todas las oportunidades de recuperar tus datos, así que el formateo se debe realizar una vez terminada la crisis.

4. No borres programas o archivos. Podría desencadenar acciones no controladas que nos harían perder más información.

5. Si has iniciado el escaneo del antivirus, no realices acciones de borrar o desinfectar.

6. Si te ha infectado un Ransomware, te recomendamos firmemente no pagar. Lo más probable es que nadie te responda, y si lo hacen, lo más probable es que te hagan pagar y no te den ningún remedio. Si pagas, además, te pondrán en la lista negra: saben que eres un blanco fácil y débil y volverán a intentar infectarte.

Nadie en NEO conoce ningún caso, ni siquiera de oídas, en el que tras pagar se haya resuelto el problema.

Estas reglas son básicas y esenciales, y en el caso de infección, las debería realizar un responsable informático. Si el vuestro intenta saltarse alguna de ellas, o incumplirlas de algún modo, te recomendamos que lo cambies en el momento y busques a otro (muchas de estas acciones no tienen vuelta atrás de modo que no esperes a impedírselo).

AUDITORÍA

Es fundamental auditar la seguridad cada cierto tiempo. De nada sirve todo lo anterior si no hay alguien encargado de que se cumplan los procesos. Algunas empresas que invierten en hacer copias y escaneos de seguridad dejan de realizarlas tras un periodo en el que no han tenido ningún ataque. Es ese momento cuando somos más vulnerables y una infección puede convertirse en un auténtico desastre: más tiempo sin realizar copias, más archivos creados, mayor pérdida.

Hay que ser constante. Debemos tener a una persona encargada de la seguridad y que, con un calendario anual, marque las fechas para realizar las auditorías.

Una auditoría no es más que la comprobación de que las cosas funcionan correctamente y se cumplen los procedimientos: en copia de seguridad, en actualización de antivirus, en uso del correo, en configuración de la red, etc. No necesitamos contratar a una empresa externa que nos la haga, ni gastarnos grandes cantidades de dinero.

Con estos sencillos pasos, bastará para que las puedas realizar tú mismo:

· Restaura, eventualmente, las copias de seguridad y asegúrate de que están en buen estado. Desde el primer al último archivo que guardaste.

· Pon a prueba el uso del correo entre los empleados. Utiliza herramientas como Phish Threat, que hace un envío simulado de correos fraudulentos, para asegurarte de quién lo ha abierto o descargado.

· Revisa los antivirus instalados en los ordenadores de los que han fallado la prueba de correo y verifica que están actualizados.

Y, no nos cansaremos de decirlo, refréscales la formación a TODOS LOS EMPLEADOS. Tu seguridad será tan débil como el menos formado de tus empleados. Si eres vulnerable a un ataque de ingeniería social, serás infectado y dará igual el antivirus, las copias o la red... eres vulnerable.

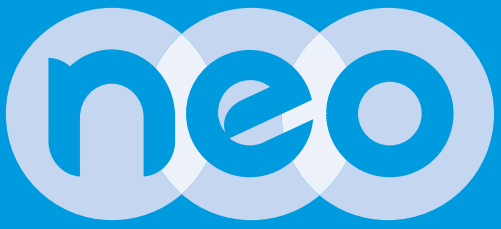
Tómanos a nosotros como ejemplo: somos una compañía especialidad en software donde el 90% de nuestra plantilla son profesionales del sector tecnológico: desarrolladores, técnicos, analísticas. Hace unas semanas realizamos una prueba de Phising, como la que te hemos recomendado, y ¿sabes cuál fue el resultado? Un 10% de nuestros empleados, picó en la trampa. ¿Porqué? Porque nos confiamos: pensamos que, al saber mucho de software, estábamos por encima del riesgo. ¡Error! Da igual quién sea, qué puesto tengas y lo que sepas: siempre estas expuesto y es importante que te lo recuerden cada poco tiempo.

Recuerda que la única manera de gestionar bien la seguridad de tu empresa es formando a tus empleados. Ningún antivirus nos protege de la falta de sentido común.

Como te decíamos, nos preocupamos tanto por nuestros clientes como por los que no lo son, por eso, te ofrecemos estos consejos para que los compartas con tus contactos. Si en alguna ocasión tienes una infección y necesitas ayuda, contacta con nosotros. No nos dedicamos a la seguridad, ni somos los que más sabemos del tema pero estaremos encantados de asesorarte y recomendarte a dónde dirigirte para recibir ayuda.

El equipo de NEO.

managing mobility



www.neo-si.com
T. 91 575 18 06

Operaciones
Pollensa 4, Edificio Atenea 4
28290, Las Rozas de Madrid · Madrid

Central
Pollensa 2, Edificio Artemisa 17
28290, Las Rozas de Madrid · Madrid

Factoría de Software
P. Científico de Murcia
30100 · Murcia