Decálogo de ciberseguridad para empresas.

Grupo Galilea

CIBER RIESGOS

Contenido

Introducción

El buen funcionamiento, e incluso la supervivencia, de las empresas depende en gran medida de su **adaptación al medio**. Hoy en día en las empresas, inmersas en un entorno tecnológico en constante cambio, la ciberseguridad se convierte en una prioridad.

Para abordar la seguridad resulta útil tener una visión integral del entorno, interno y externo, que tenga en cuenta no solo **aspectos técnicos** si no también físicos, organizativos y legales**.** Con esta perspectiva panorámica será más fácil adaptarse al medio identificando **los riesgos** a los que se expone la empresa y localizando los **puntos débiles**.

Hoy en día los sistemas de información con base tecnológica están presentes de alguna forma **en todos los procesos de cualquier empresa**: comunicación interna, relación con los proveedores, logística, producción, marketing, atención al cliente, selección y formación de personal, internacionalización, innovación, etc. Las pymes no están al margen de este entorno tecnológico. Las que no han nacido digitales se ven obligadas a evolucionar, por sus clientes o por la competencia, arrolladas por la necesidad de supervivencia.

Es cada vez más frecuente el uso de dispositivos móviles y servicios en la nube para el desarrollo de nuestra actividad. Estos avances tecnológicos nos ofrecen la oportunidad, no exenta de riesgos, de nuevos modelos de negocio, nuevas formas de interacción con los clientes y nuevas formas de trabajo para los empleados. Por otra parte, llegamos a nuestros clientes por diferentes medios: correo electrónico, página web, redes sociales, aplicaciones móviles, etc.

En este entorno tecnológico la ciberseguridad es un factor diferenciador para la empresa al **generar confianza** en clientes, proveedores.

Decálogo para la pyme cibersegura

La pyme preocupada por su ciberseguridad tiene que seguir este camino. Los que aquí proponemos los diez pasos que consideramos esenciales.

En primer lugar, la pyme tiene que analizar su estado de seguridad y definir a dónde quiere llegar. Esto se plasmará en una serie de **políticas y normativas** que van a dirigir la forma de abordar la seguridad en el día a día.

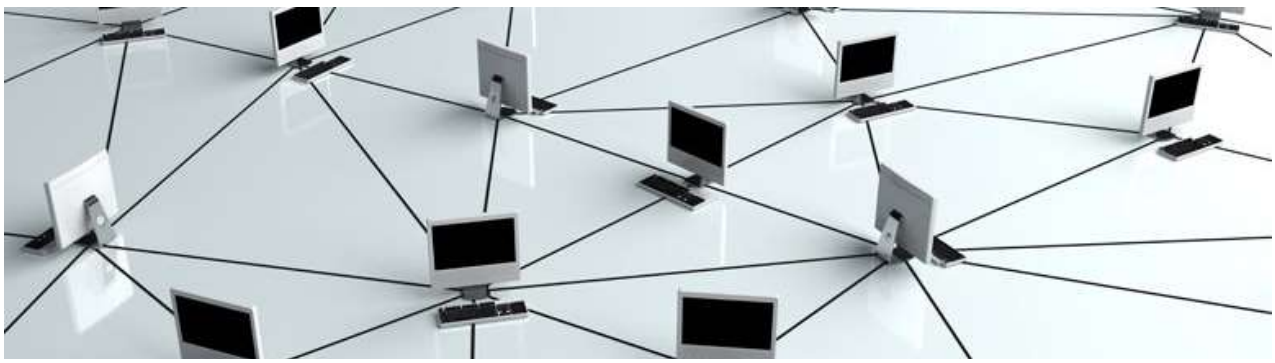
Como resultado de lo anterior, pondrán en marcha, si aún no lo han hecho, o mejorarán su sistema de **control de accesos lógicos**, pues al igual que controlamos quién entra en nuestras instalaciones, debemos controlar quién entra en nuestros sistemas.

Cualquier reflexión que se haga sobre seguridad llevará a la conclusión de las **copias de seguridad** son la forma de recuperarse de casi cualquier incidente. No deben faltar en cualquier pyme que quiera sobrevivir a un incidente.

Básico y esencial es también la **protección antimalware** pues los virus mutan para hacerse cada vez más dañinos y peligrosos. Ninguna pyme está exenta de este riesgo.

Y no habrá protección eficaz si utilizamos sistemas o aplicaciones obsoletas y desactualizadas pues son más vulnerables. Por ello **actualizar todo el software** es fundamental.

Nuestra **red** ha de estar protegida para evitar todo tipo de intrusiones en nuestros sistemas. Y como el **acceso desde el exterior** de clientes y colaboradores se hace imprescindible en un medio comercial electrónico no descuidaremos la seguridad de la información cuando es comunicada hacia y desde el exterior.



No menos importante es proteger la información almacenada en todo momento pues los soportes pueden extraviarse o deteriorarse. **Controlar los soportes** de la información durante toda su vida útil es también una medida de seguridad elemental. Vigilar nunca está de más y para ello pondremos los medios para llevar un **registro de actividad** dónde podamos observar cómo interaccionan los usuarios con los sistemas y detectar anomalías en su comportamiento.

Por último, pero no menos importante es dar los pasos necesarios para garantizar la **Continuidad de negocio** pues es todos, incluso las pymes, podemos sufrir un incidente de seguridad.

Política y normativa

El compromiso con la seguridad se demuestra definiendo, documentando y difundiendo una **política de seguridad** que defina cómo se va a abordar la seguridad. También se concreta con el desarrollo de **normativas y procedimientos** que recojan las obligaciones a las que están sujetos los usuarios en lo que respecta al tratamiento y seguridad de la información.

Cada empresa es diferente y con características únicas: número de empleados, dependencia tecnológica, área de actividad, internacionalización, etc. Por este motivo, para concretar.

la política en hechos lo haremos mediante un **Plan director de ciberseguridad**. Para ello tendremos que:

- Determinar el punto de partida de la empresa en materia de ciberseguridad, identificando los procesos críticos de nuestra organización, los empleados, equipos o activos esenciales para el funcionamiento de nuestra empresa.
- Determinar el nivel de seguridad que querríamos conseguir en función de las características de la empresa, el sector de negocio al que pertenecemos, los objetivos estratégicos o los requisitos que define el mercado, etc.

En este proceso, habremos detectado los **riesgos** que afectan o pueden afectar a corto o medio plazo a nuestro negocio. Conociendo los riesgos, podemos realizar **planes de acción personalizados,** adecuados a nuestra singularidad**,** con las medidas de seguridad a aplicar.

La ciberseguridad es un proceso y como tal los planes para abordarla deben revisarse periódicamente, ya que las amenazas cambian y evolucionan constantemente.

Como resultado de nuestro Plan director de Ciberseguridad, definiremos y priorizaremos los proyectos de ciberseguridad necesarios para nuestra empresa. Estos proyectos no sólo consistirán en la instalación de productos o la contratación de servicios de seguridad, también es necesario aplicar cambios en la forma de hacer las cosas. Por esto, del plan se derivan una serie de **normativas de uso interno** y unos procedimientos para verificar su cumplimiento.

Normativa interna

La normativa interna va a plasmar la forma en la que abordamos la ciberseguridad, es decir, nuestros compromisos. Estos deben empezar desde el momento de la contratación de los empleados y durante todo el tiempo que este permanezca en la empresa con sesiones periódicas de formación y concienciación.

Cuando se contrata un empleado y al resto de empleados, al menos una vez al año, debemos recordarles cómo han de proteger los recursos de la empresa, entre ellos la información, los sistemas y equipos informáticos, los móviles o portátiles de empresa, los pendrives, los servicios en la nube, la página web, las redes sociales, etc.

El empresario tiene que informar al empleado de los usos aceptables y no aceptables, por ejemplo, con estas **políticas, normativas y buenas prácticas**:

- Política de seguridad en el puesto de trabajo
- Normativa de uso de software legal o política de aplicaciones permitidas
- Política de uso de dispositivos personales (BYOD)
- Política de uso de portátiles
- Política de uso de wifis externas o de conexión desde el exterior
- Buenas prácticas de movilidad o teletrabajo
- Clasificación de la información corporativa
- Políticas de almacenamiento (local, red corporativa, dispositivos externos y en la nube) y copias de seguridad
- Política de gestión de soportes, borrado seguro y de destrucción de la información
- Política de uso del correo electrónico
- Política de contraseñas
- Política de actualizaciones
- Checklist para detectar fraude en pedidos online

Esta información estará a disposición de los empleados. Debemos revisarlas para que se adapten a nuestras necesidades y circunstancias, pues cambian con frecuencia. También debemos establecer un procedimiento para refrescársela a los empleados, cada vez que haya un cambio y al menos una vez a año, porque no podremos exigirle que las cumpla si no las conoce.
Es también habitual que se firmen con los empleados y colaboradores acuerdos de confidencialidad, a la vez que se firma el contrato laboral, de acuerdo con la sensibilidad de los datos que va a tratar.

Además de esta normativa, existirán una serie de procedimientos para que los técnicos o los encargados de la tecnología sepan cómo actuar para lleva a cabo:

- El control de accesos lógicos, es decir, qué medidas de seguridad se toman al dar de alta/baja a usuarios en los sistemas, en el correo electrónico, etc.
- El control y mantenimiento del software y del hardware instalado, desde su adquisición llevando un control de las licencias; durante su vida útil llevando a cabo las actualizaciones o los cambios necesarios; o destruyendo de forma segura los dispositivos y soportes obsoletos.
- Las copias de seguridad con detalles como dónde, cuándo y cómo han de realizarse.
- La gestión de incidentes o cómo actuar en caso de que ocurra alguno.

Cumplimiento legal

La ciberseguridad de nuestras empresas no se limita únicamente a la protección frente a amenazas que pongan en riesgo nuestros sistemas informáticos o la información confidencial que tratemos con ellos.

Hay otro tipo de seguridad que debemos tener en cuenta a la hora de proteger nuestras empresas, y es la **seguridad legal**. Debemos garantizar el cumplimiento de todas las normativas y leyes que afecten a nuestros sistemas de información. Más allá de no exponernos a posibles sanciones económicas, la pérdida de clientes o al daño a la reputación de nuestra imagen corporativa, la importancia de su cumplimiento radica en que nos servirá como medidas generadoras de confianza.

Con este tipo de seguridad, hacemos referencia a:

- **Las normativas legales que toda empresa debe cumplir**. Leyes aplicables a toda empresa que opera en territorio nacional y que están relacionadas con la gestión y protección de la información de sus usuarios y clientes, así como los sistemas informáticos que la tratan. Las principales leyes son:
    - **Ley Orgánica de Protección de Datos** (LOPD)]. Es una ley que afecta a la gran mayoría de empresas y vela por la seguridad de los datos y ficheros de datos de carácter personal que gestionan las empresas. Esta ley obliga a implantar diferentes medidas de seguridad según la sensibilidad de la información.
    - **Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico** (LSSI). Esta ley afecta a las empresas dedicadas a actividades lucrativas o económicas, que permitan la contratación online de servicios, ofrezcan información de productos a través de páginas web, o se dediquen al comercio electrónico. Esta ley requiere que incluyamos en nuestra página web, diferentes datos e información referente a la identificación de nuestro negocio y los servicios o productos que ofrecemos.
    - **Ley de Propiedad Intelectual** (LPI). Esta ley protege los proyectos, desarrollos u obras fruto de la actividad empresarial.

- **Seguridad con terceros**. Cuando contratamos servicios externos, tenemos que acordar con los proveedores los niveles del servicio (en inglés *Service Level Agreement* o **SLA**) que nos prestan, mediante contratos, firmados por escrito, donde se establezcan los niveles de calidad del servicio contratado, estableciendo penalizaciones en caso de incumplimiento. Se tendrán en cuenta aspectos como el tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc. De cara a la seguridad, en estos acuerdos de nivel de servicio se deben contemplar:
    - los activos cuya seguridad vigilará el proveedor y los que vigilaremos nosotros;
    - las tareas de seguridad (parcheado, actualización,) que realizará el proveedor y las que realizaremos nosotros;
    - una clasificación de incidentes con sus objetivos de tiempos de respuesta o recuperación;
    - las obligaciones contractuales, por ejemplo, compensaciones financieras por pérdidas, etc.

- **Seguridad interna con los empleados.** También en nuestra relación con empleados y colaboradores tenemos que garantizar la confidencialidad de la información de nuestros proyectos y los datos personales de nuestros clientes. De no hacerlo puede suponer un incumplimiento desde el punto de vista legal sujeto a sanciones económicas. Para ello, elaboraremos unos **acuerdos de confidencialidad** con los que regularemos los aspectos relativos a la prestación del servicio, incluyendo las sanciones en caso de incumplimiento. Los empleados aceptarán y firmarán por escrito estos acuerdos, que tendrán en cuenta aspectos como los siguientes:

    - ¿Quién interviene y a qué servicio va asociado el acuerdo de confidencialidad?
    - ¿Qué se considera información confidencial?
    - ¿A qué se comprometen las partes que intervienen en el acuerdo?
    - Auditoría y legislación aplicable

Control de acceso

Al igual que controlamos el acceso en el mundo físico para entrar en edificios o en sus dependencias con sistemas como tornos de entrada, tarjetas RFID, guardias de seguridad o videovigilancia, en el mundo digital controlar el acceso a los recursos de información de la empresa es la primera forma de protegerlos. Identificar quién puede acceder a dónde y para hacer qué es básico y esencial.

Hace no mucho tiempo, los sistemas informáticos de la empresa estaban encerrados en una sala y los accesos desde el exterior consistían en conexiones por cable desde el mismo edificio o desde alguna oficina remota. El control de accesos estaba «controlado».

Actualmente la tecnología permite que los servicios y aplicaciones salgan de la sala en la que estaban encerrados. Por ejemplo, contratamos a *partners* tecnológicos el alojamiento de nuestra página web o servicios de terceros (tiendas online, pasarelas de pago,), e incluso tenemos a nuestro alcance servicios en la nube. Nuestros usuarios y empleados pueden acceder a través de Internet o con sus dispositivos móviles a las aplicaciones de la empresa y las conexiones inalámbricas (wifi, por ejemplo) son muy habituales. Es decir, el control de accesos se ha vuelto complejo.

Además, hoy en día los dispositivos móviles superan a los ordenadores en conexiones a Internet. Lo que hasta hace unos años era impensable es cada vez más habitual: los empleados utilizan sus propios dispositivos y aplicaciones para su trabajo. Es lo que comúnmente se suele llamar: BYOD (*Bring Your Own Device*).

En resumen, por una parte, las empresas han adoptado la tecnología, en todas sus expresiones, para sus procesos y actividades. Nuestros sistemas son ahora una mezcla compleja y dispersa de servicios, equipos, aplicaciones y estándares. Por otra, el acceso ya no es sólo local e interno ya que gran parte de nuestros servicios se ofrecen a través de Internet o de forma remota tanto a nuestros empleados y colaboradores como a nuestros clientes y usuarios externos. El control de accesos se ha complicado… ¡y mucho!

El control de accesos está formado por los mecanismos para hacer cumplir los criterios que se establezcan para permitir, restringir, monitorizar y proteger el acceso a nuestros servicios, sistemas, redes e información. Para ello tenemos que identificar a los usuarios, quienes son y qué les vamos a permitir hacer.

En primer lugar, es necesario dar de alta en los sistemas a los usuarios y gestionar de forma automática todo el ciclo de vida de sus identidades.

Para identificar a los usuarios se utilizan:

- credenciales como el ID de usuario y la contraseña
- permisos, derechos y privilegios
- atributos, como el horario o el cargo para nuestros empleados
- información biométrica, etc.

Después se ha de comprobar que los usuarios que intentan acceder son realmente quienes dicen ser (autenticación). Para la autenticación se pueden utilizar distintos factores y en ocasiones más de uno a la vez: contraseñas, PIN, *OTP (One Time Password), passphrases, smartcards,* claves criptográficas o biometría en sus distintas formas.

De forma esquemática:

Identificación	Es el método mediante el cual decimos quienes somos, es decir, que nombre nos han puesto en el sistema y como nos reconoce. Así la entidad que accede mostrará su nombre de usuario, o una id de proceso si es una máquina, por ejemplo.
Autenticación	Es el método para comprobar que somos quienes decimos ser. Esto se realiza generalmente con algo que poseemos, somos o sabemos y que previamente (al darnos de alta) el sistema había asociado a nuestra identidad. Es la segunda parte de las credenciales de acceso. Son ejemplos: contraseñas, claves criptográficas, PIN, huellas dactilares, etc.

Autorización	Es el mecanismo para comprobar si el usuario autenticado tiene los derechos de acceso a los recursos que quiere acceder y los privilegios para hacer con ellos lo que solicita. Si es así, le autoriza, en caso contrario no.
Accountability	Es el mecanismo para registrar todos los eventos que tienen lugar en relación con los accesos, básicamente: quién quiere acceder, a qué, cúando, para qué y que resultado tiene ese evento (accede, no accede, el recurso no está disponible, etc.).

Para un buen control de accesos se ha de establecer una **política de acceso** que defina una gestión de usuarios y una segregación de funciones. De esta política se derivan los procedimientos para la gestión de contraseñas (cada cuanto se deben cambiar, su fortaleza) para la gestión de alta/baja de usuarios (cuando entra un nuevo empleado por ejemplo o cuando abandonan la empresa) y sus permisos (perfiles por departamento o por funciones, por ejemplo).

Para controlar el acceso en nuestra organización seguiremos el principio de mínimo conocimiento, conocido como *need-to-know*. Principio que al aplicarlo deberá de garantizar que cada persona de la organización accederá a lo que necesita saber, ni más ni menos.

A continuación, detallamos los puntos que deben recogerse como mínimo dentro del procedimiento o política de control de acceso:

- **Definir una clasificación e inventario de la información** que establezca los requisitos de control de acceso aplicables. La información clasificada como confidencial debe estar protegida mediante una política de contraseñas.
- Determinar los **grupos** de la empresa **que deben tener acceso** a cierto tipo de información. Por ejemplo, tan solo el personal de RRHH y del departamento financiero disponen de acceso autorizado a la información de nóminas.
- Establecer los **permisos** que un grupo posee sobre determinada información. Por ejemplo, el personal de RRHH solo posee permisos de lectura para la información referida a nóminas, mientras que el departamento financiero dispone de todos los permisos para el acceso a dicha información.
- Generar un procedimiento para **solicitar accesos extraordinarios** a la información. Es posible que una persona de administración, en ausencia o baja del personal financiero, deba acceder de manera extraordinaria a la información de nóminas para poder realizar los pagos.
- Establecer una periodicidad para realizar **revisiones** de los permisos asociados a cada uno de los grupos, con el fin de detectar desviaciones.
- Generar un procedimiento para **revocar la asignación** de una persona a determinados grupos.

Por último, hay que añadir que, para no cometer errores en las asignaciones de acceso a nuestra información es recomendable seguir el principio de mínimo privilegio, donde a cada grupo se le asignará lo mínimo necesario para poder desempeñar su trabajo diario de una manera correcta.

Es importante tener claro que no todas las personas necesitan tener acceso a toda la información de la empresa para poder realizar correctamente su trabajo. Establecer un control de acceso basado en la necesidad de conocimiento mínimo del personal «*need-to-know*» nos ayudará a proteger nuestra información y a evitar problemas de fugas o borrados no intencionados de información sensible de la empresa.

El control de acceso a la información en cualquier empresa es fundamental para prevenir situaciones como el espionaje por parte de la competencia, fugas de información por personal interno, borrado de información y otro tipo de acciones que ponen en riesgo nuestros procesos de negocio y que, en caso de producirse, tienen unas consecuencias económicas considerables.

Copias de seguridad

La información que tratamos en nuestros procesos productivos es el activo más importante de nuestras empresas y, como tal, debe protegerse adecuadamente. Esto es lo que conocemos como **seguridad de la Información.**

Debemos garantizar la **disponibilidad, integridad y confidencialidad** de la información de la empresa, tanto la que se encuentra en soporte digital, como la que se gestiona en papel.

Independientemente de la empresa o la actividad de esta, hay una serie de medidas básicas que debemos aplicar para la protección de la información:

- copias de seguridad
- cifrado de información
- control de acceso a la información
- destrucción de información

Las copias de seguridad son la salvaguarda básica para proteger la información. Dependiendo del tamaño y necesidades de la empresa, los soportes, la frecuencia y los procedimientos para realizar las copias de seguridad pueden ser distintos.

El soporte escogido dependerá del sistema de copia seleccionado, de la fiabilidad que sea necesaria y de la inversión que deseemos realizar. Estas tres variables van estrechamente unidas y deben estar en consonancia con la estrategia de nuestra organización.

En la implantación de un sistema de copias debemos tener en cuenta al menos las siguientes consideraciones:

- **Analizar la información** de la que se va a realizar la copia, así como los sistemas y repositorios donde se encuentra. Debemos tener en cuenta las configuraciones de dispositivos de red, los equipos de los usuarios o incluso información en *smartphones*. Este paso debe permitirnos descartar información sin relación directa con el negocio o ficheros históricos de los que ya existen copias.

- Debemos definir formalmente el **número de versiones** que vamos a almacenar de cada elemento guardado, y su periodo de conservación. Esto es lo que se conoce como política de copias de seguridad.

En esta decisión influyen las necesidades del negocio y la capacidad de almacenamiento disponible. En cualquier caso, dependerá de la complejidad de la organización y el volumen de los datos. Si el volumen de información es bajo, puede ser factible realizar una copia total diaria.

La principal diferencia entre la copia completa y los otros dos tipos de copia es la información que se almacena en cada iteración del proceso de copia de seguridad.

  - En la **copia total**, se realiza una copia completa y exacta de la información original, independientemente de las copias realizadas anteriormente.
  - En el caso de los sistemas de **copia incremental**, únicamente se copian los archivos que se hayan añadido o modificado desde la última copia realizada, sea total o incremental.
  - En el sistema de **copias diferenciales** cada vez que se realiza una copia de seguridad, se copian todos los archivos que hayan sido modificados desde la última copia completa.

- Hacer **pruebas de restauración periódicas**, para garantizar que no se producirán problemas en caso de necesitar recuperar la información. Esto es especialmente importante si no se solicitan restauraciones con frecuencia. Los sistemas de copia o los soportes pueden fallar y es fundamental detectarlo antes de que sean necesarios. El método para utilizar para la restauración depende de la copia que utilicemos para reponer los datos.
- Llevar un **control de los soportes de copia**, mediante un etiquetado y un registro de la ubicación de los soportes. Las copias de seguridad tienen que estar en un lugar protegido, por ejemplo, en una caja ignífuga bajo llave. Esto implica también llevar el control de la vida útil de los mismos.
- Si la información almacenada en las copias es confidencial, debemos valorar la posibilidad de cifrarlas, para evitar que, ante una pérdida o sustracción de un soporte, sea posible acceder a ésta. Esta medida debe abordarse con especial cuidado para evitar la pérdida de información en caso de pérdida de las claves. Puede ser preferible que el cifrado se realice en el origen sobre archivos específicos y no en la copia de seguridad, especialmente en caso de utilizar servicios de almacenamiento «en la nube», dado que el acceso a la información reside en un tercero.

- Debemos **disponer de una copia de seguridad fuera de la organización**, para evitar la pérdida de la información en caso de incendio, inundación, robo o ser víctima de un malware que rastree nuestra red buscando estas copias de seguridad. Es necesaria una selección adecuada de la localización de dichas copias. De manera alternativa y más segura, existen empresas de guarda y custodia que garantizan la seguridad de los soportes que les confiemos. Si utilizamos los servicios de otras empresas, el cifrado de la información puede servirnos para evitar el acceso no autorizado en caso de robo de la información.
- Por último, se debe **documentar el proceso de realización y restauración** de copias. Esto permitirá agilizar el proceso de recuperación ante una contingencia o ausencia del personal habitual.

En caso de que utilicemos el almacenamiento en la nube para las copias de seguridad, debemos considerar la posibilidad de que no podamos acceder a la información de manera temporal, por un fallo del servicio o de nuestra conexión a Internet. Adicionalmente, deben considerarse los costes implicados y leer las políticas de privacidad y seguridad del servicio, especialmente si vamos a almacenar información con datos de carácter personal.

Protección antimalware

Del mismo modo que ha evolucionado la tecnología que utilizamos para desarrollar el trabajo en la empresa, lo ha hecho la ciberdelincuencia y los peligros a los que nos exponemos. Los ataques e intrusiones no se limitan ya a «curiosos» o a personas que buscaban superar retos personales introduciéndose en sistemas «ajenos», sino que ahora tienen una motivación principalmente económica, con grupos y mafias altamente organizadas y especializadas de ciberdelincuentes, con medios tecnológicos muy avanzados, que buscan el provecho económico.

Los ciberdelincuentes atacan sistemas informáticos, extorsionan, realizan delitos de fraude y falsificación, etc. con el fin de obtener información valiosa de la que sacar partido económico. Aunque también tienen como objetivo tomar el control de otros sistemas para utilizarlos en ataques más sofisticados. Para conseguir sus objetivos, los atacantes suelen utilizar software especialmente diseñado para dañar o infiltrarse en los sistemas, sin el consentimiento del usuario, llamado **malware**.

La **seguridad antimalware** en las empresas, debe aplicarse a la totalidad de los equipos y dispositivos corporativos, incluidos los dispositivos móviles y los medios de almacenamiento externo como USB, discos duros portátiles, etc., y deben contar con las medidas necesarias para prevenir, detectar y contener cualquier tipo de amenaza a la que se vea expuesta nuestra organización.

Es útil considerar la planificación e instalación de software dedicado especializado que utilice una combinación de técnicas proactivas (para posibles amenazas desconocidas) y reactivas (para amenazas conocidas) para la detección e interceptación de código malicioso que pueda ser potencialmente peligroso para nuestros sistemas y actividades, y que pueda prevenir o limitar el daño que nos pueda causar. También se deben implantar las medidas preventivas o buenas prácticas para evitar que se den situaciones de riesgo.

Algunas de estas medidas o buenas prácticas que debemos aplicar en los sistemas de nuestras empresas para combatir el malware son:

- dividir la red de forma que un atacante que acceda tenga restringido el acceso a otros segmentos de red;
- proteger los privilegios administrativos, especialmente para cuentas por defecto y de administración, restringiendo su uso;
- realizar un listado de aplicaciones permitidas, para prevenir la ejecución de código malicioso;
- limitar la comunicación entre equipos y dispositivos de trabajo para reducir los objetivos donde el malware puede propagarse y ocultarse;
- aumentar la seguridad perimetral mediante cortafuegos perimetrales y de aplicación, *proxies*, *sandboxes* y filtrado dinámico;
- monitorizar los equipos de la red de forma centralizada, habilitando los logs en todos los equipos;
- actualizar y parchear del antivirus y de los sistemas;
- mantener el sistema de respaldo de las copias de seguridad protegido para que no le afecten los posibles ataques;
- tener un plan de respuesta a incidentes con roles, responsabilidades y procedimientos bien documentados.

La implantación de un sistema antimalware debe pasar por la instalación de software dedicado y especializado que detecte y neutralice todo tipo de amenazas. Deben cumplir las siguientes características:

- debe actualizarse de manera automática;
- aunque la mayoría de antivirus disponen de análisis en tiempo real, es recomendable realizar y planificar análisis periódicos;
- no debe ser posible desactivar el antivirus por el usuario final;
- si es posible, debe incluir la funcionalidad de análisis de páginas web y correo electrónico.

La concienciación y formación de los empleados es fundamental para garantizar el éxito de las medidas de seguridad implementadas.

¿Qué debe tener un antimalware?

Desde que aparecieron los primeros virus a finales del siglo pasado, disponer de un antivirus es una medida básica en la protección de cualquier empresa. Pero, como el de la gripe, es habitual que los virus informáticos muten para hacerse más dañinos y resistentes. En su evolución se han diversificado tanto que hemos terminado por llamarlos *malware*, abarcando este término, además de los virus otros tipos de software malicioso: troyanos, gusanos, spyware, *adware*, etc. Con tanta «cepa» suelta, ¿cómo nos preparamos para luchar contra el malware?, ¿cuáles deben ser las armas y defensas de un buen antimalware?

La concienciación y la aplicación de unas buenas prácticas en el uso de los sistemas tecnológicos y dispositivos móviles son algunas formas de luchar contra el malware. Aunque todo esto será más efectivo si seleccionamos un buen antimalware, que será nuestro mejor aliado en esta lucha. Para ello haremos como hacían los luchadores romanos, escoger y preparar cuidadosamente las armas y protecciones que vamos a utilizar en la batalla. Todo antimalware que se precie debe seleccionar, como buen gladiador, las armas y protecciones más adecuadas que le haga ganar la lucha sin perder la vida (o la empresa) en el intento.

Ha de ser ágil y capaz de poder detectar cuanto más malware mejor. Para ello comprobaremos **que detecte todo tipo de amenazas** y también que las detecte en **tiempo real**. Como muchas veces el malware entra vía correo electrónico o visitando páginas web, comprobaremos que dispone tanto de ***antiphishing* y *antispam* para el email**, como de **análisis de páginas web**. No menos importante es que realice **comprobaciones automáticas** ante cualquier descarga de ficheros.

También debe disponer de medidas para evitar, por error o mala intención, una mala utilización de los recursos de la empresa. Así, nuestro antimalware tendrá que dejarnos **filtrar las páginas web y las aplicaciones permitidas** (lista blanca) y necesarias para nuestra actividad. Así mismo tendrá que permitirnos bloquear esta configuración para evitar que el empleado pueda modificarla o desactivarla.

Es esencial que nuestro antimalware pueda **actualizarse con las nuevas firmas de malware**, es decir, de todas las nuevas cepas que van apareciendo. Finalmente tendrá que permitirnos programar **análisis periódicos** para comprobar que todo está bien y así rematar la tarea.

Actualizaciones

Para mantener un nivel adecuado de la ciberseguridad de nuestros sistemas de información, es imprescindible realizar una adecuada planificación de la **seguridad de las aplicaciones** que manejan la información.

Cualquier aplicación es susceptible de tener fallos de seguridad en su diseño, es decir vulnerabilidades, por lo que el fabricante va lanzando actualizaciones y parches que corrigen estos fallos. Los usuarios de estas aplicaciones debemos actualizarlas e instalar los parches cuando salgan para evitar que un ciber atacante o un usuario no autorizado puedan aprovechar estos agujeros de seguridad. Los atacantes escanean las redes en busca de equipos desactualizados para averiguar por donde poder atacarlos, aprovechando sus fallos del software. También se aprovechan de defectos de la configuración.

Es fundamental mantener constantemente actualizado y parcheado todo el software, tanto de los equipos como de los dispositivos móviles para mejorar su funcionalidad y seguridad, evitando riesgos como el robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, etc.

Es conveniente realizar un inventario de todos los activos y dispositivos informáticos de la empresa, donde se incluyan las características técnicas de los equipos, los sistemas operativos, versiones, licencias y aplicaciones instaladas con todas sus características. Para ello podemos ayudarnos de una base de datos de la gestión de configuración o **CMDB** (del inglés *configuration management database*), que permite inventariar servicios, hardware (ordenadores, servidores, *routers*, periféricos, etc.), redes, software, documentación, licencias, etc.

Para asegurar la correcta **actualización** de nuestros sistemas deberemos de seguir las siguientes pautas:

- mantener permanentemente **vigilado** el estado de actualización de todos los dispositivos y aplicaciones con los que contamos en nuestro inventario;
- configurar los sistemas para que las actualizaciones se instalen de manera **automática** en un horario en el que no afecte al trabajo de los usuarios;
- instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus;
- evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.

Actualización del gestor de contenidos

Es habitual que actualmente las páginas web estén basadas en los llamados gestores de contenidos (CMS), ¡como Joomla!, Drupal, Wordpress, etc. Se trata de herramientas que facilitan enormemente el proceso de creación y actualización y mantenimiento de una página web. Si este es nuestro caso es fundamental que mantengamos el gestor de contenido correctamente actualizado.

Cuando se descubre una vulnerabilidad nueva en un CMS, los ciberdelincuentes realizan sondeos mediante sistemas automáticos en busca de páginas con esas versiones vulnerables. Además, el gestor de contenidos (CMS) puede hacer uso de algún complemento (o *plugin*).
Es conveniente que al seleccionar dichos complementos nos fijemos en que sean ampliamente utilizados en internet, lo que garantiza su soporte y frecuente actualización frente a posibles incidencias de funcionalidad y seguridad.

Tanto si la gestión de la página web la llevamos nosotros como un tercero, la actualización del gestor de contenidos y sus complementos, además de la actualización del software del servidor deberán ser algunas de las tareas periódicas a realizar. Por otra parte, es conveniente estar suscrito a un servicio de avisos de seguridad del propio fabricante del gestor de contenidos y de otro software que utilicemos.

Seguridad de la red

Cada vez más, nuestras empresas manejan más y más información a través de los distintos sistemas de almacenamiento, equipos y dispositivos móviles que están permanentemente conectados a la red de trabajo y a internet. Internet es una fuente inagotable de amenazas para la seguridad de nuestras redes corporativas. Cualquier descuido al utilizar la web, el correo electrónico, algún tipo de mensajería instantánea, o un sistema de almacenamiento online, puede ser la puerta de entrada a un posible ataque que dañe la información y los sistemas de nuestras empresas.

El nivel de **seguridad de la red** corporativa es otro de los puntos clave para mantener nuestra empresa dentro de unos parámetros aceptables de ciberseguridad. Es esencial mantenerla protegida frente a posibles ataques o intrusiones. Para ello, es conveniente establecer unas pautas básicas como:

- restringir al máximo los accesos a nuestra red, deshabilitando las conexiones por defecto y habilitando únicamente los accesos necesarios;
- asegurarnos que cualquier nuevo equipo o dispositivo, que se conecte a la red corporativa, esté correctamente configurado y con el software antimalware actualizado;
- controlar y gestionar el uso de dispositivos móviles y medios de almacenamiento externo como USB, discos duros portátiles, etc., que son una puerta habitual de entrada de malware en la red y que pueden ser una importante fuente de fuga de información;

- limitar la navegación por internet para evitar la exposición a virus y otras amenazas que puedan hacer vulnerable nuestra red, poniendo especial atención a las conexiones a redes sociales y P2P;
- eliminar las cuentas y contraseñas por defecto que pueden dar lugar a posibles ataques de ciberdelincuentes;
- monitorizar todas las actividades de la red, de forma que dispondremos de información de los eventos y actividades que se desarrollan en la red, analizando la manera con que se utilizan los recursos para poder mejorar la gestión de estos;
- definir responsabilidades y procedimientos de trabajo para la gestión del equipamiento de red. Todas estas medidas serán incluidas dentro del plan de seguridad de la empresa.

Otro aspecto importante que no podemos descuidar es la **configuración de nuestra wifi** pues puede permitir el acceso a nuestra red corporativa a personas ajenas.

Algunas buenas prácticas para aumentar la seguridad de la red wifi corporativa son:

- cambiar el usuario y la contraseña de acceso a la configuración del *router*, pues suelen ser contraseñas por defecto que son de conocimiento público,
- modificar, y cambiar regularmente, la contraseña de acceso a la red wifi que viene configurada de fábrica en el *router*, por otra personalizada que cumpla los requisitos mínimos de seguridad,
- ocultar el nombre de la red wifi (SSID) de la empresa, para que esta no sea «visible» por dispositivos ajenos a la empresa. De esta forma dificultamos los intentos de conexión indeseados,
- proteger la red wifi utilizando cifrado en las comunicaciones (activando cifrado WPA/ WPA2),
- permitir acceder a la red únicamente a los dispositivos de trabajo (esto se puede hacer activando el filtrado de direcciones MAC).

Cabe destacar también el peligro que suponen las conexiones realizadas por los dispositivos móviles desde el exterior, ya que pueden acceder a sistemas y recursos internos de la empresa desde **redes wifi públicas abiertas** o sin las debidas garantías de seguridad, como son wifis de cortesía de restaurantes, hoteles, aeropuertos, etc. Hay que evitar el uso de estas redes en la medida de lo posible, y si se utilizan se deben extremar las medidas de seguridad, adoptando sistemas de cifrado de datos y comunicaciones, haciendo uso de una **Red Privada Virtual o VPN** (del inglés *Virtual Private Network*) o utilizando conexiones 3G/4G.

Información en tránsito

La globalización y la deslocalización de los procesos productivos de las empresas, hace que necesitemos trabajar y acceder a la información de trabajo desde cualquier lugar; de manera inmediata, rápida y ágil. Por ello, para ser más productivos, hace que cada vez más utilicemos nuestros dispositivos móviles, ya sean de uso corporativo o personal, para acceder y compartir la información de trabajo con otros compañeros, clientes, proveedores, etc. desde cualquier lugar o dispositivo autorizado, ya sea desde dentro de la empresa o desde fuera de ella.

Esta «movilidad» nos aporta grandes ventajas, pero hay que tener muy presente también los riesgos que conlleva y cómo gestionarlos. Riesgos como:

- pérdida o robo de información confidencial,
- el mal uso que se pueda hacer de los dispositivos,
- robo de dispositivos,
- robo de credenciales,
- utilización de sistemas de conexión no seguros, etc.

Todo esto hace que establezcamos los mecanismos necesarios para asegurar la **seguridad en movilidad** de estos dispositivos y de las redes de comunicación utilizadas para acceder a la información corporativa.

Para la protección de la información almacenada en estos dispositivos, debemos aplicar una serie de medidas básicas como las siguientes:

- Contemplar el uso de los dispositivos móviles, teletrabajo e información almacenada fuera de las instalaciones de la empresa, dentro de la política de seguridad de la empresa.
- No dejar los dispositivos móviles desatendidos en lugares públicos, coche, etc.
- Evitar utilizar redes wifi ajenas, especialmente aquellas que no llevan contraseña. Cuando sea posible, utiliza tu propia conexión 3G/4G.
- Utilizar siempre una conexión VPN para enviar o recibir información sensible desde una red poco confiable.
- Tener siempre el antivirus y el dispositivo actualizado, especialmente fuera de las redes corporativas.
- Utilizar siempre herramientas de cifrado de datos y comunicaciones para proteger la información sensible de los dispositivos.
- Salvaguardar la información periódicamente según su criticidad, mediante la realización de copias de seguridad periódicas.

BYOD

Especial atención hay que tener en cuenta al modo de trabajar denominado ***BYOD*** (por sus iniciales en inglés, *Bring Your Own Device*), caracterizado por el hecho de **permitir a los empleados la incorporación de sus dispositivos móviles personales** (portátiles, *smartphones* y tabletas**) a las redes corporativas** desde su casa**,** la propia oficina o cualquier otro lugar, aceptando su uso compartido, tanto para las tareas profesionales de uso corporativo como para las personales de los empleados.

Una buena parte de los riesgos que conlleva el BYOD estriba en el uso que haga de los dispositivos el usuario. Para minimizar los riesgos derivados del uso de dispositivos BYOD a la hora de integrarlos dentro de la organización y obtener el mayor rendimiento posible de los mismos, seguiremos estos consejos:

- **Involucrar a los usuarios en la protección de sus propios dispositivos**. Debemos incentivar, concienciar y formar al usuario para que tome medidas destinadas a proteger los datos corporativos y personales.
- **Mantener una base de datos de usuarios y dispositivos**. Es conveniente mantener una base de datos con la relación de dispositivos que acceden a los recursos de la empresa, los usuarios que los manejan y los privilegios de seguridad que nos permitan autenticar y autorizar estos usuarios y dispositivos.
- **Tomar precauciones con el almacenamiento de datos de trabajo**. Hay que tener especial cuidado con las herramientas que utilizamos para el almacenamiento de datos corporativos, especialmente a la hora de utilizar aplicaciones de intercambio de archivos en la nube. Las aplicaciones públicas instaladas por los usuarios no son tan seguras como las corporativas para proteger los datos sensibles de nuestra empresa. A la hora de trabajar con los datos de la empresa, es más seguro tener estos almacenados en la nube y consultarlos, que realizar un intercambio de archivos real.
- **Implementar** medidas para el acceso seguro a la información. Desde la empresa se deben implementar en los dispositivos mecanismos adicionales de seguridad como el cifrado de la información y la correcta autenticación de usuarios. Se puede optar por sistemas de autenticación mediante contraseñas, utilizando aplicaciones gestores de contraseñas, que facilita el uso de contraseñas fuertes personalizadas para cada aplicación, o sistemas mixtos de utilización de contraseña y medios biométricos como huellas digitales.
- **Modificar las políticas de seguridad de la empresa**. Se deben actualizar las políticas de seguridad para incluir el uso de BYOD, reforzando el apartado referente a la política de protección de datos corporativa. También debemos concienciar a los usuarios de la importancia y la necesidad de la aplicación de esta política de protección de datos.

Comunicaciones inalámbricas

En la mayoría de las redes inalámbricas que utilizan los trabajadores fuera del entorno empresarial debemos **asumir que no existe protección de datos alguna**. A menudo, información confidencial de nuestra empresa puede transmitirse a través de redes inalámbricas que no están bajo nuestro control, por lo que debemos asegurarnos de que los datos viajan convenientemente protegidos.

La manera de evaluar la seguridad de una solución inalámbrica es a través de su capacidad para mantener la confidencialidad, la integridad y la autenticidad de los datos a través de la red inalámbrica, desde el dispositivo móvil hasta la red corporativa.

Redes wifi de terceros

Es habitual que un empleado utilice con frecuencia redes públicas abiertas o poco seguras para el intercambio de correo electrónico corporativo o acceder a aplicaciones de la empresa. Este tipo de redes podemos encontrarlas como servicio de cortesía en restaurantes, hoteles, aeropuertos, etc.

Los motivos habituales para el uso de estas redes inseguras suelen ser la velocidad de la red, no disponer de conexión de datos (3G, 4G,…) en el portátil, ahorrar tarifa de datos o por el tipo y calidad de la cobertura. Sin embargo, a menudo su uso se realiza sin pensar en las posibles consecuencias.

Es primordial utilizar este tipo de redes con algún tipo de seguridad adicional. Utilizar este tipo de redes con algún tipo de cifrado punto a punto como los sitios web con SSL (que son los que empiezan con HTTPS y tienen un candado junto a la dirección) o como la posibilidad que ofrece VPN.

A modo orientativo se podría decir que:

Wifi	**A dónde te conectas**	**¿Qué puedes hacer?:**
Pública y no segura	A un sitio web no seguro	Sólo actividades de bajo riesgo: Navegar Leer noticias
Pública y no segura	A un sitio web cifrado (https://) y con candado	Actividades de riesgo moderado: Login (inicio de sesión) en sitios en los que estás suscrito
Público pero segura (WPA)	A un sitio web cifrado (https://) y con candado	Actividades de alto riesgo Email Trabajar con documentos online Redes sociales
Pública y segura	A sitios web cifrados o no	Actividades de muy alto riesgo Banca online Paypal o tarjetas de crédito

No obstante, algunas aplicaciones, como las de correo electrónico o archivo de documentos en la nube, redes sociales, tienen la posibilidad de configurar cuándo se sincronizan. En la sincronización intercambian credenciales de acceso. **Desactiva la sincronización automática** cuando utilices redes en las que no confíes.

A veces el usuario piensa que conectarse a este tipo de redes para tareas que no necesitan una seguridad considerable (como leer el periódico) no conlleva riegos. Sin embargo, en los dispositivos móviles las aplicaciones como el correo siguen funcionando, aunque la aplicación no esté en pantalla. Por tanto, no es posible asegurar que los datos que atraviesan la red segura son de poca importancia.

Redes inalámbricas de corta distancia

Hoy en día disponemos de otro tipo de redes inalámbricas de corta distancia como /Bluetooth y Zigbee, que nos permiten conectar varios dispositivos cercanos entre sí.

Las redes Bluetooth se utilizan para conectar ratones y teclados con el ordenador, o los relojes (*smartwatches*), pulseras de actividad con el ordenador de a bordo del coche con el Smartphone. Las redes Zigbee se utilizan en dispositivos domóticos y en automatización de edificios. En general, si se usa en dispositivos corporativos o personales, se han de tomar las siguientes medidas de seguridad:

- activarlos sólo cuando se vayan a utilizar
- no aceptar ninguna conexión desconocida y requerir siempre autenticación
- configurar los dispositivos para que no resulten visibles a terceros y revisar periódicamente la lista de dispositivos de confianza registrados
- asignar nombres a los dispositivos que no reflejen marcas ni modelos
- mantener actualizado el software del *smartphone*

Acceso remoto

El mejor sistema para la conexión remota a los equipos de nuestra organización es mediante la utilización de una red privada virtual, también llamada VPN. Esta tecnología de red proporciona un acceso seguro a las aplicaciones y sistemas corporativos a empleados dispersos geográficamente, de una manera equivalente al tipo de acceso que tendrían en los locales de nuestra empresa.

Una red privada virtual se basa en la técnica de *tunneling*, en la que haciendo uso de ciertos protocolos (IPSEC, SSTP, etc.) permite a los datos transferidos de un extremo a otro de la VPN, (por ejemplo, nuestro dispositivo y la red de la organización) ser asegurados por algoritmos de criptografía.

El término «túnel» se utiliza para simbolizar el hecho de que los datos de entrada y salida se transmiten por un canal cifrado, por tanto, incomprensibles para cualquier persona pueda interceptar el tráfico de la VPN.

Una conexión remota utilizando esta tecnología presenta las siguientes ventajas:

- Permite al usuario conectarse a la organización de una manera totalmente segura, incluso desde redes abiertas o poco seguras.

- Funciona sobre conexiones 3G, 4G y wifi, de modo que es una capa de seguridad extra sobre la red que estemos utilizando.
- Limita el medio de acceso remoto a nuestra organización a un único punto con autenticación, lo que permite un mayor control de los accesos.
- Reduce los servicios expuestos a Internet, disminuyendo la posibilidad de ser atacados.

Sin embargo, si la contraseña de acceso a la VPN resulta comprometida por un atacante, éste dispone de un acceso a la red interna de nuestra empresa, por lo que puede resultar muy peligroso. Existen opciones de seguridad ofrecidas en los sistemas VPN que pueden minimizar o anular estos riesgos:

- Por un lado, la posibilidad de usar certificados para la autenticación mutua confiere protección frente al riesgo de que alguien se pueda hacer pasar por el usuario de uso legítimo.
- Por otra parte, una doble autenticación utilizando certificado y contraseña hace muy difícil robar las credenciales de acceso, ya que se necesitan los dos elementos para autenticarse.

Gestión de soportes

La creciente dependencia de la mayoría de las organizaciones de sus sistemas de información pone de manifiesto la necesidad de contar con medios y técnicas que permitan almacenar la información de la manera más adecuada.

Una correcta gestión de este proceso permite mantener en todo momento la integridad, confidencialidad y disponibilidad de la información.

Las empresas necesitan infraestructuras de almacenamiento flexibles y soluciones que protejan y resguarden la información y se adapten a los rápidos cambios del negocio y las nuevas exigencias del mercado, garantizando el rápido retorno de la inversión efectuada. Alineando las diferentes soluciones de almacenamiento con los requerimientos del negocio se consigue hacer un uso más correcto de las mismas. Estos son los tipos de almacenamiento de información en la empresa:

- almacenamiento local
- servidores de almacenamiento en red
- dispositivos externos
- servicios de almacenamiento en la nube

Tipos de dispositivos de almacenamiento

Los dispositivos de almacenamiento constituyen una parte vital de cualquier sistema o instalación informática. La tendencia general en el mercado de los dispositivos de almacenamiento de información se dirige, por un lado, al continuo incremento de su capacidad y, por otro, a desarrollar funcionalidades como la rapidez, la fiabilidad, la economía y el tamaño. Esta evolución se traduce en una disminución del coste, lo que ha permitido aumentar el número de empresas que utilizan estos dispositivos. La gama es amplia y las funcionalidades dependen del tipo de dispositivo, aunque como aproximación, se indican los siguientes:

- Discos duros (HDD y SSD): dispositivo de almacenamiento utilizado en todos los ordenadores como almacenamiento principal. Los HDD son discos duros magnéticos y llevan piezas mecánicas. Los SSD, discos de estado sólido, son electrónicos, más rápidos y silenciosos, pero de menor capacidad. En ambos casos se pueden encontrar de distintas capacidades de almacenamiento y permiten tanto la lectura como la escritura. Los discos duros también se utilizan como medios de almacenamiento externos conectados a los equipos por medio de conectores USB (*Universal Serial Bus* o conductor universal en serie), eSATA, Firewire o Thunderbolt. En el mercado también hay discos duros que se conectan de forma inalámbrica.
- Cintas magnéticas DAT/DDS (*Digital Audio Tape/Digital Data Storage*) / LTO (*Linear Tape-Open*): utilizadas principalmente como medio de almacenamiento en los sistemas de copias de seguridad, ya que resultan económicas para almacenar grandes cantidades de datos. El acceso a los datos es sensiblemente más lento que el de los discos duros.
- CD (*Compact Disc*) / DVD (*Digital Versatile Disc*) / Blu-ray Disc (BD): dispositivos de almacenamiento óptico con diferentes capacidades de almacenamiento. Son un medio económico y fácil de transportar o conservar. También al ser dispositivos que permiten una escritura y muchas lecturas, son adecuados para hacer copias de seguridad anti-ransomware, es decir, que no podrán ser secuestradas por malware que pida rescate para su recuperación.
- sistemas de almacenamiento en red: las empresas que necesitan almacenar gran cantidad de información utilizarán los sistemas de almacenamiento en redes del tipo NAS (*Network Attached Storage*), para archivos compartidos, o SAN (*Storage Area Network*) de alta velocidad para bases de datos de aplicaciones. Presentan un volumen de almacenamiento grande, ya que unen la capacidad de múltiples discos duros en la red local como un volumen único de almacenamiento. Las reglas de acceso permiten llevar un control de quién tiene acceso y a qué partes de la información almacenada se tiene acceso.
- Memorias USB y USB-OTG: denominado con múltiples nombres como llavero USB, memoria USB o pendrive. Es un pequeño dispositivo de almacenamiento que dispone de una memoria electrónica de altas prestaciones para el almacenamiento de la información. La capacidad de los pendrives es cada vez mayor y es uno de los medios más utilizados para transportar la información de un lugar a otro. Esta movilidad, unida a la rapidez con la que se conecta y desconecta en diferentes equipos, lo hace especialmente susceptible a la pérdida de información, por extravío o sustracción del dispositivo o por rotura física del mismo.

En general para adquirir un dispositivo de almacenamiento se ha de tener en cuenta, además del precio y del tamaño, estas consideraciones:

- Capacidad de almacenamiento (en GB, TB…) adecuada a nuestras necesidades.
- Compatibilidad del sistema de archivos, el formato lógico en el que se almacena la información, con nuestro sistema operativo. Por ejemplo, NTFS y FAT en Windows o HFS y HFS+ para Mac OS.
- Compatibilidad del interfaz de conexión (USB 2.0, 3.0…) con el de nuestro sistema.
- Velocidad de transferencia (Kb/s, Mb/s); y si tiene o no caché o buffer, una memoria de intercambio que agiliza la transferencia, en el caso de discos duros.
- Tipo de almacenamiento, ya que influye en la velocidad de acceso (óptico, magnético o electrónico) y si tiene partes mecánicas, como los HDD, por el ruido que pueda producir y por la necesidad de algún tipo de mantenimiento.

Gestión de soportes

Para garantizar un correcto uso de los soportes en la empresa se ha de llevar un control de los soportes permitidos, etiquetándolos y controlando su uso.

Los soportes extraíbles constituyen una de las principales amenazas de fuga de información, así como de infección por malware. Limitar la utilización de dispositivos USB, quizá sea una medida demasiado drástica. No obstante, debemos evaluar la posibilidad de bloquear estos puertos y eliminar las unidades lectoras/grabadoras de soportes ópticos de los equipos de usuarios.

Por otra parte, para incrementar la seguridad de la información en tránsito debemos cifrarla.

Por último, cabe señalar la importancia de hacer un borrado seguro de la información de los soportes que queden obsoletos o se vallan a sustituir por otros.

Registro de actividad

Una de las herramientas que nos permite detectar posibles problemas o deficiencias de los sistemas de información es la **monitorización,** que nos permite evaluar los parámetros de calidad establecidos en los distintos servicios, como su grado de disponibilidad y rendimiento, el espacio de almacenamiento, etc.

Para poder tener una idea global de lo que ocurre en los sistemas de información y redes corporativas, es preciso recabar toda la información posible sobre todas las actividades de los distintos procesos y actividades llevadas a cabo en ellos. Para ello debemos monitorizar y analizar constantemente todos estos elementos. Este proceso de monitorización pasa por las fases de:

- recolección de la información y datos,
- detección de posibles anomalías y
- análisis de la información.

A la hora de recolectar la información, debemos registrar y analizar toda la información de la actividad de los sistemas, como la relativa al tráfico de red, accesos autorizados o rechazados a sistemas o aplicaciones, cambios en la configuración de sistemas, uso de privilegios especiales, registros de los sistemas antimalware, volumen de tráfico de red y de entrada/salida a internet, alarmas o avisos de incidentes generados en los sistemas, etc.

Al realizar un análisis de toda esta información podremos prever y detectar situaciones anómalas o de riesgo, o posibles fallos de seguridad antes de que ocurra un incidente de seguridad. También nos servirá para identificar y mitigar los fallos de seguridad con más rapidez, una vez producidos estos.

Los sistemas de monitorización deben contemplar también los problemas físicos y de rendimiento de los sistemas como el nivel de funcionamiento de un SAI, la temperatura de los servidores, la carga de CPU o Disco Duro de los servidores, etc. De esta forma podremos realizar un análisis de la capacidad de los servidores y sistemas corporativos para detectar problemas de seguridad, rendimiento o funcionalidad permitiéndonos, de forma proactiva, programar cambios o sustituciones de los equipos susceptibles de fallar antes de que ocurra cualquier problema.

Continuidad de negocio

Las empresas deben estar preparadas para prevenir, protegerse, y reaccionar ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permitan a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. De esta forma se garantiza poder dar una respuesta planificada ante cualquier fallo de seguridad. Esto repercutirá positivamente en el cuidado de nuestra imagen y reputación como empresa, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes.

Debemos tener en cuenta que el término continuidad del negocio no hace referencia exclusivamente a aspectos relacionados con las tecnologías de la información.

Aunque podría pensarse que la continuidad del negocio es un ámbito exclusivo de las grandes organizaciones, esto no es cierto. Si bien existe una diferencia significativa, cada organización establece las medidas necesarias y proporcionales a sus necesidades para garantizar su continuidad en caso de desastre. Si hablamos del ámbito tecnológico, por ejemplo, mientras que una gran organización puede requerir el despliegue de un centro de respaldo alternativo, tanto de comunicaciones, sistemas como servidores en una ubicación remota, en otros casos podría ser óptimo realizar copias de seguridad en la nube, primando el rendimiento frente al coste.

Los planes de continuidad de negocio pueden ayudarnos a:

- Mantener el nivel de servicio en los límites definidos.
- Establecer un periodo de recuperación mínimo.
- Recuperar la situación inicial ante cualquier incidente.
- Analizar los resultados y los motivos de los incidentes.
- Evitar que las actividades de la empresa se interrumpan.

Por todo ello, debemos considerar, desde un punto de vista formal, aquellos factores que pueden garantizar la continuidad de una empresa en circunstancias adversas. Este proceso implica las siguientes fases:

- Fase 0. Determinación del alcance. Si nuestra empresa presenta cierta complejidad organizativa, abordar un proceso de mejora de la continuidad puede suponer emplear un número de recursos y un tiempo excesivo. Por tanto, es recomendable comenzar por aquellos departamentos o áreas con mayor importancia y progresivamente ir ampliando la continuidad a toda la organización. Para ello siempre con el compromiso e implicación de la dirección.
- Fase 1. Análisis de la organización. Durante esta fase recopilamos toda la información necesaria para establecer los procesos de negocio críticos, los activos que les dan soporte y cuáles son las necesidades temporales y de recursos.
- Fase 2. Determinación de la estrategia de continuidad. Conocidos los activos que soportan los procesos críticos, debemos determinar si en caso de desastre, seremos capaces de recuperar dichos activos en el tiempo necesario. En aquellos casos en los que no sea así, debemos establecer las diversas estrategias de recuperación.
- Fase 3. Respuesta a la contingencia. A partir de las estrategias de recuperación escogidas, se realiza la selección e implantación de las iniciativas necesarias, y se documenta el Plan de Crisis y los respectivos documentos para la recuperación de los entornos.
- Fase 4. Prueba, mantenimiento y revisión. A partir de la infraestructura tecnológica de nuestra empresa, desarrollaremos los planes de prueba y mantenimiento.
- Fase 5. Concienciación. Además del análisis y la implantación, es necesario que tanto el personal técnico como los responsables de nuestra empresa conozcan qué es y qué supone el Plan de Continuidad de Negocio, así como qué se espera de ellos.

CONTACTE CON GRUPO GALILEA

Gran Via Carles III, 62 · 08028 · BARCELONA
93 414 51 51
info@grupogalilea.com