CASTILLA Y LEÓN

“MANUAL DE SEGURIDAD INFORMÁTICA EN LA EMPRESA”

Proyecto COMPETIC

Apoyo a emprendedores, autónomos y microempresas del entorno rural para crear y hacer crecer sus negocios aprovechando las oportunidades de las TIC

Cámara Zamora

ipb Instituto Politécnico de Bragança

Diputación de Avila

ACISAT

Interreg España - Portugal

Fondo Europeo de Desarrollo Regional
Fundo Europeu de Desenvolvimento Regional

UNIÓN EUROPEA
UNIÃO EUROPEIA

COMPETIC

Junta de Castilla y León

COMPETITIVIDAD

Este Manual ha sido elaborado por ENCLAVE FORMACIÓN para las actuaciones de sensibilización y formación en ciberseguridad y confianza en el ámbito digital, desarrolladas en el proyecto COMPETIC que se desarrolla en el ámbito del Programa Operativo de Cooperación Transfronteriza España – Portugal 2014-2020, Programa INTERREG V A España - Portugal (POCTEP), dentro del Objetivo Temático 3: Mejorar la competitividad de las pequeñas y medianas empresas. Este proyecto se encuentra cofinanciado en un 75% por el Fondo Europeo de Desarrollo Regional (FEDER).

Más información del proyecto:

Web: http://competic-poctep.com

Email: info@competic-poctep.com

ÍNDICE

CAPÍTULO 1. LA IMPORTANCIA DE LA SEGURIDAD TIC EN LAS PYMES.

1. CONCEPTOS BÁSICOS SOBRE CIBERSEGURIDAD.

Hoy en día, las empresas y profesionales, utilizamos las nuevas tecnologías para llevar a cabo nuestra actividad profesional por las posibilidades que nos ofrece:

- Somos más productivos.
- Llegamos a mercados a los que hace unos años era impensable acceder.
- Disponemos de nuevos canales, y más económicos, de comunicación con clientes y proveedores.

La Tecnología llegó hace años a nuestros entornos personales y profesionales para quedarse y no se va a marchar nunca, fundamentalmente porque ya no sabríamos ni vivir ni trabajar sin ella.

A través de Internet, desarrollamos nuestros negocios, sin embargo, **sólo alcanzarán el éxito aquellos que se adapten a este nuevo medio de trabajo**, sacando el máximo partido de ellas. Al resto les pasará, probablemente, como a los dinosaurios, que acabarán desapareciendo.

Estamos en el siglo en el que la Tecnología va a cambiar radicalmente nuestra forma de vivir y trabajar. No dejamos de oír hablar de términos como **BigData**, **Machine Learning**, **IA** (Inteligencia Artificial), **IoT** (Internet de las Cosas), **Vehículos Autónomos**, … y **Ciberseguridad**.

Si hay algo que trasciende a todas las Tecnologías existentes y futuras es la necesidad imperiosa de dotarlas de una seguridad que haga que su uso nos ayude, no para lo contrario. Las tecnologías, como ha ocurrido siempre, aparecerán y desaparecerán, sin embargo, la Ciberseguridad perdurará para siempre.

Por otro lado, y ciñéndome a lo que ha ocurrido en los últimos 50 años, la realidad es que no sabemos construir tecnología segura. Al principio la escusa era que la tecnología se diseñó atendiendo a su usabilidad, sin pensar en su seguridad (porque en ese momento no era necesario), sin embargo, la que seguimos creando hoy día sigue viéndose afectada por innumerables vulnerabilidades que provocan riesgos por el mero hecho de usarlas. Por eso también oiremos que “la seguridad informática 100% no existe”.

Para comprobar que esto es así sólo tenemos que fijarnos en los datos que nos ofrecen los organismos internacionales que se encargan de catalogar las vulnerabilidades que reportan los fabricantes de hardware y software, por ejemplo, Mitre (https://www.cve.mitre.org).

De acuerdo con **CVE Details**, de Mitre, en 2017, las vulnerabilidades han sobrepasado por mucho los registros de años previos, habiendo sido reportadas más de **14.700 vulnerabilidades**, contra las **6.447 de 2016**. El crecimiento se ha más que duplicado respecto a los reportes de 2016, con un aumento por encima del 120% de un año a otro. Y cuando veamos las cifras de este año 2018, veremos que la progresión sigue siendo exponencial.

Por otro lado, la **ciberdelincuencia** también está disparada. Y no es de extrañar. El anonimato que ofrece el uso de la tecnología para cometer delitos hace que sea muy rentable asumiendo un riesgo muy bajo.

La máxima de, "**o te sacan el dinero o te convierten en dinero**" es una realidad para todos: empresas grandes y pequeñas, administraciones públicas, estados y particulares, no se libra nadie. Se trata de un aspecto de crucial importancia en un entorno interconectado y dependiente de la tecnología.

Por este motivo debemos intentar evitar la sobreexposición a la que nos vemos afectados por el uso de la tecnología y esto lo conseguiremos si sabemos protegernos.

De todos depende alcanzar un grado de seguridad y de confianza en el ámbito digital que permita un desarrollo económico favorable para todos.

Pero… ¿estas cosas a mí no me pasan?

Acabamos de decir que nos afecta a todos. Además, las pequeñas empresas y los autónomos somos un objetivo más fácil y barato de atacar, por parte de los ciberdelincuentes, que las grandes empresas y sus costosas y sofisticadas medidas de seguridad.

Más de la mitad de las empresas españolas ha sufrido algún tipo de fraude económico en los últimos dos años. Esta es una de las principales conclusiones de la encuesta mundial sobre el delito económico que PwC ha elaborado, a partir de 7.228 entrevistas en 123 países. Esta cifra sitúa a España por encima de la media mundial, por encima de los principales países de nuestro entorno.

Fuente: Informe PwC 2018

Desde 2009, el porcentaje de empresas españolas, víctimas de delitos económicos ha crecido casi 20 puntos, pasando del 35% al 54%. Un incremento que tiene que ver con aumento de las Nuevas Tecnologías y paradójicamente con el aumento de los controles y de una mayor consciencia y persecución de este tipo de fraudes por parte de las compañías.

La apropiación indebida, la corrupción y el soborno, la manipulación contable y los ciberataques son los principales delitos económicos que padecen las empresas. Y todo apunta a que, en los próximos dos años, el ciberfraude va a ir ganando peso significativamente.

Para combatir esta situación, las empresas españolas están aumentando los presupuestos destinados a luchar contra los ciberataques. Sin embargo, una de cada diez empresas todavía no ha realizado ningún tipo de revisión ni evaluación de riesgos.

Por eso, tenemos más probabilidades de ser objetivo de un ciberataque o de sufrir un incidente de seguridad. Tenemos que ser conscientes de que debemos proteger nuestros recursos, ya que nos arriesgamos a:

- Perder información vital para muestro negocio.
- No disponer de los equipos, sistemas o servicios cuando los necesitemos.
- Que nos roben nuestro dinero.
- Que nos extorsionen, secuestrando nuestros equipos informáticos al vernos afectados por ataques de tipo Ransomware o similares.

En definitiva, no podemos permitirnos que ni nuestros negocios ni nuestros clientes puedan sufrir perjuicio alguno.

Los riesgos asociados al uso de la tecnología pueden estar provocados por diversas causas:

- **Descuidos o errores**, en un porcentaje muy elevado de las ocasiones.
- **Falta de concienciación** de la importancia de la ciberseguridad.
- **Ataques externos** o internos malintencionados.
- **Causas naturales** como incendios, inundaciones, etc.

Todo esto puede causarnos daños económicos y comprometer la continuidad de nuestro negocio. Por ello, es importante que conozcamos los riesgos derivados del uso de las nuevas tecnologías, de cara a intentar minimizar el riesgo de sufrir uno de estos problemas.

Internet, la nube y más recientemente los desarrollos de Big Data, Machine Learning e Internet de las cosas (IoT), están provocando un cambio de paradigma:

- El mundo físico y digital están hiperconectados.
- Los usuarios son un elemento activo.
- La información es procesada, almacenada y transmitida sin restricciones.
- Hoy día generamos más información en un solo año de la que habíamos generado hasta el año 2011.
- Y las organizaciones tenemos a nuestro alcance mecanismos que antes sólo podían imaginar.

Este hecho tiene una gran trascendencia tanto para las empresas como para la sociedad. Los mercados y la economía se han hecho globales y digitales. La ciberseguridad se hace indispensable.

Proteger la privacidad del consumidor, protegernos frente a las ciberamenazas (malware, fugas de datos, extorsiones, robos de identidad, ...), intencionadas o no; y fomentar la seguridad en servicios constituyen un factor esencial para el desarrollo de la sociedad. Por ello la legislación está adaptándose para que las sociedades puedan aprovechar las ventajas de este nuevo paradigma sin que haya una merma de derechos y libertades.

Será complicado que se legislen estos nuevos ciberproblemas a la misma velocidad a la que avanza la tecnología, sin embargo, esa legislación debe ser más rápida, ya que surgen constantemente nuevos ciberdelitos que, o se apoyan en la tecnología para cometerse o directamente se cometen en el ciberespacio, sin que hasta la fecha se pueda hacer gran cosa para perseguirlos. Las mismas FFSS del Estado nos dicen que, como el ciberdelincuente no se encuentre físicamente en España o si el dinero que nos han robado sale del país, prácticamente no hay nada que hacer.

Para que nos hagamos una idea del calado del problema, informes de Europool, de finales de 2016, ya hacen referencia a que ya hay países en los que los ciberdelitos superan, porcentualmente, a los delitos tradicionales.

Recuerda. La ciberseguridad de tu empresa es imprescindible y depende en gran parte de ti.

La mayoría de las grandes multinacionales son conscientes de los riesgos que asumen al utilizar la tecnología en sus procesos productivos y lo reflejan con inversiones, cada vez mayores, en ciberseguridad. Sin embargo, la percepción de este peligro en empresas más pequeñas es reducida y son pocas las que tienen entre su lista de prioridades proteger sus sistemas.

Y necesitamos cambiar el chip, porque para las pymes, la informática siempre se ha considerado un gasto y no una inversión y no iba a suceder de forma distinta en lo referente a la ciberseguridad. Necesitamos invertir en tecnología y su seguridad para conseguir que nuestros negocios puedan competir con las mismas garantías que los demás.

Las pymes ocupan a diez millones de trabajadores en España y suponen más del 60% del PIB nacional, según datos del Ministerio de Economía. La Confederación Española de la Pequeña y Mediana Empresa puede presumir de que estas compañías conforman la práctica totalidad del tejido empresarial del país. Por eso, no es de extrañar que el 70% de los ataques informáticos que se produjeron el año pasado —que rondan los 125.000, según estimaciones del Instituto Nacional de Ciberseguridad— estuvieran dirigidos a pymes.

La inversión de las empresas con menos de 250 empleados en ciberseguridad es inversamente proporcional al riesgo que tienen de ser atacadas.

Las pymes piensan que no son objetivos de los ciberdelincuentes, pero la realidad es que normalmente estos no son personas atacando ordenadores, sino máquinas atacando a máquinas; por lo que los ataques son indiscriminados. Además, con cientos de miles de sistemas, ¿por qué atacar al que está protegido?

Visto así parece que todos tuviéramos la obligación de ser ingenieros informáticos para vivir/trabajar más seguros en el mundo actual, pero no es así. Lo que si es necesario es un proceso de concienciación generalizado, al igual que ocurre con otros aspectos de nuestras vidas que ya tenemos interiorizados, y para eso está este curso.

1.1. EL VALOR DE LA INFORMACIÓN EN LA EMPRESA.

Antes de nada, debemos tener claras dos ideas:

- La primera es que **lo que realmente tiene valor en tu negocio es la información** con la que trabajas y tenemos que identificar que activos de información utilizamos y cuales son las fuentes de las que proceden.
  Tener que sustituir los equipos informáticos puede ser más o menos costoso, sin embargo, la mayoría de las empresas que pierden sus datos no pueden seguir desarrollando su

actividad con normalidad, llegando a desaparecer, en un corto periodo de tiempo, cuando la recuperación de la información no es factible.

Algunos definen a los datos como el petróleo del siglo XXI.

- La segunda es que **debemos diferenciar entre Seguridad Informática y Seguridad de la Información**.

  Cuando hablamos de **Seguridad Informática** nos referimos a la Seguridad de la infraestructura tecnológica (equipos informáticos y de comunicaciones) que utilizamos para que nuestro negocio pueda desarrollarse a diario.

  Cuando hablamos de **Seguridad de la Información**, nos referimos a ese activo que decíamos que era el que realmente tiene valor, los datos, la información.

Nuestra empresa obtiene la información desde **múltiples fuentes (internas y externas)**, la almacena en **múltiples soportes** (digitales y no digitales) y la utiliza a través de **múltiples servicios** (documentos internos, correos electrónicos, información mostrada en nuestras páginas web, datos que almacenamos en nuestras bases de datos, …).

También tenemos que tener en cuenta lo que se denomina **ciclo de vida de la información**, ya que lo que hoy es importante para nosotros puede dejar de serlo en el futuro.

Por todo lo descrito anteriormente, debemos realizar un análisis que nos permita:

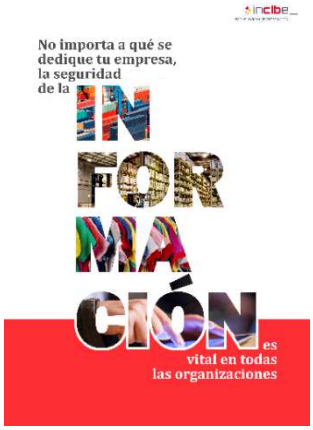
- Estructurar nuestros sistemas de información.
- Nos permita clasificar nuestros activos de información en base a su criticidad actual y futura, de tal manera que nos permita identificar los procedimientos que debemos seguir para protegerlos, cumpliendo con la normativa vigente.
- Y nos permita definir una serie de controles que nos permitan medir cómo de eficaces son las medidas de seguridad que adoptamos.

Por otro lado, la concientización y educación de los usuarios debe realizarse de forma periódica, implicando a todos en el programa de seguridad que estamos definiendo. Nunca conseguiremos un resultado óptimo sin involucrar a todo el personal de la empresa.

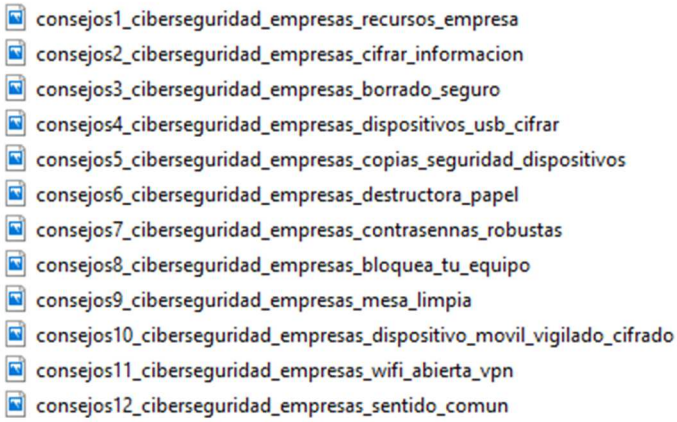
Instrumentos de concienciación:

- **INCIBE**: Desde https://www.incibe.es/protege-tu-empresa, conviene:
  - Seguir las publicaciones y formación sectorial que se publica recientemente el Instituto Nacional de Ciberseguridad.

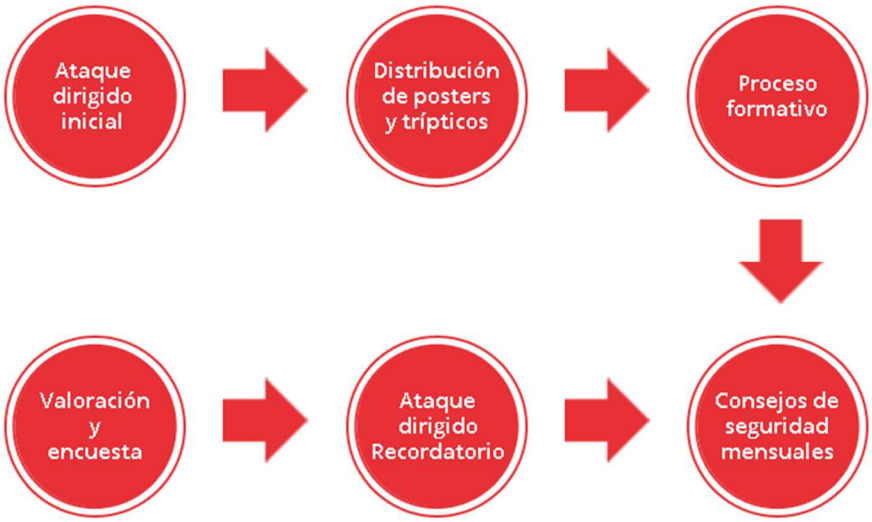
- Descargar los kits de concienciación que encontramos en la misma página web en los que tendremos acceso a pósteres y trípticos que podremos colocar en la empresa.



- Publicar en las redes internas los consejos que se nos ofrecen desde los kits de concienciación para un uso seguro de la tecnología.



Estas son las etapas que INCIBE propone para la formación de nuestros trabajadores, a partir de sus kits de concienciación:



- **La Oficina de Seguridad del Internauta**: (https://www.osi.es/es)
  Ente que depende también de INCIBE y desde el que se proporciona información y soporte para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.
  Su objetivo es reforzar la confianza en el ámbito digital a través de la formación en materia de ciberseguridad.
  En la OSI de INCIBE trabajan para:
  - Ayudar a los usuarios a llevar a cabo un cambio positivo de comportamiento en relación con la adopción de buenos hábitos de seguridad.
  - Hacerles conscientes de su propia responsabilidad en relación con la ciberseguridad.
  - Contribuir a minimizar el número y gravedad de incidencias de seguridad experimentadas por el usuario.
- **La Agencia Española de Protección de Datos**: (https://www.aepd.es/)
  La AEPD es la autoridad encargada de velar por la privacidad y la protección de datos de los ciudadanos.
  Su objetivo es, por un lado, fomentar que los ciudadanos conozcan sus derechos y las posibilidades que la Agencia les ofrece para ejercerlos y, por otro, que los sujetos obligados tengan a su disposición un instrumento ágil que les facilite el cumplimiento de la normativa.
  Todas las empresas grandes y pequeñas, públicas y privadas deben cumplir con la normativa vigente en lo relacionado con la protección de datos de sus trabajadores, clientes, proveedores, … y más si son uno de los colectivos críticos: salud, telecomunicaciones, …

- Potenciar las formaciones orientadas a la seguridad de todos nuestros trabajadores, permite afianzar las medidas y controles implementados. Las iniciativas del propio INCIBE o esta misma de la Junta de Castilla y León son marcos idóneos para comenzar en el mundo de la ciberseguridad de la empresa y para conocer los cambios que se van produciendo de forma constante: nuevas vulnerabilidades, nuevos riesgos, nuevos tipos de ataques, nuevas formas de defendernos.

1.2. CIBERSEGURIDAD PARA PYMES.

Como hemos dejado entrever, la gestión de la seguridad es el componente clave para elaborar un plan de protección de la información que se adapte a la idiosincrasia de cada empresa.

Sin gestión no hay control, que asegure eficientemente los datos de la organización, ni evaluación de los riesgos a los que nos exponemos.

Esta gestión debe entenderse como un proceso dinámico:

1. Análisis de situación.
2. Definición de un plan de control de seguridad.
3. Implementación de medidas.
4. Evaluación de resultados.
5. Mejora continua. Implica volver a empezar desde el punto uno.

Para esto definimos una serie de documentos que permiten a cualquiera en la organización concientizarse respecto de la seguridad de la información y conocer qué está permitido y qué no lo está, en el uso diario de los recursos. Además, establecen cómo se deben llevar adelante ciertas tareas que involucran el uso de la información dentro de la organización.

Un programa de Seguridad de la Información debe contemplar medidas relacionadas con el personal, la gestión y el uso de las tecnológicas. El funcionamiento de la organización está directamente relacionado con los componentes informáticos y los sistemas de información, por lo tanto, aumenta su criticidad en relación con los resultados de la empresa.

Por tal motivo, un plan de seguridad debe comenzar en los rangos jerárquicos de la organización, y ser funcional en todos los niveles de la misma, contemplando la **Integridad, Disponibilidad y Confidencialidad** de la información.

1.2.1. Clasificación de la información.

Como indicábamos anteriormente, necesitamos clasificar la información de acuerdo a su criticidad y el impacto negativo que tendría la pérdida de la misma. Esto permite determinar los recursos (tanto económicos, humanos, como de otra índole) que necesitamos asignar a la protección de dicha información. Y cuando hablamos de seguridad no todo se resuelve con dinero.

Clasificar la información de la organización es un componente clave para la valorización de esta, tanto por los criterios de asignación de recursos, antes mencionados, como para la optimización de las medidas de control a implementar para cada tipo de información. Cuánto más valiosa sea la información para la empresa, más recursos deberemos asignar para su protección.

Previo a la clasificación de la información, es necesario identificar todo dato de valor para la organización. Para ello definimos una serie de documentos que, en conjunto, permiten a cualquier integrante de la organización concientizarse respecto de la seguridad de la información y conocer qué está permitido y qué no lo está, durante el uso diario de los recursos. Además, establecen cómo se deben llevar adelante ciertas tareas que involucran el uso de la información dentro de la organización.

NIVELES DE CLASIFICACIÓN

Aunque los criterios para catalogar la información pueden ser más complejos y extensos, en una empresa del tipo PyME podemos clasificarla en:

- **Confidencial**: para uso interno y de carácter restrictivo. Es información valiosa que hace a la empresa competitiva. Su divulgación sin autorización puede afectar seriamente a la organización. Por ejemplo: un proyecto de I+D, un código fuente, etc.
- **Privada**: Información de uso interno de la organización. Es información sensible y, por lo general, de carácter privado. Su divulgación puede afectar moderadamente a la organización. Por ejemplo: datos financieros, datos médicos, datos personales, etc.
- **Pública**: Información que no implica un impacto negativo en la organización. Por ejemplo: listado de direcciones de correo de los empleados.

1.2.2. Políticas de Seguridad.

Una Política de Seguridad es una declaración de intenciones que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se pretenderán.

Es un documento de alcance global, valido para cualquier integrante de la empresa. Es una descripción general de los fundamentos de las medidas de seguridad, qué se desea proteger y cómo se debe proteger.

Entre otras cosas, puede incluir:

- Objetivos y alcance.
- Clasificación de la información.
- Operaciones permitidas y denegadas con la información.
- Acuerdos y contratos.

1.2.3. Normas y estándares.

Los estándares son normas que impactan en la interacción de los usuarios con los recursos de la empresa y la información que manejan. Pueden ser internos o externos.

Entre los estándares internos más habituales están:

- El uso del equipamiento informático por parte de los empleados.
- Software permitido (y prohibido) en el puesto de trabajo.
- Acceso o no a redes sociales particulares y otros servicios web con contenidos ilegales o ale
- Políticas de contraseñas y cifrado de información, sobre todo cuando hablamos de dispositivos móviles (smartphones, tablets o portátiles) que salen de la organización, con información sensible de la misma.

Los estándares externos suelen ser reglamentaciones o legislaciones que debe cumplir la empresa, las cuales pueden ser:

- De obligado cumplimiento al verse afectada la empresa por la legislación vigente del país o
- Necesarias para poder trabajar con socios que nos obligan a adoptar ciertos procedimientos de trabajo en nuestra relación con ellos: normas ISO, sello de ciberseguridad, …

1.2.4. Procedimientos.

Estos son acciones documentadas que describen con precisión las tareas a realizar para cumplir con un objetivo. Permiten homogeneizar las tareas que involucren la utilización de información o recursos informáticos de la empresa, consiguiendo minimizar los riesgos que afecten a la seguridad de la misma.

Algunos ejemplos de los procedimientos que pueden utilizarse en una PyME son:

- Configuración de las cuentas de correo.
- Configuración de VPNs (Redes Privadas Virtuales) para acceder a los sistemas informáticos desde el exterior de una forma segura.
- Configuración de las copias de seguridad de la información y procedimientos de restauración.

2. USO SEGURO DE MEDIOS DIGITALES Y NUEVAS TECNOLOGÍAS EN LA EMPRESA.

La transformación digital que estamos viviendo obliga a replantear el uso que hacemos de nuestros puestos de trabajo, del entorno laboral en el que desempeñamos nuestro trabajo, del espacio y la cultura del propio trabajo, y de la gestión que hacemos del uso, correcto o incorrecto, de la tecnología por parte de nuestros trabajadores.

La tecnología juega un papel esencial, que nos aporta ventajas competitivas si la utilizamos correctamente pero que puede ocasionarnos perjuicios importantes si no la utilizamos como debemos o si no implementamos unas medidas de seguridad razonables para protegerla.

Resulta fundamental cómo las nuevas maneras de trabajar están dibujando un nuevo escenario en la cultura de trabajo y la gestión de los recursos. El espacio de trabajo se ha redefinido permitiendo la movilidad de nuestros trabajadores de una forma como antes no se había producido. Sin embargo, este es uno de los principales problemas que nos encontramos cuando intentamos asegurar una infraestructura informática. Como se dice ahora, **el perímetro se ha perdido**, lo que quiere decir que ya no sirven las herramientas y protocolos de seguridad que se implementaban hace unos años cuando la información no era accesible desde el exterior de la empresa.

Como vamos dejando entrever a lo largo de este curso, **la seguridad de la información se ocupa de la protección de la información y de los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada con independencia de su formato.**

Además, para protegerla podremos aplicar medidas de seguridad tanto físicas (videovigilancia, biometría, …) como lógicas (contraseñas, cifrado, …).

Debemos plantearnos ¿qué ocurriría si esa información cae en manos de terceros?

- ¿Podría perder ventaja competitiva? (información de mi negocio)
- ¿Podrían cometer un delito con esa información? (fraude, robo…)
- ¿Estaría desvelando datos privados de los clientes o violando derechos de los consumidores? En estos casos podríamos ser sancionados. Y no nos va a servir como excusa el “no lo sabía”. Debemos ser conscientes de que el desconocimiento de una ley no te exime de tener que cumplirla.

¿Y si perdemos o se destruye esa información, como nos afectaría?

- ¿Es información crítica y necesaria para el desarrollo de nuestro negocio?
- ¿El coste de recuperarla o de volver a generarla sería muy alto?
- ¿Podría darse una hipotética situación en la que no pudiese recuperar la información?

La empresa debe comenzar a implementar medidas y controles para el resguardo de la información y hay que tener en cuenta que el lugar donde debemos comenzar a implementar esos controles técnicos es en la **infraestructura de la organización**.

Denominamos infraestructura de red a todo componente informático disponible para la realización de nuestro trabajo. No solo nos referimos a los ordenadores de los usuarios; sino también a los routers, los switches, el cableado de red o las redes wifi, las impresoras, los dispositivos móviles, los servidores, etc.

Seguridad por capas

Como los riesgos a los que estamos expuestos son diversos, debemos seguir un modelo de seguridad por capas, que consiste en organizar las medidas de seguridad en diferentes niveles, garantizando que, si resulta comprometido un nivel, el atacante deberá traspasar otra capa de seguridad para vulnerar los sistemas.

Comunicaciones y Networking

Uno de los principales problemas que tienen las pymes hace referencia al router que le facilita su proveedor de comunicaciones para disponer de servicio de acceso a internet.

El 100% de esos dispositivos se ponen en marcha con la configuración por defecto de usuario administrador del dispositivo y contraseña, y muy pocos cambian esa configuración posteriormente.

Esto permite, de una forma muy sencilla, acceder desde el exterior al dispositivo para poder cambiar la configuración del mismo. Por ejemplo, un atacante podría cambiar los servidores dns a los que el router hace las consultas cuando navegamos por internet, redirigiendo el tráfico hacia servidores ilegítimos. De esta forma, un atacante puede tener acceso al tráfico de nuestras comunicaciones externas, conociendo dónde navegamos e identificando nuestros usuarios y contraseñas de acceso.

BYOD

Bring Your Own Device es una tendencia cada vez más generalizada en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

Sin un control básico de este tipo de dispositivos, tenemos un agujero de seguridad muy importante en nuestra organización. Un atacante podría localizar a uno de nuestros trabajadores, infectarle su equipo informático (si trabaja desde casa, por ejemplo), sus dispositivos móviles (si se conecta desde el exterior para realizar su trabajo), o sus dispositivos de almacenamiento USB (llevando y trayendo información sensible para la empresa), llegando a comprometer nuestra infraestructura cuando nuestro trabajador utilice su dispositivo.

Si nuestras empresas utilizan, todavía, pocos mecanismos de seguridad, nuestros trabajadores, a título personal, suelen usar menos todavía.

Esquema Cliente–Servidor

Uno de los errores más frecuentes, particularmente en las PYMEs, es la descentralización de la información. Entre las desventajas de tener la información distribuida en muchos equipos de la red (y particularmente en puestos de trabajo) se encuentran:

- **Problemas de disponibilidad**. Algunos usuarios de la red pueden necesitar información y no saber dónde encontrarla o cómo ubicar a quien sabe dónde está almacenada.
- **Confidencialidad**. Alguna información, no controlada, podría ser accedida por personas no autorizadas para tal fin.
- **Dificultad para hacer backup**. Es extremadamente complejo mantener un backup completo de la información disponible en todos los puestos de trabajo. Puede darse el caso de que información valiosa no tenga copias de respaldo.

Políticas de almacenamiento

La existencia de un servidor de archivos no significa que cualquier tipo de archivos deben ser almacenados allí por cualquier tipo de personas. Es por ello que es necesario definir las políticas de almacenamiento para el servidor de archivos.

En definitiva, hay que dejar muy claro, e implementar las medidas para conseguirlo, a que información puede acceder cada usuario y a cuál no.

Redundancia

Cuando todos los datos están almacenados en un único equipo, normalmente un servidor de ficheros, la criticidad de dicho servidor aumenta. Siendo imprescindible:

- Contar con un sistema de backup de la misma.
- Utilizar sistemas de redundancia que permitan la continuidad del negocio en el caso que el disco duro donde se almacena la información tenga algún fallo mecánico.

AMENAZAS ACTUALES

Desde la aparición de los virus informáticos, en la década de los 80, los códigos maliciosos han evolucionado encontrando nuevas características y métodos de propagación para afectar a los usuarios.

Por un lado, es importante poder clasificarlos, para conocer la diversidad de amenazas existentes, sus características, sus metodologías, sus índices de infección, etc.

La clasificación es importante para comprender lo que representa la amenaza del malware en la actualidad. Sin embargo, debemos recordar que todos estos tipos de malware poseen un factor

común: hacernos daño. Por lo tanto, la protección de amenazas debe abarcar todas las clases de códigos maliciosos, ya que cualquiera de ellos es un riesgo para nuestros intereses.

MALWARE

Malware es el acrónimo, en inglés, de las palabras "**mal** icious" y "soft **ware** " (en español, programa malicioso). Se puede considerar como malware todo programa diseñado con algún fin dañino.

Malware es el término principal que se utiliza para hablar de todas las amenazas informáticas. Dentro de esta categoría ya tenemos diferentes clasificaciones bastante más específicas de para las amenazas, como la de los troyanos, los gusanos, los virus informáticos, el adware, el spyware o ransomware entre otras. También es muy frecuente la existencia de malware que combina diferentes características de cada amenaza.

El Malware ya es considerado el mayor problema de seguridad de lo que llevamos de S.XXI, con un crecimiento exponencial.

El top 10 en el año 2017 de familias de malware fueron **WannaCry, Upatre, Cerber, Emotet, Locky, Petya, Ramnit, Fareit, PolyRansom y Terdot/Zloader.**

VIRUS

Los virus informáticos requieren de un anfitrión donde alojarse. Este puede variar, siendo un archivo (tanto ejecutable como no), el sector de arranque o incluso la memoria de la computadora. Su origen data de los comienzos de los años 80, siendo en aquel entonces el único código malicioso existente (no existía el concepto de malware).

Es más, al principio, el malware era un tipo de virus mientras que ahora se considera a los virus un tipo de malware.

GUSANO

Un gusano es un programa informático creado para producir algún daño en el sistema del usuario y que posee dos características: actúa de forma transparente al usuario y tiene la capacidad de reproducirse a sí mismo.

Esa reproducción es fundamental para que un ataque resulte exitoso, ya que nos resultará mucho más complicado erradicar la infección de la casi totalidad de nuestros equipos, que si sólo se infectara uno.

TROYANO

Los Troyanos tienen algunas semejanzas con los virus informáticos, pero su funcionamiento no es exactamente el mismo. Mientras que un virus suele ser destructivo, un troyano trata de pasar inadvertido mientras accede a nuestros dispositivos con la intención de ejecutar acciones ocultas con las que abrir una puerta trasera para que otros programas maliciosos puedan acceder a él.

Sin embargo, uno de los puntos en común entre varios tipos de malware es que los troyanos también llegarán a ti disfrazados de archivos legítimos. Lo harán con ejecutables que aparentemente no harán nada malo al ser utilizados, pero que enseguida empezarán a trabajar a tus espaldas sin que te des cuenta.

ADWARE

El Adware (acrónimo de **ad** vertisement –anuncio publicitario- y soft **ware**) es un programa malicioso, que se instala en el sistema sin que el usuario sepa realmente su objetivo principal, que es descargar y/o mostrar anuncios publicitarios en la pantalla de la víctima.

Existiendo hoy en día, la realidad es que su presencia es mucho más baja que la que había en el pasado. La gran diferencia respecto al adware de hace unos años, es que hoy día busca otros fines, como puede ser el **minado de criptomonedas**.

Normalmente la infección actual por adware viene vinculada a la visita de ciertas paginas web, a la instalación de algunas extensiones en nuestros navegadores, sin comprobar que son legítimas, o a la descarga de apps en nuestros dispositivos, incluso desde las Store oficiales de los Microsoft, Apple o Google.

SPYWARE

El spyware, también conocido como programa espía, es una aplicación cuyo fin es recolectar información del usuario, sin su consentimiento.

Inicialmente el spyware nació como un conjunto de aplicaciones incluidas junto al software gratuito, con el objetivo de generar estadísticas sobre la actividad del usuario en su computadora, a fin de poder determinar su perfil de navegación e intereses.

ROGUE

El rogue es un código malicioso que simula ser un programa de seguridad, con el fin de lograr que el usuario pague por una aplicación dañina o inexistente. Es una de las técnicas que mayor crecimiento ha experimentado en los años 2008 y 2009. Emplea como herramienta la generación de miedo en el usuario, indicando falsas alertas sobre infecciones y/o problemas que pudiera tener el sistema; logrando de esta forma que el usuario desee instalar el falso producto.

RANSOMWARE

El ransomware es una de las amenazas informáticas más similares a un ataque sin medios tecnológicos: el secuestro, directamente relacionado con las criptodivisas, monedas virtuales a las que no podemos seguir el rastro en la red, y que son utilizadas para cobrar el rescate solicitado.

El ransomware es un código malicioso que, por lo general, cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La

víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este comunique.

Algunas de las técnicas para el secuestro son las siguientes:

- Cifrado de archivos del disco.
- Bloqueo de acceso a ciertos archivos (frecuentemente documentos de ofimática).
- Bloqueo total de acceso al sistema (previo al login, o bloqueo de pantalla una vez que el usuario accedió al sistema).

INCIBE tiene un servicio que ayuda a las empresas que han sufrido ataques de tipo ransomware.

OTRAS AMENAZAS

- **SPAM**

  Se denomina spam al correo electrónico no solicitado enviado masivamente por parte de un tercero. En español también es identificado como correo no deseado o correo basura.

- **HOAX**

  Un hoax es un correo electrónico distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores que algo falso es real. A diferencia de otras amenazas, como el phishing o el scam; los hoax no poseen fines de lucro, al menos como intención principal.

- **SCAM**

  Scam es el nombre utilizado para las estafas a través de medios tecnológicos. A partir de la definición de estafa, se describe scam como el "delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro, utilizando como medio la tecnología".

- **PHISHING**

  El phishing consiste en el robo de información personal y/o financiera del usuario, mediante la falsificación de comunicaciones provenientes de un ente confiable.

  De esta forma, el usuario cree ingresar los datos en un sitio que conoce cuando, en realidad, estos son enviados directamente al atacante. En su forma clásica, el ataque comienza con el envío de un correo electrónico simulando la identidad de una organización de confianza, como por ejemplo un banco o una reconocida empresa.

  Las características de un correo de phishing son las siguientes:

  - Uso de nombres de organizaciones con presencia pública.
  - El correo electrónico del remitente simula ser de la compañía en cuestión.

- El cuerpo del correo presenta el logotipo de la compañía u organización que firma el mensaje.
- El mensaje insta al usuario a reingresar algún tipo de información que, en realidad, el supuesto remitente ya posee.
- El mensaje incluye un enlace.

El enlace es un componente importante del ataque. Cuando el usuario hace clic sobre él es redireccionado a un sitio web, donde podrá ingresar la información solicitada en el correo electrónico. A pesar de que el texto sobre el que usuario haga clic mencione una dirección web válida, el mismo puede apuntar a cualquier otro sitio web; en este caso, al sitio falsificado. De esta forma el correo induce al usuario a hacer clics sobre los vínculos del mensaje.

3. AMENAZAS, VULNERABILIDADES Y RIESGOS.

Saber identificar conceptos como los de amenaza, vulnerabilidad y riesgo y cómo puede afectar un incidente a tu empresa, te permitirá saber si tu empresa está en peligro.

Vulnerabilidad y amenaza son términos que se confunden a menudo, por lo que es necesario definirlos correctamente desde el principio, al igual que ocurre con el riego:

Una **vulnerabilidad** (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma. Necesitaremos por tanto encontrarlas y corregirlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

Por otro lado, una **amenaza** es toda acción que se aprovecha de una vulnerabilidad para atacar a un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado).

Desde el punto de vista de una organización, las amenazas pueden ser tanto internas como externas.

Por tanto, las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas. El problema es que, en el mundo real, si existe una vulnerabilidad, siempre existirá alguien que intentará sacar provecho de su existencia.

Una vez que tenemos clara la diferencia entre amenaza y vulnerabilidad, debemos saber que el **riesgo** es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un ciberdelincuente, un ataque de denegación de servicio, un virus… El riesgo depende entonces de la probabilidad de que la amenaza se

materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo.

Asociados al riesgo, hablamos de **análisis de riesgos** cuando nos referimos al uso sistemático de la información para identificar las fuentes y calcular el riesgo, y de g**estión del riesgo**, cuando nos referimos a las actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Este análisis/gestión nos llevará a obtener una imagen rigurosa de los riesgos a los que se encuentra expuesta nuestra empresa. Estas fases son las siguientes:

En función de la relevancia de los riegos podremos optar por:

- **Evitar el riesgo** eliminando su causa, por ejemplo, cuando sea viable optar por no implementar una actividad o proceso que pudiera implicar un riesgo.
- **Adoptar medidas que mitiguen el impacto o la probabilidad del riesgo** a través de la implementación y monitorización de controles.
- **Compartir o transferir el riesgo** con terceros a través de seguros, contratos etc.
- **Aceptar la existencia del riesgo** y monitorizarlo.

El tratamiento del riesgo supone unos claros beneficios para la «salud» de la ciberseguridad de nuestra empresa. De esta manera mantendremos protegida nuestra información confidencial y la de nuestros clientes frente a la mayoría de amenazas y vulnerabilidades detectadas (o no), evitando robos y fugas de información.

Algunas de las fuentes de amenazas más comunes en el ámbito de sistemas de información son:

- **Malware o código malicioso**: comentados en el apartado anterior.
- **Ingeniería social**: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.

- **APT o Amenazas Persistentes Avanzadas** (Advanced Persistent Threats): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.
- **Botnets**: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.
- **Redes sociales**: el uso no controlado de este tipo de redes puede poner en riesgo la reputación de la empresa.
- **Servicios en la nube**: una empresa que contrate este tipo de servicios tiene que tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios. Se ha de asegurar de contratarlos con empresas cuya seguridad este demostrada, y firmar SLA o ANS (Acuerdos de Nivel de Servicio) en los que quede definida la seguridad que necesita la empresa.
- Algunos incidentes pueden implicar **problemas legales** que pueden suponer sanciones económicas y daños a la reputación e imagen de la empresa. Por eso, es importante conocer los riesgos, medirlos y evaluarlos para evitar en la medida de lo posible los incidentes, implantando las medidas de seguridad adecuadas.

4. BUENAS PRÁCTICAS.

4.1. SEGURIDAD FÍSICA.

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y detección, destinados a proteger físicamente cualquier recurso del sistema.

Este hecho cobra vital importancia en aquellos equipos (portátiles, tablets o smartphones) que salen de la empresa para desarrollar su trabajo.

Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque es preferible pecar de exceso de celo: mínima exposición/mínimo privilegio.

Por otro lado, tenemos que interiorizar el concepto de **resiliencia**, que hace referencia a la capacidad de una empresa de adaptarse y continuar con sus funciones y su trabajo en situaciones de riesgo. Cómo actuar y cómo **gestionar la situación de forma eficiente** afectando el mínimo posible al desempeño general de la empresa. O, en otras palabras, una empresa es resiliente si tiene implementadas las medidas correctas para reestablecer cualquier servicio en el menor tiempo posible cuando se ha producido un incidente de seguridad/ciberseguridad.

A continuación, destacaremos algunos de los problemas de seguridad física con los que nos podemos enfrentar y las medidas que podemos tomar para minimizar su impacto.

Debemos realizar una monitorización continua de nuestra infraestructura para conocer, en tiempo real, la situación de riesgo en la que nos encontramos y, además, debemos fomentar una cultura de la seguridad empresarial educando a todos los miembros de la empresa en buenas prácticas para evitar riesgos y saber cómo actuar en caso de incidente.

PROTECCIÓN DEL HARDWARE

Problemas a los que nos enfrentamos:

- Acceso físico.
- Desastres naturales.
- Alteraciones del entorno.
- Acceso al propio dispositivo informático.

ACCESO FÍSICO

Si alguien que desee atacar un sistema tiene acceso físico al mismo todo el resto de medidas de seguridad implantadas se convierten en inútiles. Esto no sería un gran problema si protegiésemos lo que habitualmente no protegemos correctamente: ni los espacios en los que ubicamos nuestros equipos informáticos, ni el acceso a los mismos.

En cuanto a proteger el espacio en el que tenemos nuestros equipos informáticos, deberemos implantar mecanismos de **prevención** (control de acceso a los recursos) y de **detección** (si un mecanismo de prevención falla o no existe debemos al menos detectar los accesos no autorizados cuanto antes).

Para la **prevención** hay muchas posibilidades que permiten registrar quien accede a qué recursos y en qué momento:

- Sistemas Biométricos: analizadores de retina, lectores de huellas digitales, …
- Tarjetas inteligentes.
- CCTVs.
- ...

En muchos casos es suficiente con controlar el acceso a las salas y cerrar siempre con llave los despachos o salas donde hay equipos informáticos y no tener cableadas las tomas de red que estén accesibles.

DESASTRES NATURALES

Además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los *desastres naturales* pueden tener muy graves consecuencias, sobre todo si no los contemplamos en nuestra política de seguridad y su implantación.

Algunos desastres naturales a tener en cuenta:

- Terremotos y vibraciones.
- Tormentas eléctricas.
- Inundaciones y humedad.
- Incendios y humos.

Los terremotos son el desastre natural menos probable en un país como España, por lo que no se harán grandes inversiones en prevenirlos, sin embargo, si fuéramos a abrir una delegación en Japón, la situación cambiaría drásticamente. Además, hay varias cosas que se pueden hacer sin un desembolso elevado y que son útiles para prevenir problemas causados por pequeñas vibraciones:

- No situar equipos en sitios altos para evitar caídas.
- No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos.
- Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen.
- Utilizar fijaciones para elementos críticos.

- Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.

Otro desastre natural importante son las tormentas con aparato eléctrico, especialmente frecuentes en verano, que generan subidas súbitas de tensión muy superiores a las que pueda generar un problema en la red eléctrica. A parte de la protección mediante el uso de bases de enchufe con toma de tierra, podemos usar SAIs que mantengan encendidos los equipos críticos en caso de pérdida de corriente. En estos casos es recomendable desconectar los equipos cuando haya tormenta.

En entornos normales es recomendable que haya un cierto grado de humedad, ya que en si el ambiente es extremadamente seco hay mucha electricidad estática. No obstante, tampoco interesa tener un nivel de humedad demasiado elevado, ya que puede producirse condensación en los circuitos integrados que den origen a un cortocircuito. En general no es necesario emplear ningún tipo de aparato para controlar la humedad, pero no está de más disponer de alarmas que nos avisen cuando haya niveles anómalos.

Otro tema distinto son las inundaciones, ya que casi cualquier medio (servidores, routers o switches, sistemas de almacenamiento y backup de datos, ...) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos. Contra ellas podemos instalar sistemas de detección que apaguen los sistemas si se detecta agua y corten la corriente en cuanto estén apagados. Hay que indicar que los equipos deben estar por encima del sistema de detección de agua, sino cuando se intente parar ya estará mojado.

Por último, mencionaremos el fuego y los humos, que en general provendrán del incendio de equipos por sobrecarga eléctrica. Contra ellos emplearemos sistemas de extinción, actualmente son más o menos inocuos y nos evitarán males mayores. Además del fuego, también el humo es perjudicial para los equipos (incluso el del tabaco), al ser un abrasivo que ataca a todos los componentes, por lo que es recomendable mantenerlo lo más alejado posible de los equipos.

ALTERACIONES DEL ENTORNO

En nuestro entorno de trabajo hay factores que pueden sufrir variaciones que afecten a nuestros sistemas que tendremos que conocer e intentar controlar.

Deberemos contemplar problemas que pueden afectar el régimen de funcionamiento habitual de las máquinas como la alimentación eléctrica, el ruido eléctrico producido por los equipos o los cambios bruscos de temperatura.

Electricidad

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo ...

Como hemos indicado anteriormente, para corregir los problemas con las subidas de tensión podremos instalar tomas de tierra o filtros reguladores de tensión y SAIs (Sistemas de Alimentación Innnterrumpida).

Por último, indicar que además de los problemas del sistema eléctrico también debemos preocuparnos de la corriente estática, que puede dañar los equipos. Para evitar problemas se pueden emplear espráis antiestáticos o ionizadores y tener cuidado de no tocar componentes metálicos, evitar que el ambiente esté excesivamente seco, etc.

Ruido eléctrico

El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

Para prevenir los problemas que puede causar el ruido eléctrico debemos no situar el *hardware* cerca de los elementos que pueden causar el ruido. En caso de que fuese necesario hacerlo siempre podemos instalar filtros o apantallar las cajas de los equipos.

Temperaturas extremas

No hace falta ser un genio para comprender que las temperaturas extremas, ya sea un calor excesivo o un frio intenso, perjudican gravemente a todos los equipos. En general es recomendable que los equipos operen entre 10 y 32 grados Celsius. Para controlar la temperatura emplearemos aparatos de aire acondicionado.

Protección de los datos

Además de proteger el hardware, nuestra política de seguridad debe incluir medidas de protección de los datos, ya que en realidad la mayoría de ataques tienen como objetivo la obtención de información, no la destrucción del medio físico que la contiene.

Soportes no electrónicos

Otro elemento importante en la protección de la información son los elementos no electrónicos que se emplean para transmitirla, fundamentalmente el papel. Es importante que en las organizaciones que se maneje información confidencial se controlen los sistemas que permiten exportarla tanto en formato electrónico como en no electrónico (impresoras, plotters, faxes, ...).

Cualquier dispositivo por el que pueda salir información de nuestro sistema ha de estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos.

Además de esto es recomendable disponer de trituradoras de papel para destruir todos los papeles o documentos que se quieran destruir, ya que evitaremos que un posible atacante pueda obtener información rebuscando en nuestra basura.

ACCESO AL PROPIO DISPOSITIVO INFORMÁTICO

Debemos acostumbrarnos a utilizar contraseña de BIOS en todos los equipos y dispositivos informáticos, más aún en aquellos que sacamos de la empresa.

Además, usaremos contraseñas seguras de acceso al sistema operativo, que obligaremos a cambiar con la periodicidad que establezcamos.

Por último, debemos cifrar los discos duros de los dispositivos, para que la información sea ilegible en caso de caer en manos de quien no debiera. En tablets y smartphones, podemos configurar el borrado remoto del dispositivo en el caso de que nos le hayan sustraído o le hayamos perdido.

4.2. COPIAS DE SEGURIDAD.

Ya hemos comentado que lo que realmente tiene valor en la empresa es la información y necesitamos disponer de un procedimiento de copia de seguridad y otro, paralelo, de restauración de la copia.

El sistema de copia de seguridad que implementaremos dependerá de la información que debamos proteger y dónde esté almacenada. No utilizarán los mismos procedimientos las empresas si virtualizan sus sistemas o si no lo hacen, o si disponen, o no, de sistemas gestores de bases de datos, o si utilizan sistemas operativos Windows o los usan Linux, …

Por eso, antes de nada, hay que hacer una auditoría que nos permita elegir la solución que mejor se adapte a nuestras necesidades.

Por otro lado, debemos combinar las copias de seguridad que almacenamos “en local”, en nuestras oficinas, con copias de seguridad en la nube. Actualmente los costes de estos servicios son asumibles y permiten tener, fuera de la empresa, una copia de seguridad que nos permita continuar con nuestra actividad en caso de una catástrofe.

Aunque sean situaciones extremas, recuerda lo ocurrido en los atentados del 11 de septiembre en Estados Unidos, o el incendio del edificio Windsor en Madrid. Las empresas que tenían oficinas en esos edificios, y no tenían copias de seguridad online, no pudieron continuar con su actividad al no poder recuperar la información, aunque tenían copias de seguridad en sus oficinas.

Para entornos con servidores Windows Server, podemos utilizar la herramienta de copia de seguridad que viene integrada en el propio sistema.

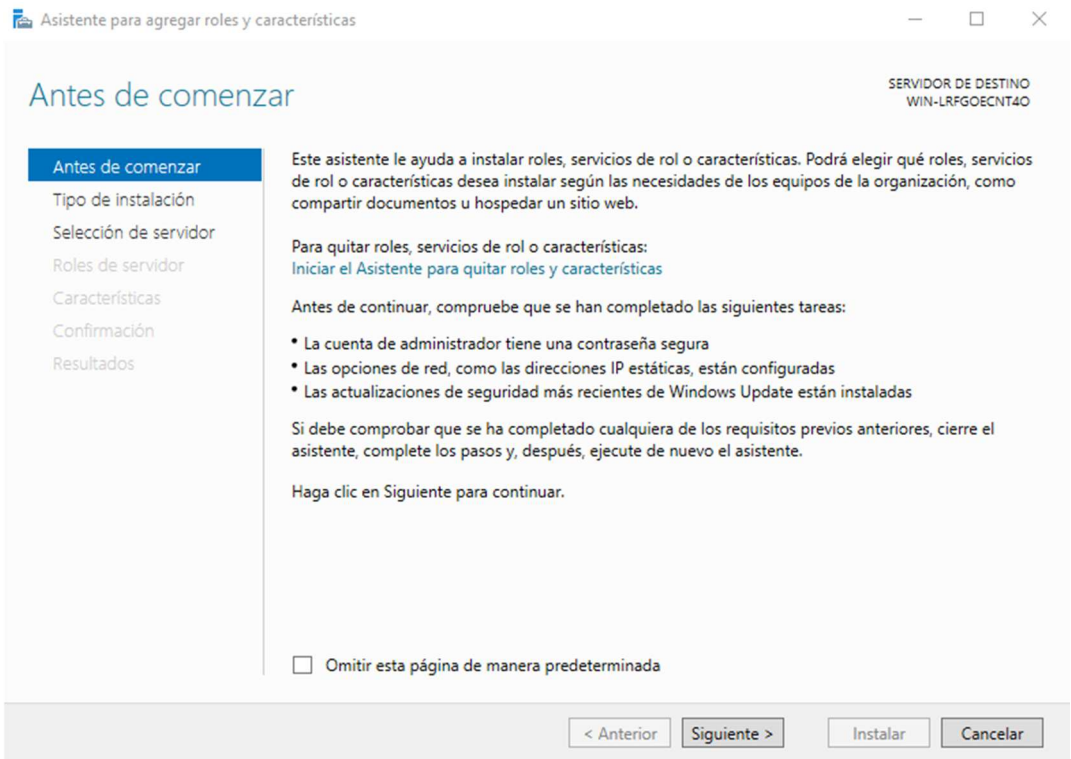
Desde ella podemos:

- Hacer backup completo del Servidor.

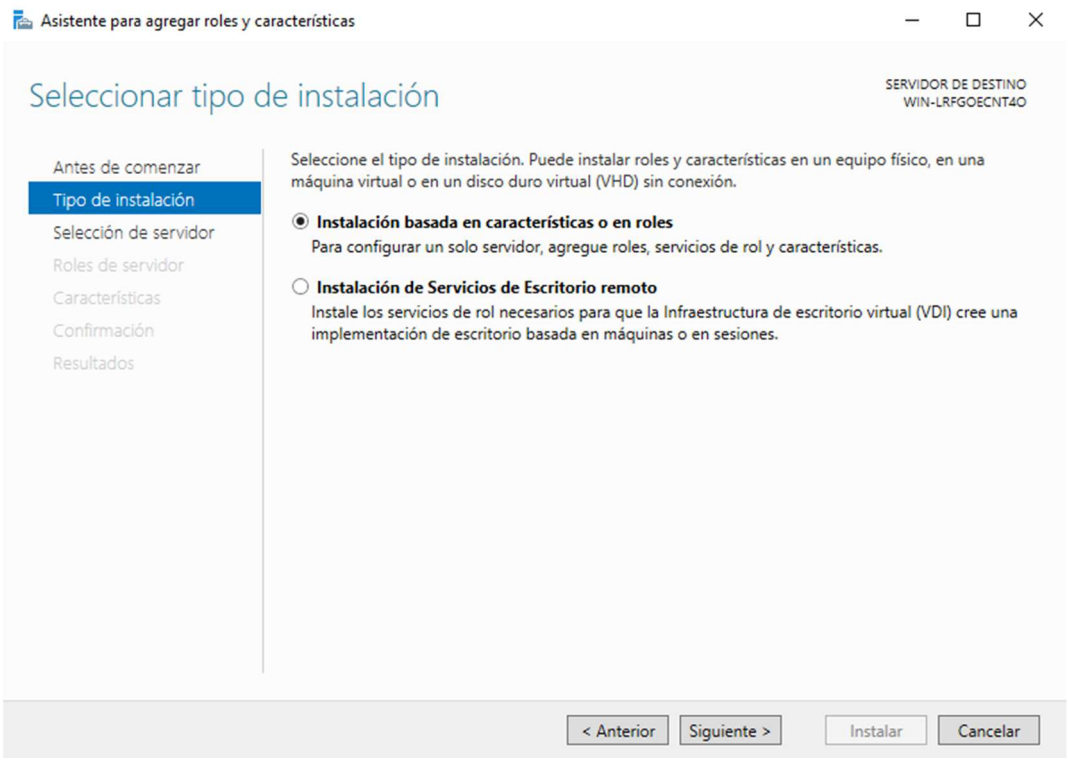
- Hacer backup de las unidades de almacenamiento de datos, ubicadas en el propio servidor o en unidades de red.
- Programar la periodicidad de las copias de seguridad: diarias, semanales, …, en aquellas horas del día en el que no se desarrolle actividad.
- Combinar esa periodicidad con la realización de backups completos o incrementales.

Podemos acceder la herramienta desde Herramientas en el Administrador del Servidor.

A continuación, seguiremos el asistente de agregación de roles y características:

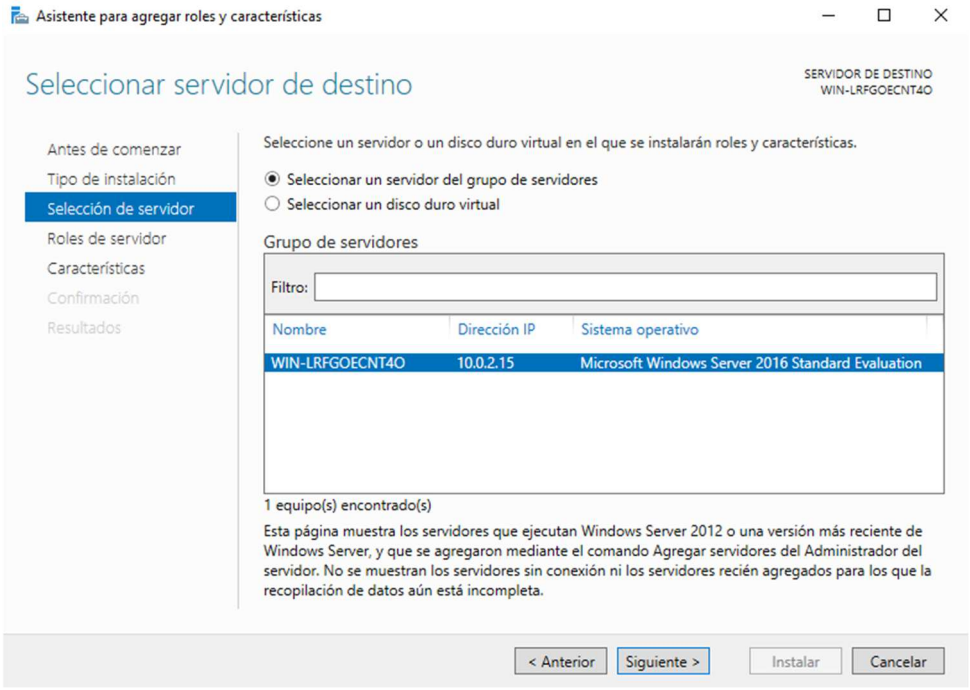


En este momento nos muestra una descripción de lo que podemos hacer a través del asistente. Elegimos Siguiente y, a continuación, elegimos la opción que viene por defecto:

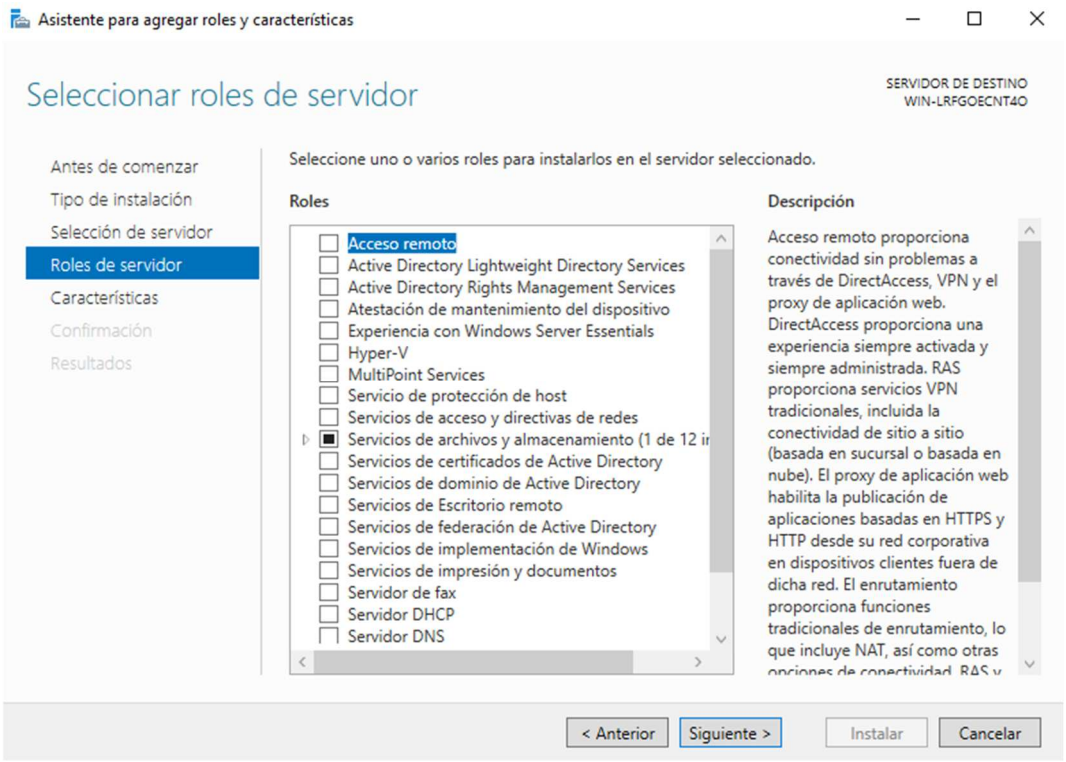


Con esta opción le estamos diciendo que queremos hacer una instalación para acceder localmente al servicio en el servidor en el que lo instalemos.

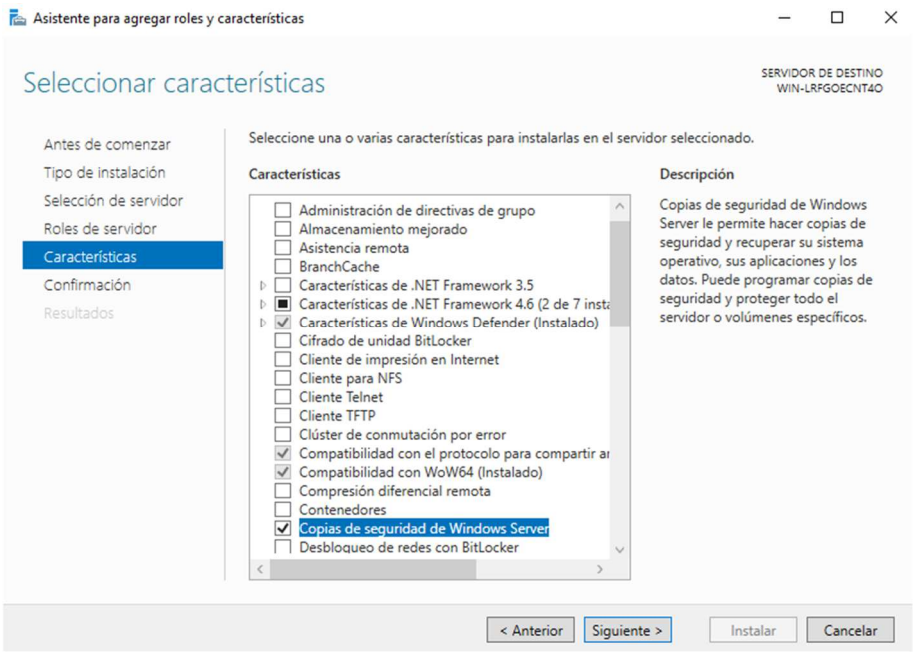
A continuación, le indicamos en que servidor queremos instalarlo. Si sólo tenemos uno, como en el ejemplo, simplemente hacemos click en Siiguiente:



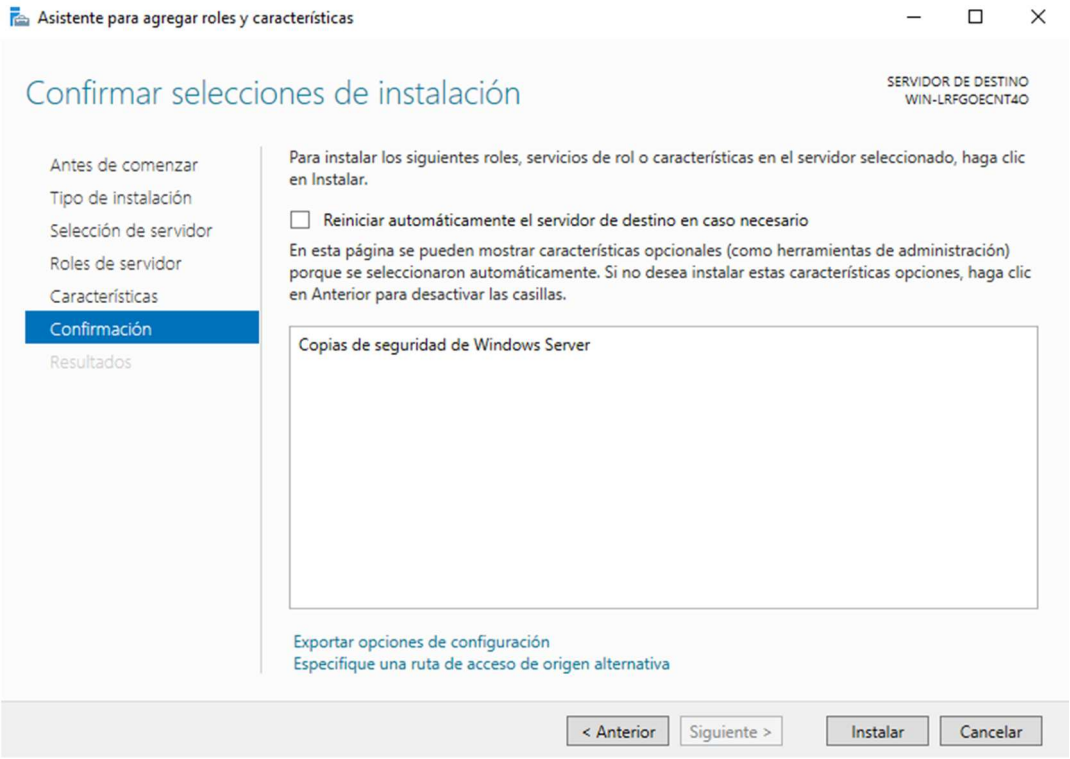
Una vez en la sección de Roles de Servidor, haremos click en Siguiente sin seleccionar ninguna opción porque la herramienta no es un rol, es una característica:



Una vez en la Sección de Características elegimos Copias de seguridad de Windows Server y hacemos click en Siguiente:

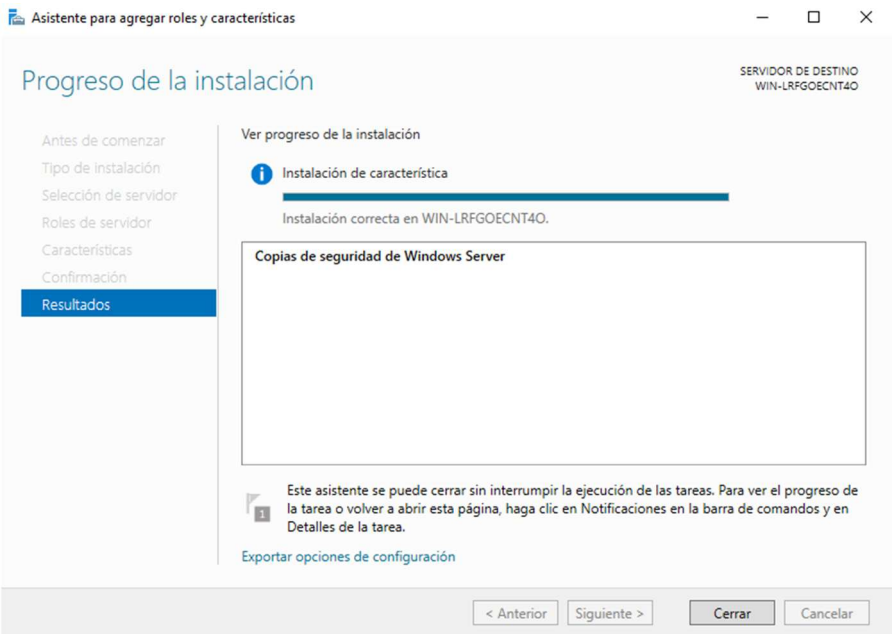


En este momento podemos indicar si permitimos o no reiniciar automáticamente el servidor en caso de que la instalación lo requiriera y hacemos click en Instalar:

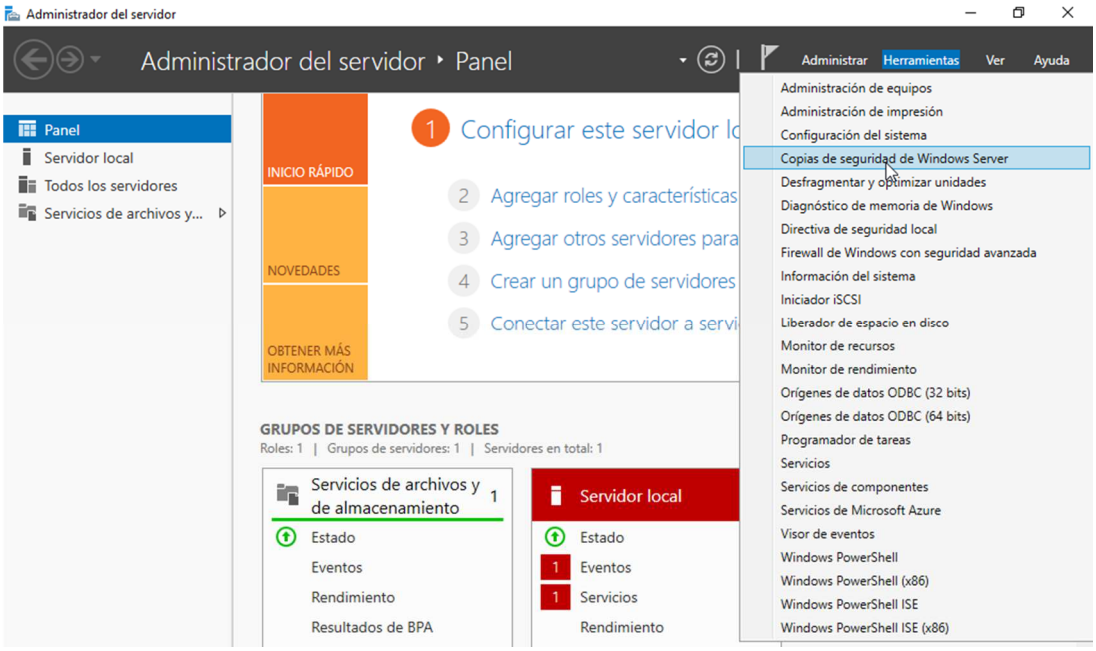


El proceso de instalación es rápido e incluso podemos dejarle en segundo plano haciendo click en cerrar.

Una vez que finaliza nos mostrará una ventana indicando que el proceso se ha realizado correctamente:



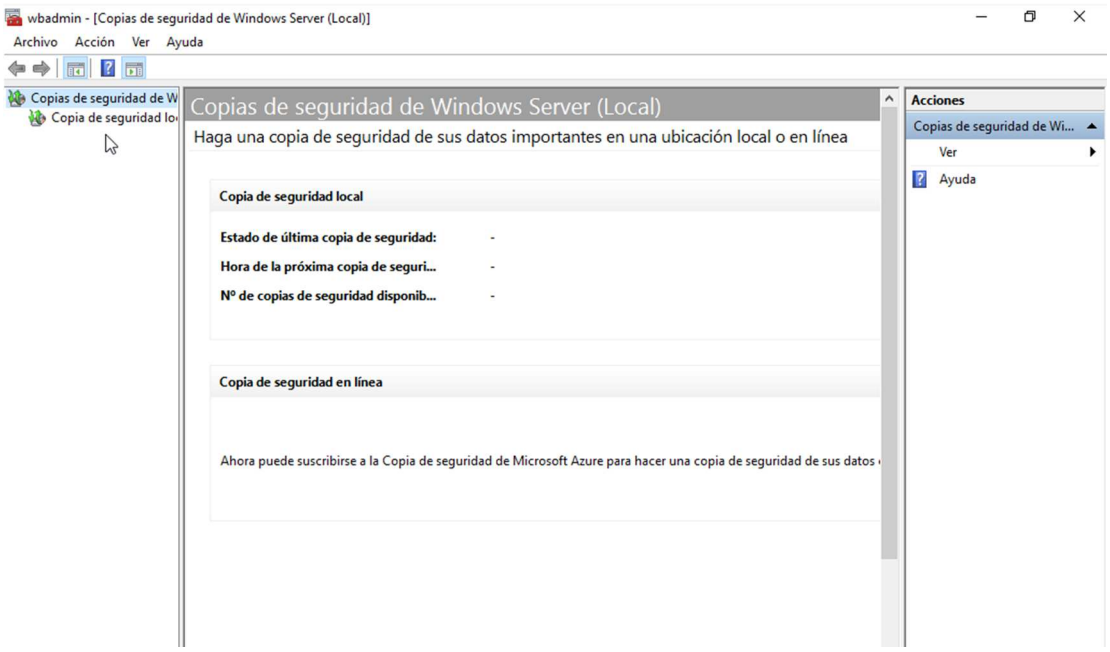
Una vez instalada la herramienta de backup podemos acceder a ella desde las Herramientas del Administrador del Servidor:



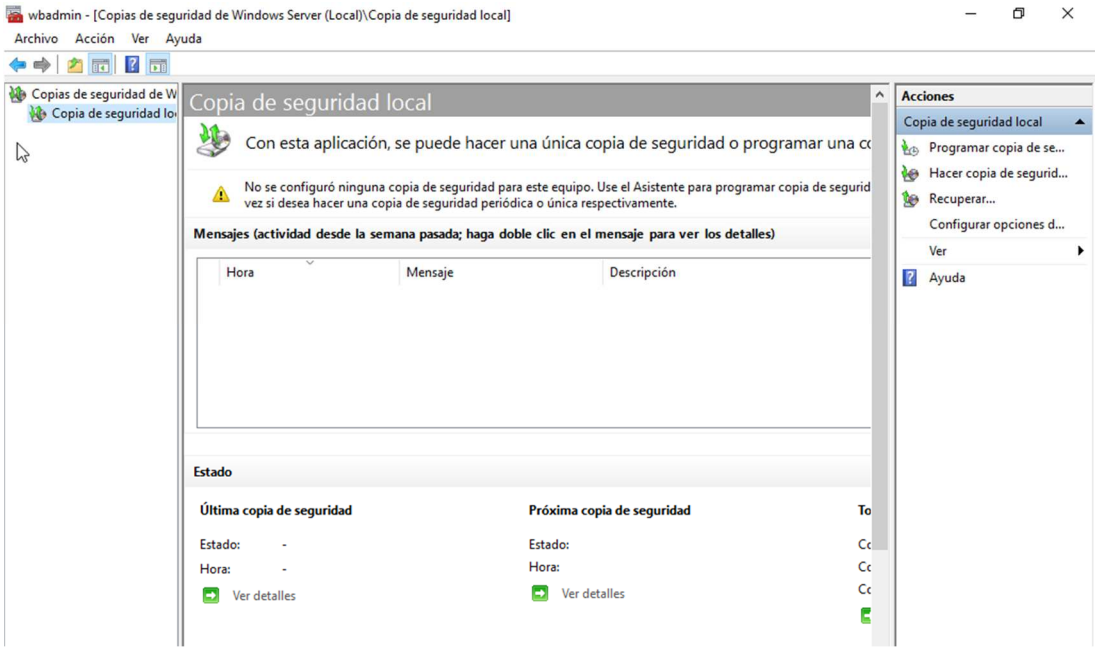
Como puedes observar, hasta el momento, el proceso de instalación no es complejo y no exige grandes conocimientos informáticos para realizarlo.

A continuación, veremos cómo podemos usarla y observaremos que su uso también es sencillo y tampoco exige grandes conocimientos.

Una vez que hacemos click sobre la Herramienta de Seguridad de Windows Server, nos encontramos con la siguiente interfaz:



Hacemos click sobre Copia de Seguridad Local y buscará copias de seguridad ya realizadas para mostrarnos. En este primer momento nos dirá que todavía no se ha configurado ninguna copia:



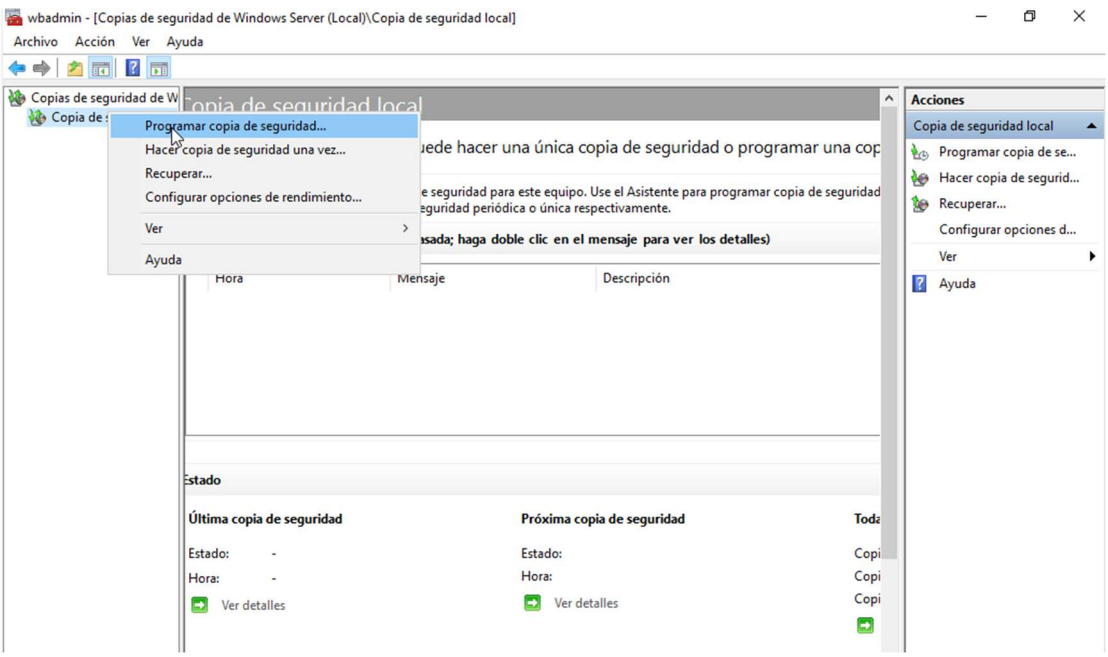
Estamos listos para programar nuestra primera copia de seguridad, pero, antes de nada, debo hacer un análisis de qué información necesito hace copia de seguridad y con qué periodicidad. Por otro lado, también podremos hacer una copia de seguridad completa de nuestro servidor, lo que nos permitirá recuperarlo muy rápidamente en caso de que se haya visto comprometido.

Ten en cuenta de que nuestro principal objetivo es ser resilientes, es decir, debemos ser capaces de volver a levantar un servicio caído en el menor tiempo posibles, para que el impacto de la parada sea mínimo.

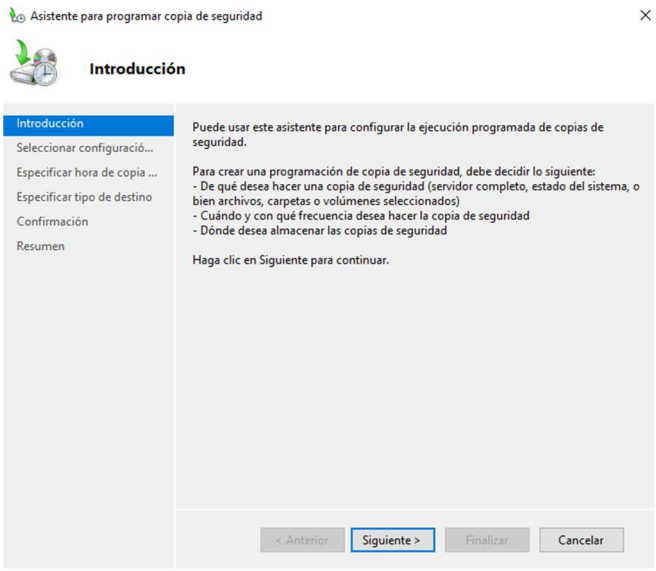
En este momento debemos indicar si queremos realizar una copia de seguridad en este momento o si queremos programar un proceso que se repita periódicamente. Independientemente de que en un momento concreto me interese hacer una copia de seguridad puntual debemos programar copias periódicas.

Estas copias deben realizarse fuera del horario de actividad de la empresa ya que suelen causar un alto impacto en el rendimiento del servidor y, además, no se podrían guardar aquellos archivos que se estuvieran utilizando en el momento de hacer la copia.

Vamos a ver cómo podemos programar una copia de seguridad. Hacemos click con el botón derecho del ratón sobre Copia de Seguridad Local:

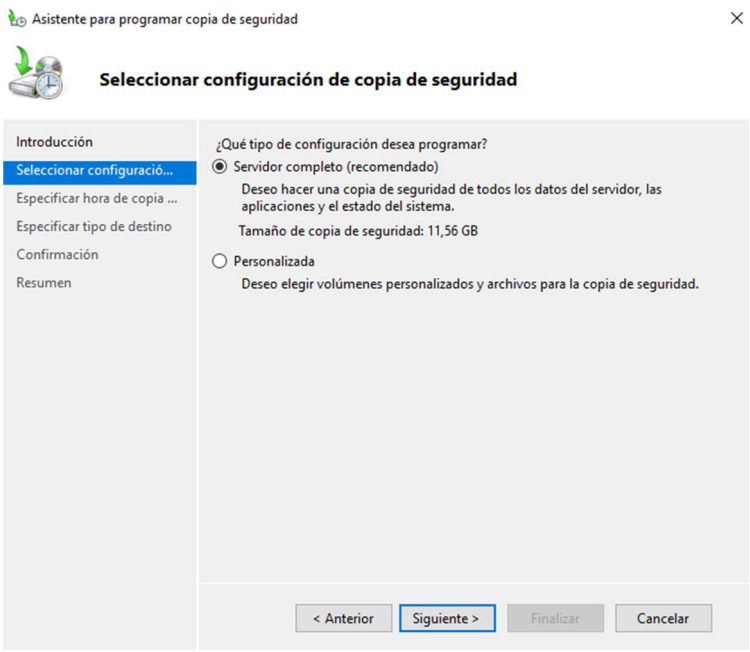


A continuación, nos aparece el asistente que debemos seguir:



En esta pantalla nos indica que debemos tener en cuenta antes de continuar.

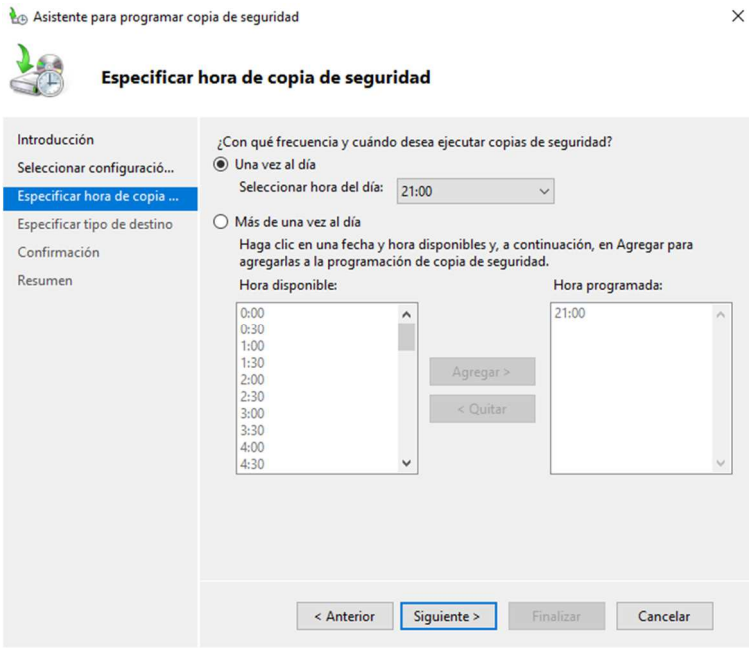
Hacemos click en Siguiente y le indicamos si queremos hacer una copia completa del servidor o seleccionamos lo que queremos incluir en la copia:



Debemos tener dos tipos de copias de seguridad. Una periódica completa, a diario, que como hemos indicado nos permitirá restaurar el sistema en poco tiempo cuando tengamos un incidente grave, y debemos realizar otra copia sólo de la información. Está última deberá realizarse a través de dos copias de seguridad independientes: una semanal completa y otra diaria incremental, lo que

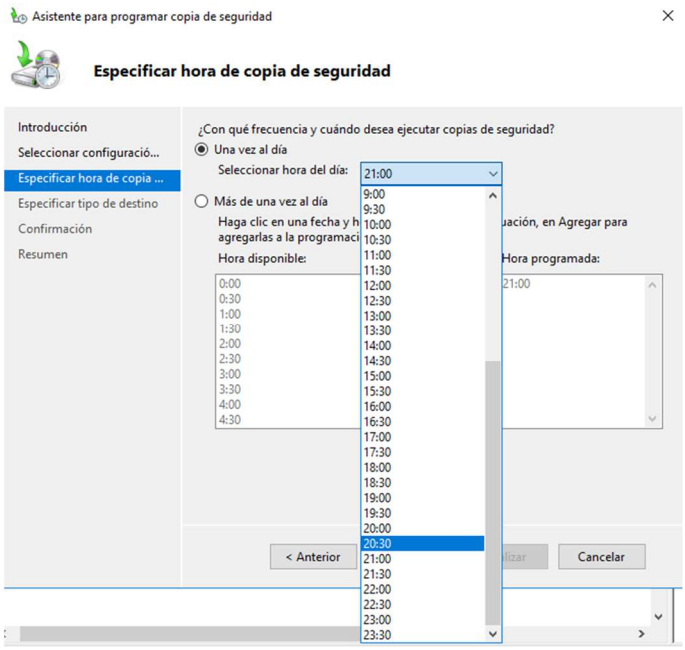
permitirá que se realice de una forma más rápida al guardar sólo la información modificada desde la última copia de seguridad.

En este momento vamos a ver como hacemos una copia completa del servidor haciendo click en Siguiente. Nos aparecerá la siguiente pantalla del asistente:

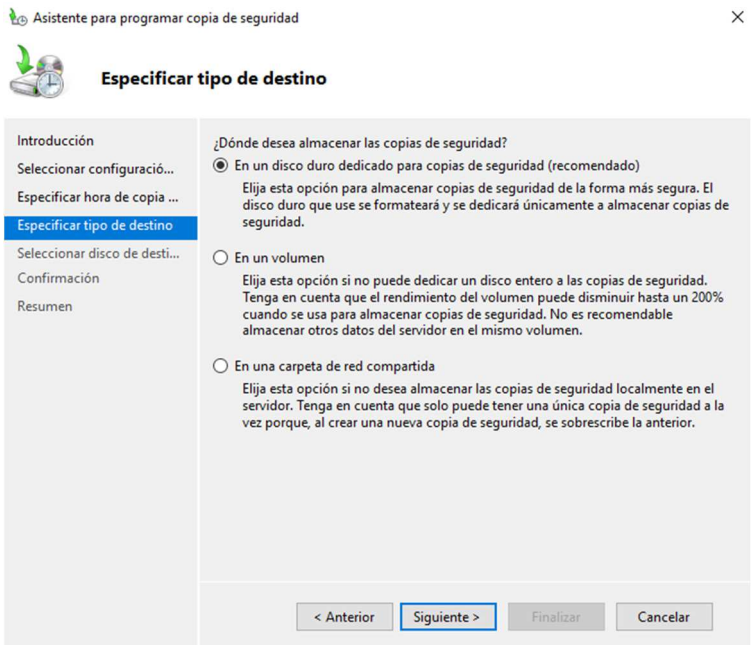


Lo primero que nos pregunta es que cuantas veces queremos hacer la copia al día. En principio esto depende de cada empresa, de la información que es capaz de asumir que puede perder y del tiempo que tarde en realizar la copia de seguridad ya que, como hemos indicado antes, debemos realizar las copias de seguridad fuera del horario de actividad.

Suponiendo que sólo quisiéramos hacer una copia al día, indicaríamos la hora:



A continuación, hay que indicar dónde queremos almacenar la copia de seguridad:



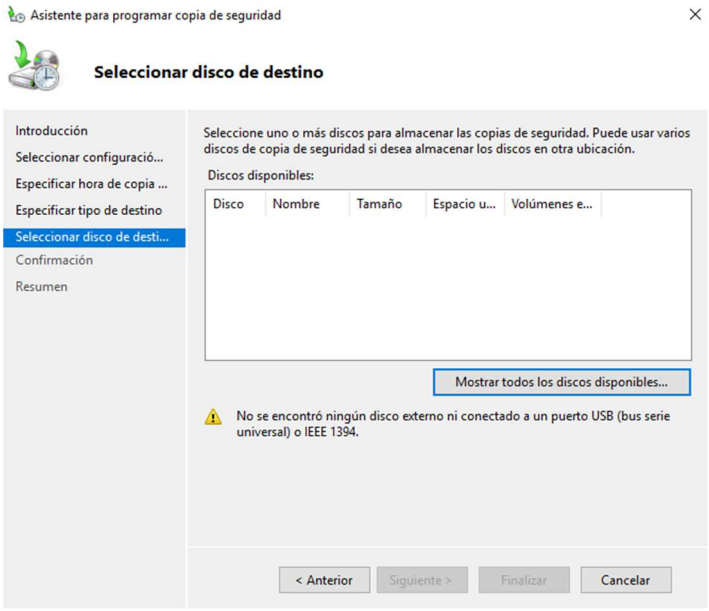
La mejor opción es la primera, dedicando un disco exclusivamente para guardar nuestras copias. Además, este disco no debe estar en el mismo servidor ya que si el problema fuera físico podrían perderse la información y su copia de seguridad. Por otro lado, y aunque se puedan usar discos usb, es recomendable usar dispositivos NAS que ofrezcan redundancia a fallos, es decir, que disponga

de varios discos para que, si uno falla, la información no se pierda porque está distribuida también entre el resto de los discos.

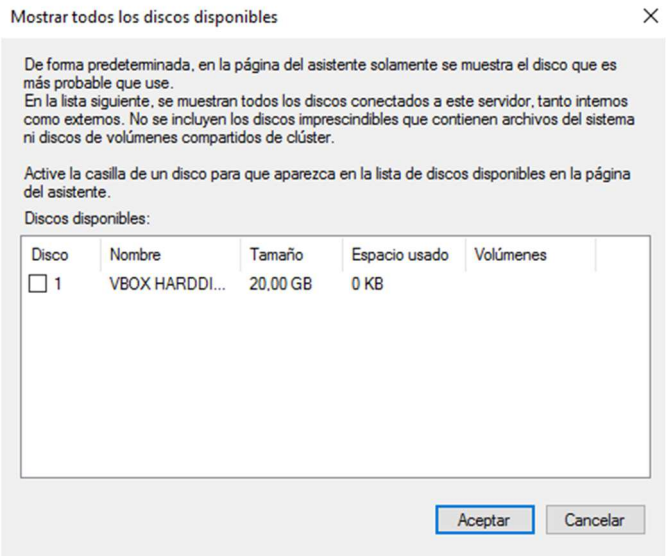
Hoy día tienen precios asequibles y permiten el acceso y el backup incluso en remoto.

La opción menos recomendable es la de utilizar una unidad de red ya que hay Ransomwares que, aparte de cifrar los discos duros locales de los servidores, también cifran todas las unidades de red, por lo que nos quedaríamos sin información y sin copias de seguridad.

En este momento seleccionamos el disco en el que vamos a guardar las copias de seguridad:

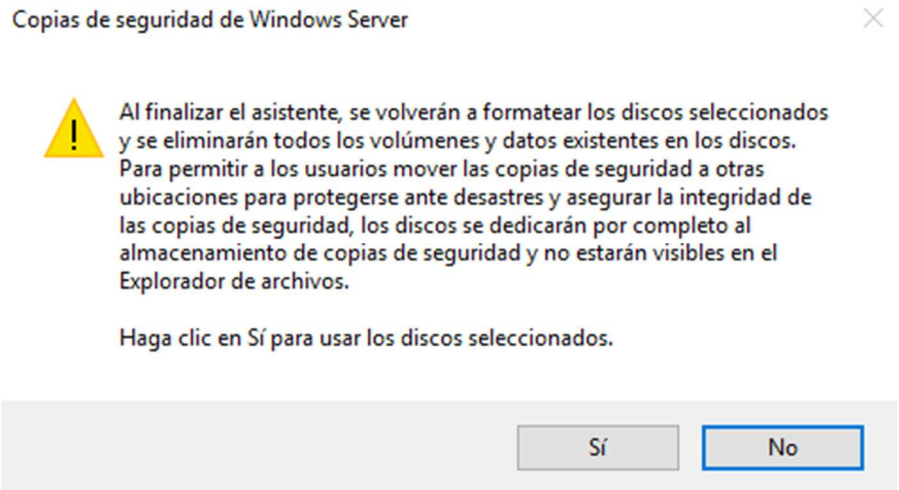


Accedemos a Mostrar todos los discos disponibles y, en nuestro caso nos muestra un disco virtual que hemos creado para la demostración, el cual seleccionamos:

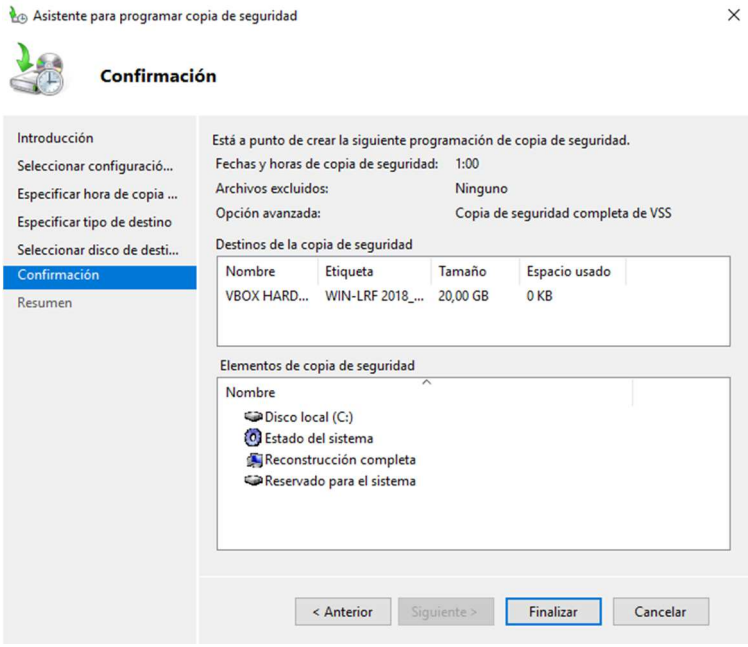


Una vez seleccionado volveremos a la ventana anterior. En el caso de que tuviéramos más de un disco para almacenar copias de seguridad, aparecerían mostrados en esa lista, teniendo que elegir el que nos interese en cada ocasión.

Hacemos click en Siguiente y continuamos. Ahora nos indicará que este disco se usará exclusivamente para almacenar copias y que deberá darle formato, por lo que no debemos usar discos con información guardada porque la eliminará.



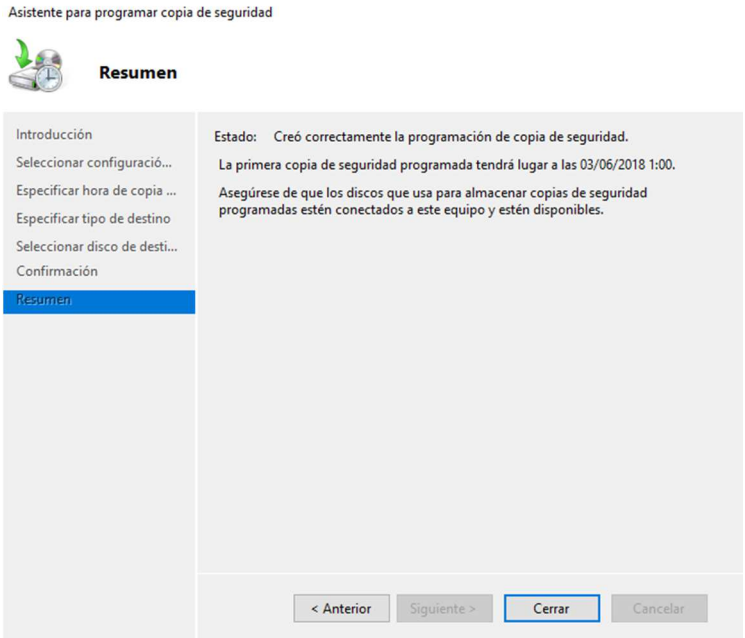
Le indicamos que queremos continuar haciendo click en Sí:



En este momento debemos revisar si está correcta la selección de opciones que hemos elegido y en el caso de que sea correcto, hacemos click en Finalizar:

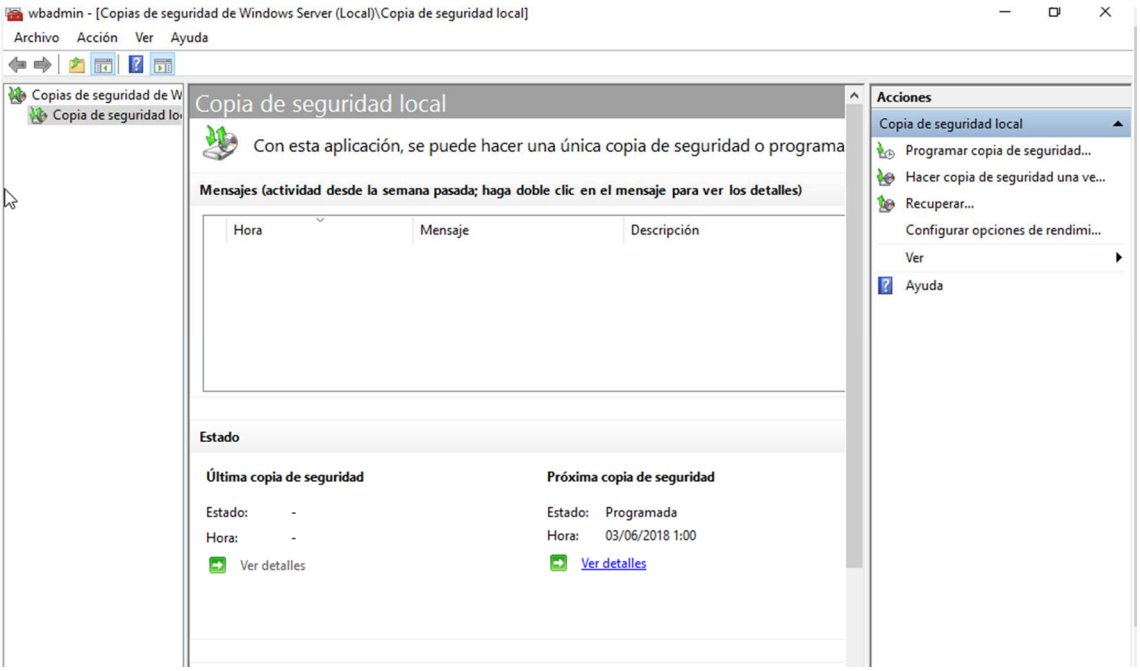
En este proceso, formatea el disco y genera la programación que hemos indicado en el proceso de configuración de la copia.

Si todo finaliza correctamente, nos mostrará un mensaje de que el proceso de configuración de la copia de seguridad se realizó correctamente como se ve en la siguiente imagen:

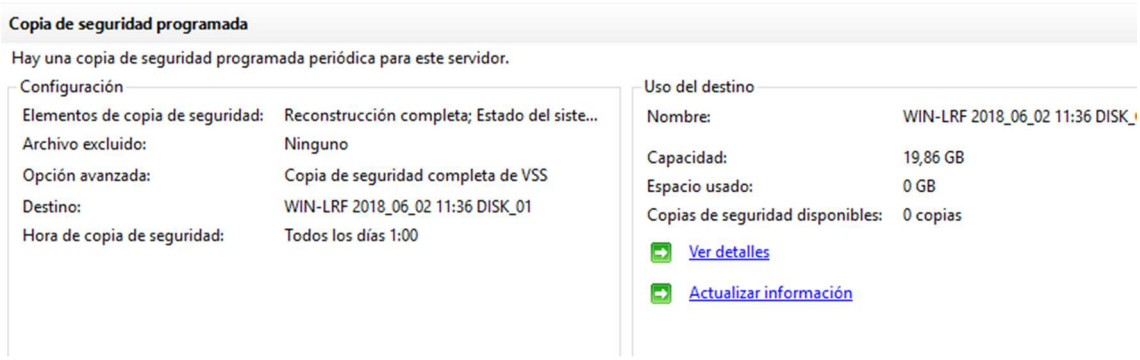


La primera copia no se realizará hasta que llegue la hora a la que hemos programado que se realice.

Una vez finalizamos el asistente, aparecerá en la pantalla principal la copia que hemos programado:



Y si bajamos un poco con la barra de desplazamiento vertical veremos la información relativa a la siguiente copia de seguridad que se va a realizar en base a la programación que hemos realizado:

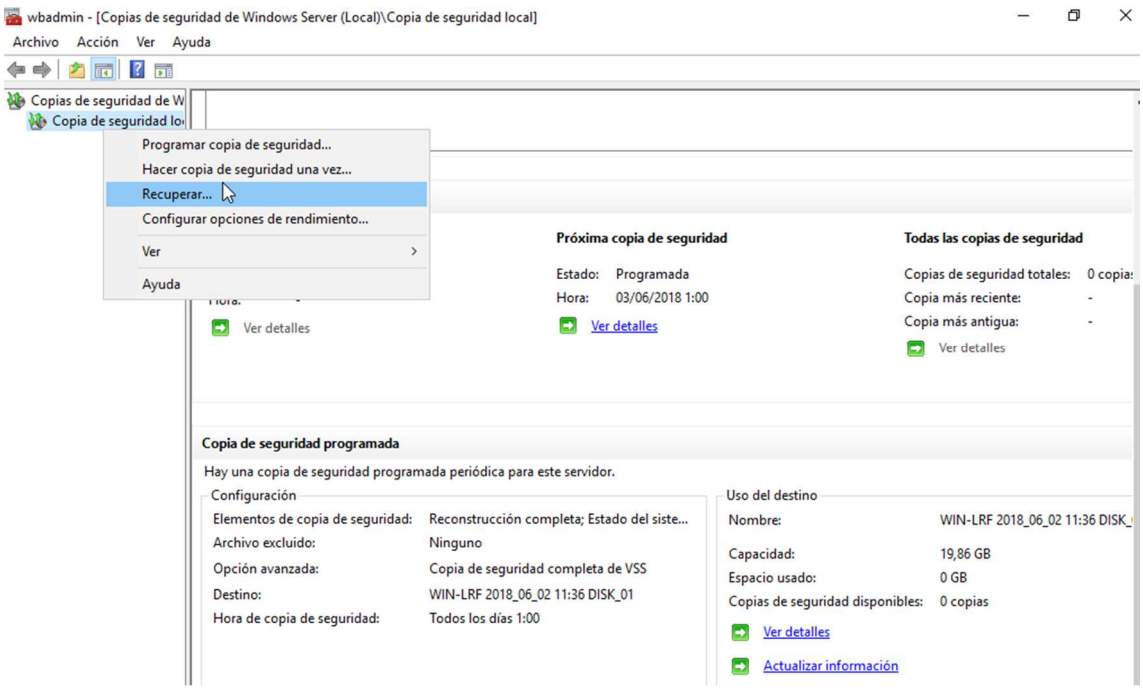


También me indica, a la derecha, en qué disco se va a almacenar, cuál es la capacidad completa del disco, cuanto espacio ha utilizado hasta el momento, cuantas copias de seguridad ha almacenado e incluso nos permite ver más detalles sobre las copias.

Por otro lado, debemos comprobar frecuentemente si las copias de seguridad se están realizando correctamente y cada cierto tiempo realizar un proceso de restauración de las copias para tener la

certeza absoluta de que el día que tengamos un incidente serio no vamos a tener ningún problema para recuperar la última copia de seguridad que tengamos.

Este proceso podemos realizarlo desde Recuperar:



Es un proceso inverso al anterior en el que siguiendo el asistente que aparece indicaremos:

- Si la copia está almacenada en este servidor o en otra ubicación.
- Una vez seleccionada la ubicación indicaremos de que fecha queremos recuperar la copia, ya que estas aparecen ordenadas en el tiempo, tal y como se van realizando.
- A continuación, indicaremos que tipo de recuperación queremos y que elementos queremos recuperar. En el caso de que fuera el servidor completo tendrían que estar seleccionadas todas las opciones.
- Indicaríamos dónde queremos recuperar la información y confirmaríamos la acción después de revisar el resumen de acciones que le hemos indicado que realice.

Cómo has podido ver, el proceso de creación de copias de seguridad y su posterior recuperación se basan en seguir unos asistentes, bastante bien explicados, en los que, sin grandes conocimientos podremos realizar o programar la realización de nuestras copias de seguridad.

Insisto en lo indicado anteriormente. Debemos comprobar con frecuencia que las copias se realizan correctamente y que podemos recuperarlas. De esta forma evitaremos sorpresa desagradables el día que por obligación tengamos que realizar un proceso de recuperación de nuestra información.

4.3. CONTRASEÑAS SEGURAS.

Las contraseñas son el sistema más utilizado para autentificarnos cuando necesitamos acceder a algún tipo de servicio. Sin embargo, son uno de los principales dolores de cabeza de los profesionales que se encargan de la seguridad de las organizaciones.

¿Por qué? Sobre todo, por la incapacidad que tenemos de recordar más de tres o cuatro contraseñas complejas. Habitualmente, todos utilizamos esas tres o cuatro contraseñas para acceder a todo: desde redes sociales a servicios bancarios, pasando por los inicios de sesión de nuestros ordenadores.

El problema es que cuando una de nuestras contraseñas ha sido comprometida se ven comprometidos todos los servicios en los que usamos esa contraseña.

Siguiendo unas sencillas pautas, minimizamos enormemente el problema, sin embargo, muy pocas personas las aplican:

- Utilizar una contraseña para cada servicio.
- Utilizar contraseñas complejas, que combinen números, letras (mayúsculas y minúsculas) y caracteres especiales.
- Utilizar contraseñas que no estén vinculadas con datos personales: fechas de nacimiento, nombres de familiares o mascotas, …
- Cambiar con cierta periodicidad esas contraseñas.
- Utilizar dobles factores de autenticación: pines enviados al móvil, tarjetas de coordenadas, … Estos sistemas si solemos usarlos en nuestros accesos a banca online, pero no extendemos su uso a otros servicios.
- Utilizar algún servicio de gestión de contraseñas centralizado.

Por otro lado, el problema de las contraseñas aumenta en el espacio de trabajo. O directamente no las usamos, o todos los compañeros conocen las contraseñas de todos, o las tenemos apuntadas en pósT-it pegadas en los monitores, …

Si tenemos en cuenta que lo único que necesita un ciberdelincuente para acceder a nuestros sistemas son un nombre de usuario y una contraseña, debemos entender el problema que surge si no gestionamos correctamente las contraseñas en nuestra empresa.

Es más que evidente que el uso de contraseñas no es, ni de lejos, el mejor sistema para asegurar el acceso a los servicios que necesitamos utilizar (más por nuestra culpa que porque el sistema no sea robusto si se usa como se debe) y se está trabajando en encontrar sistemas que sustituyan la necesidad de utilizarlas, como por ejemplo sistemas biométricos, el uso del smatphone, …

Algunos de estos sistemas, ya disponibles, llaman la atención por su originalidad:

- **El uso de nuestro corazón para identificarnos:**

El sistema utiliza un **Radar Doppler** de baja intensidad para medir los latidos de corazón de una persona y luego lo monitorea continuamente para otorgarle acceso a su computadora o a un área restringida.

Podéis ampliar la información desde este enlace: https://goo.gl/m9ZM1L

- **PalmSecure ID Login de Fujitsu:**

  La nueva solución de Fujitsu **que lee las venas de la palma de la mano y su oxígeno**, es una nueva solución de autenticación biométrica, que ayuda a las organizaciones a proteger sus redes contra el acceso no autorizado, al mismo tiempo que reduce el riesgo de ataques de ciberdelincuentes y suplantadores de identidad.

  Podéis ampliar la información desde este enlace: https://goo.gl/WysgTp

En definitiva, debemos tener presente que una buena gestión de las contraseñas reduce la posibilidad de padecer un incidente de seguridad, explicando a los trabajadores la importancia de usar contraseñas seguras y los riesgos que estamos asumiendo al utilizar las contraseñas como lo está haciendo la mayoría hasta la fecha.

4.4. DISPOSITIVOS MÓVILES.

Los dispositivos móviles, portátiles que usamos desde hace años, y tablets y smartphones, que usamos desde hace poco para facilitarnos el trabajo en movilidad, son otra de las fuentes de problemas ya que habitualmente no les integramos en nuestras políticas de seguridad.

Gracias a ellos se ha roto el perímetro, que dicen los especialistas en seguridad. Esto hace referencia a que hace unos años con proteger el perímetro de nuestra infraestructura era suficiente. Este perímetro venía definido por nuestros routers por los que nuestros equipos salen hacia el exterior. Sin embargo, hoy día casi hay más dispositivos fuera de la empresa accediendo a recursos internos que equipos informáticos dentro. Y esto plantea un problema porque debemos proteger todos esos dispositivos y las comunicaciones necesarias para que desarrollen su actividad.

¿POR QUÉ DEBEMOS PROTEGER ESTOS DISPOSITIVOS?

Fundamentalmente porque con ellos accedemos a recursos internos y en ellos almacenamos información confidencial, como por ejemplo correos electrónicos, datos de contacto de mis clientes y proveedores, documentos como presupuestos, proyectos y fotografías, credenciales de acceso (usuario|contraseña), …

Además, en muchas ocasiones, para acceder a estos servicios nos conectamos a redes inseguras, tanto en nuestros domicilios, como en hoteles, restaurantes, aeropuertos, …, sin implementar ningún sistema de acceso seguro que garantice una comunicación protegida de extremo a extremo y en la que la información se envíe cifrada.

Recuerda que, digan lo que digan los fabricantes (todo es publicidad), tan inseguros son los dispositivos basados en Android, como los que se basan en IOS de Apple o los de Microsoft, estos últimos en un porcentaje muy reducido en comparación con los otros dos.

¿CÓMO PODEMOS PROTEGER NUESTROS DISPOSITIVOS?

- Usando contraseña o patrón.
- Teniendo anotado el IMEI para anular el dispositivo en caso de robo o pérdida. Hoy día esta información suele estar disponible desde la web del proveedor de comunicaciones, cuando accedemos a nuestro espacio personal. Si no la localizamos debemos ponernos en contacto telefónicamente con la operadora.
- Utilizar dos dispositivos distintos, uno en el ámbito personal y otro en el ámbito profesional
- Cifrar el dispositivo. Esta es una opción de seguridad que permiten todos los dispositivos hoy día pero que casi nadie usa.
- Teniendo instaladas aplicaciones de control remoto del dispositivo que nos permitan:
    - Saber dónde está por geolocalización.
    - Eliminar la información.
- Realizando copias de seguridad de la información del dispositivo en la nube o en equipo s internos de la empresa.
- Instalando software antivirus.
- Evitando hacer rooting o jailbreaking de los dispositivos. Estos son procedimientos que permiten desbloquear los dispositivos para poder instalar aplicaciones no oficiales o instalar apps oficiales sin pagarlas.
- Asegurándonos de que las apps que nos descargamos son legítimas, aunque las descarguemos de las stores oficiales de Google, Apple o Microsoft.
- No utilizando apps gratuitas. Cuando algo es gratis el precio somos nosotros mismos (nuestra información).
- Actualizar los sistemas operativos de los dispositivos cuando los fabricantes ofrecen actualizaciones que, aparte de ofrecernos nuevas funcionalidades, corrigen vulnerabilidades detectadas.

¿CÓMO PODEMOS PROTEGER NUESTRAS COMUNICACIONES?

- Intentando evitar redes públicas.

- Usando herramientas VPNs, Redes Privadas Virtuales, que autentican la conexión desde el exterior (usuario|contraseña) y cifran la información que se transmite).
- Usando sistemas de escritorio remoto como Citrix, Parallels, VmWare u otros, que permiten acceder a la información y recursos de la organización, desde el exterior, evitando la necesidad de tener almacenada esa información en el dispositivo.
- Incorporar a los dispositivos móviles en las políticas de seguridad de los sistemas de servidores y gestionarlos igual que gestionamos los equipos internos, con Políticas de Grupos en Windows Server (GPOs), por ejemplo.

CONCLUSIONES

Tenemos un arma muy poderosa en nuestras manos, que nos permite ser mucho más productivos si lo usamos como debemos, pero desde el que podemos causar graves perjuicios a la empresa si lo utilizamos de una forma indebida o si lo perdemos, nos lo roban o nos lo infectan con un malware que permita monitorizar nuestras comunicaciones o que acceda al interior de nuestros sistemas cuando conectemos nuestro dispositivo a nuestros equipos informáticos para cargarlos, por ejemplo.

Entiende que estos dispositivos son como cualquier otro equipo de tu organización que debes proteger e integrar en tus políticas de seguridad. Hay que tenerlos mucho más vigilados porque, a diferencia de los otros, estos salen de tu empresa llevando información confidencial que no debe caer en manos de terceros.

Usa tus dispositivos con sentido común. En la mayoría de las ocasiones esto ya minimiza el riesgo de que nuestro dispositivo móvil origine un incidente de seguridad en nuestra empresa.

Para finalizar, debemos desarrollar periódicamente formaciones/concienciaciones entre nuestros trabajadores para que entiendan el riesgo que asumen al utilizar estos dispositivos y cómo se pueden evitar riesgos originados por un uso inadecuado.

Si vamos a permitir que nuestros trabajadores usen sus dispositivos personales (portátiles, tablets, smartphones o pinchos/discos usbs), lo que hoy día se denomina BYOD (Bring Your Own Device) implementa las medidas de seguridad oportunas.

Ten en cuenta que cuando intenten atacar a tu empresa, siempre intentarán hacerlo a través del eslabón más débil y este siempre es el trabajador. Comprometeremos al trabajador, infectaremos sus dispositivos y accederemos a los sistemas internos de la empresa a través de ellos.

4.5. PROBLEMAS DE SEGURIDAD EN NUESTRAS REDES. REDES WIFI.

En este punto vamos a hacer referencia a la seguridad de las redes wifi que nosotros gestionamos. Las consideraciones sobre cómo utilizar nuestros dispositivos móviles de forma segura en redes wifi públicas, que nosotros no controlamos ni gestionamos, ya se han indicado anteriormente.

En nuestras empresas podemos se puede dar una de las siguientes situaciones:

1. El router de acceso a Internet es, simultáneamente, nuestro punto de acceso Wifi.
2. Utilizamos un router para acceder a Internet y disponemos de APs (puntos de acceso) Wifi a los que nos conectamos con nuestros dispositivos móviles.

En el primer caso debemos tener especial cuidado ya que comprometer el router puede provocar muchos más problemas de seguridad que si los comprometidos son sólo los APs Wifi.

Sin embargo, en la mayoría de los casos, comprometer el router es muy sencillo ya que prácticamente nadie cambia las credenciales de acceso al dispositivo.

Cuando contratamos el servicio de telefonía e internet con una operadora de comunicaciones, viene un operario de la misma para hacer la instalación del router que nos da el servicio.

Este comprueba que el servicio está operativo, nos facilita la clave de acceso a la Wifi, y se marcha. Lo que no se molesta en decirnos es que todos los routers tienen un usuario administrativo con una clave de acceso por defecto que usaremos cuando queramos acceder al dispositivo para configurarlo: servicio DHCP, DNS, Firewall, o cambiar el SSID y la clave por defecto de la Wifi, entre otros aspectos.

Sabiendo cual es la marca y modelo del router y realizando una búsqueda en Google, tardamos 30 segundos en conocer cual es el nombre del usuario administrador y su clave de acceso al dispositivo.

Lo mejor de todo es que no necesitamos estar cerca. Podemos acceder a los dispositivos en remoto, a través de la dirección ip pública del router y esta podemos obtenerla utilizando buscadores como Shodan y otros.

Una vez conocemos la ip pública y el usuario y contraseña de la cuenta del administrador, podemos acceder al dispositivo y cambiar la configuración para:

- Modificar las direcciones IP de los servidores DNS para que todas las consultas de resolución de nombres pasen por nuestros DNS. Esto nos va a permitir saber a qué servicios se conectan los trabajadores.
- Esnifar (capturar) el tráfico saliente para intentar sacar usuarios y contraseñas de servicios internos.

- Modificar las tablas ARP del router. Este es un procedimiento por el que se vinculan las direcciones IP con las direcciones MAC de mis dispositivos. De esta forma conseguimos que sólo nuestros dispositivos accedan a nuestra red y, por consiguiente, a nuestros servicios.
- Cambiar los SSID de nuestras redes Wifi o cambiar las claves de acceso a las mismas provocando un ataque de denegación de servicio al impedir que los usuarios puedan acceder a la red Wifi.

SEGURIDAD EN NUESTRAS REDES WIFI

Este sistema sencillo de instalar, configurar y gestionar nos supone un ahorro de costes importante, al evitar que tengamos que instalar cableado estructurado para que nuestros usuarios se conecten a los servicios y recursos necesarios para desarrollar su actividad, ya que accedemos a ellos de forma inalámbrica.

El problema radica en que no podemos limitar la señal wifi impidiendo que alguien desde fuera de nuestra empresa se pueda conectar.

Por este motivo debemos:

- Cambiar de forma periódica la contraseña de acceso a la Wifi y asegurarnos de que la contraseña es lo suficientemente robusta como para resistir un ataque por fuerza bruta.
- No compartir la clave de la Wifi con nadie.
- Si necesitamos permitir que personas externas a la empresa accedan a nuestra wifi, configura un SSID específico para ello. Desde este:
    - Limitaremos el ancho de banda que permitimos usar.
    - No se podrá acceder a los recursos y servicios internos.
    - Filtraremos el tipo de páginas que se visitan desde ella, evitando el acceso a páginas con contenidos inapropiados, desde los que se descargan contenidos protegidos por propiedad intelectual, …

Debes tener en cuenta que nos tocará dar explicaciones si un usuario realiza algún acto delictivo utilizando nuestra infraestructura informática. Como veremos a continuación, con el nuevo Reglamento General de Protección de Datos, que viene a sustituir a la antigua Ley Orgánica de Protección de Datos, la seguridad debe ser proactiva y ya no va a servir el “no lo sabía”.

5. LEGISLACIÓN Y NORMATIVA DE SEGURIDAD. NUEVO RGPD.

Los ciberdelitos crecen tan exponencialmente como la propia tecnología. Europool ya indicaba a finales de 2016, que ya hay países en los que, porcentualmente, los ciberdelitos superan a los delitos tradicionales.

El problema ante esta situación es que la legislación, mucho más lenta que la tecnología, siempre va por detrás de estos nuevos ciberdelitos. Estamos sufriendo delitos que hace 5 años no existían y dentro de 5 años nos veremos afectados por delitos que hoy no existen.

Ante esta situación no nos queda otra que cumplir la legislación y normativa vigente en cada momento, ya que en algunas ocasiones comprometen nuestros sistemas para cometer dichos delitos.

Cumplir con la ley nos permitirá respetar los derechos de aquellos vinculados a nuestra actividad: clientes, proveedores, trabajadores, … y nos permitirá evitar sanciones que, como veremos, con el nuevo RGPD que desde el 25 de mayo de este año nos afecta, pueden llegar a los 20 millones de € o el 4% de nuestra facturación, en casos muy graves.

Hasta el 25 de mayo de 2018, en España existían las siguientes leyes vinculadas a la seguridad de la información:

- Ley Orgánica 15/99 de Protección de Datos, también conocida como LOPD.
- Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Ley 32/2003 General de Telecomunicaciones.
- Ley 59/2003 de Firma Electrónica.
- Real Decreto Legislativo 1/1996 de Propiedad Intelectual.
- Ley 17/2001 de Propiedad Industrial.
- Ley 11/2007 de Acceso Electrónico a los Servicios Públicos.
- Algunos sectores tienen legislación propia, como, por ejemplo, el agrario.
- Otros como la Banca dispone de normativa internacional.

Estas leyes buscaban proteger a personas físicas y jurídicas de aquellos delitos que se comenten contra ellos:

- Contra su intimidad, a través de la venta de datos. Recuerda que no hay nada gratis y cuando accedes a servicios gratuitos estas pagando con tu privacidad y la información que generas en internet.
- Referidos a la distribución de contenidos ilegales a través de la red, como por ejemplo los referidos a la distribución de pornografía infantil.
- Delitos económicos: robo, extorsión, suplantación de entidades bancarias, …
- Delitos contra la propiedad intelectual. En España todavía “pirateamos” más del 50% del software que utilizamos en nuestras empresas y nuestras casas.

Algo que podemos observar a simple vista, cuando nos fijamos en las leyes y los delitos que anteriormente describíamos es que:

- Las leyes son antiguas. Entre 10 y 20 años, en el mundo de la tecnología, son demasiado tiempo. Si recuerdas como era, tecnológicamente, tu empresa hace 15 años te darás cuenta de que no tiene nada que ver con la realidad actual.

Los delitos actuales (ciberdelitos), manteniendo los descritos, han aumentado en número y tipos de ellos. Los ciberdelitos se dividen en dos:

- Los que se aprovechan de la tecnología como medio para producirse:
  - Contra el honor, como los crímenes de odio a través de redes sociales.
  - Ciberbulling.
  - Amenazas y coacciones.
  - Delitos sexuales, como la pornografía infantil.
- Los que atacan a nuestras infraestructuras:
  - Acceso e interceptación ilícita.
  - Interferencia en los datos y los sistemas.
  - Falsificación informática.
  - Fraude informático.
  - Contra la protección industrial intelectual.
  - Contra la salud pública.

Si quieres obtener más información visita la página web del Observatorio Español de Delitos Cibernéticos (http://oedi.es):

- Desde la sección de ciberdelitos puedes aprender más sobre cada uno de ellos.
- Desde la sección de estadísticas puedes observar el crecimiento, año a año, de este tipo de delitos.

Otro de los problemas que existe, y que va in crescendo, vinculado a los ciberdelitos es que:

- No hay un número suficiente de peritos judiciales informáticos. Estos son los que se encargan de recopilar las evidencias tecnológicas del delito cometido. Son como los CSI de los delitos tradicionales. El trabajo del perito es fundamental para que las evidencias obtenidas puedan ser tenidas en consideración por el Juez que juzgue el caso.
- En segundo lugar, hay muy pocos ciberabogados, con formación legal y tecnológica, preparados para entender el delito tecnológico que se ha producido, por lo que estos delitos se siguen abordando como delitos tradicionales.
- En tercer lugar, no tenemos un número suficiente de jueces, con formación tecnológica que sean capaces de entender las pruebas que se les presentan.
- No hay formación específica sobre estas disciplinas.

Desde hace 25 años existe un nuevo continente, por otro lado, el más poblado de todos, llamado ciberespacio. Este ciberespacio lo usamos todos a diario en nuestro ámbito personal y profesional y su uso plantea ciertos problemas de los que muchas veces no somos conscientes:

- No tiene fronteras físicas, más allá de que las máquinas desde las que se realizan los ciberataques estén en un país físico, en el que con mucha probabilidad las exigencias legales son mucho más laxas. Debido a esto no se ve afectado por la territorialidad, base de la jurisprudencia actual.
- La tecnología permite que, en la mayoría de los casos, no lleguemos a saber desde donde se producen los ataques, ni podamos identificar a los autores.
- No está legislado y no existen poderes legislativo ni judicial.

Este ciberespacio ya está considerado desde hace años como el quinto entorno estratégico, por detrás de tierra, aire, mar y espacio, aunque a diferencia de los cuatro anteriores carece de cualquier tipo de ordenación normativa.

EL NUEVO RGPD

La siguiente legislación, que nos afectaba hasta el pasado 25 de mayo, ha sido derogada:

- La LOPD 15/1999.
- El Real Decreto 1720/2007.
- La Instrucción 1/2006 de Sistemas de Videovigilancia.
- La Directiva 95/46 del Parlamento europeo.

En su lugar, actualmente estamos obligados por:

- El nuevo Reglamento General de Protección de Datos europeo.
- En un futuro cercano, la nueva Ley Orgánica de Protección de Datos, de la que sólo se conoce el anteproyecto.

El nuevo Reglamento busca unificar criterios, a nivel europeo, en todo lo concerniente al tratamiento de datos personales y, por lo tanto, afectará a todas las empresas, independientemente de su tamaño y actividad que desarrollen su actividad en cualquiera de los países europeos o, cualquier empresa cuya sede social resida fuera del ámbito europeo pero que presten servicios a usuarios europeos.

Los principios relativos al tratamiento de la información que tratamos se basan en:

- La minimización de los datos que recabamos. Es decir, sólo recabaremos aquellos datos que sean imprescindibles.
- Estos datos deben ser exactos y tienen que estar actualizados.
- Debemos establecer el límite de la finalidad para la que se han recabado los datos.
- Debemos cumplir los principios de licitud, lealtad y trasparencia.

- Debemos limitar el plazo de conservación de los datos de acuerdo a la duración de la prestación de servicios y a las obligaciones legales que nos afecten.

Los datos los podemos obtener:

- Del propio interesado: debemos informarle en el mismo momento en el que obtenemos los datos.
- O de un tercero, debiendo informar en el plazo de un mes desde que obtenemos los datos y siempre en el primer contacto que establezcamos.

El tratamiento de los datos debe fundamentarse en:

- Una relación contractual.
- Una obligación legal para el responsable del tratamiento.
- Un interés:
    - Vitales del interesado.
    - Público o ejercicio de poderes públicos.
    - Legítimo que prevalece del responsable o terceros a los que se comuniquen los datos.
- Consentimientos.

Respecto al consentimiento, este debe ser inequívoco. No se admiten consentimientos tácitos o por omisión, ni se admiten checks premarcados, debiendo ser lo más explícito posible.

Al igual que ocurría con la LOPD, el Reglamento considera una serie de Derechos que defienden los intereses del titular de los datos:

- Derechos ARCO: Acceso, Rectificación, Cancelación (ahora Supresión) y Oposición.
- Además, se incorporan los siguientes derechos:
    - Olvido.
    - Limitación del Tratamiento.
    - Portabilidad.

Respecto al Encargado del Tratamiento, el Reglamento obliga a contratar encargados que garanticen el cumplimiento del RGPD. Esta garantía puede acreditarse:

- Mediante una formación certificada.
- Mediante la certificación de años de experiencia en el tratamiento de datos personales. Por ejemplo, los profesionales que han gestionado la LOPD estos últimos años.

El RGPD nos obliga a cambiar de paradigma. Hasta la fecha hemos tenido una mentalidad reactiva, referente a la seguridad, sin embargo, el Reglamento obliga a que nuestra seguridad sea proactiva, condicionando las medidas de seguridad al riesgo que cada uno asume en el tratamiento de datos de terceros.

Para conseguir esto estaremos obligados a realizar un análisis exhaustivo de los riesgos que nos pueden afectar, clasificando y cuantificado la probabilidad de que un riesgo se materialice y el impacto que provocaría.

Además de analizar el riesgo debemos evaluar el impacto. Ten en cuenta que

RIESGO = PROBABILIDAD X IMPACTO.

Una de las obligaciones que más llama la atención es la de tener que informar a la Agencia Española de Protección de Datos cuando hayamos sufrido un incidente de seguridad, en el que se hayan visto afectados datos personales, en el plazo de 72 horas desde que se detectó dicho incidente.

Deberemos informar sobre:

- La naturaleza y categoría del incidente.
- El número de afectados.
- Quien es el Delegado de Protección de Datos, si lo tenemos.
- Las consecuencias ocasionadas.
- En el caso de que la gravedad del incidente supone un alto riesgo para los derechos y libertades de los titulares de los datos, debemos informar a los interesados.

El Delegado de Protección de Datos es una nueva figura que aparece con el nuevo Reglamento. No todas las empresas tienen la obligación de tener uno. Si tienen la obligación:

- Organismos Públicos.
- Empresas que manejan datos a gran escala.
- Colegios Oficiales.
- Empresas del sector salud.
- Centro educativos.
- Entidades aseguradoras.
- Empresas de publicidad y prospección comercial.

No es obligatorio para empresas de menos de 250 trabajadores siempre que no traten información que pueda afectar a los derechos y libertades de los titulares.

Podrá ser DPD cualquier persona con conocimientos en legislación y experiencia en el tratamiento de datos personales o aquellas personas que superen la formación certificada al efecto.

Como novedad importante, ya no será obligatorio inscribir los ficheros, como obligaba la LOPD.

Ahora deberemos tener un registro de actividades que debe contener:

- Nombre y datos de contacto del Encargado y del Delegado.
- Finalidades del tratamiento.

- Descripción de las categorías de los interesados y categorías de los datos tratados.

Hay novedades en cuanto a:

- Los sistemas de videovigilancia.
- El tratamiento de datos de menores de edad, siendo necesario el consentimiento de los tutores legales de los menores de 13 años.
- El tratamiento de datos de fallecidos, pudiendo sus herederos solicitar el acceso a los datos, su rectificación o incluso su supresión.

Por último y no menos importante son las causas por las que debemos cumplir con el RGPD:

- No podemos exigirle a alguien que trate nuestros datos ajustándose a la ley si nosotros no lo hacemos.
- Para evitar sanciones, que han aumentado de una forma muy importante:
    - Sanciones graves: hasta 10 millones de € o el 2% de la facturación.
    - Sanciones muy graves: hasta 20 millones de € o e 4% de la facturación.

Imagina lo que le hubiera costado a Facebook la reciente sanción que le ha impuesto la AEPD, por el uso indebido de los datos por parte de WhatsApp, teniendo en cuenta que le sancionaron con 600.000€, la mayor sanción ajustada a la anterior LOPD.

Debemos darle un tiempo a nuevo RGPD para ver como se incorpora al día a día de las empresas, sin embargo, hay informes que dicen que el 65% de las empresas en España no están preparadas para tratar su información de carácter personal de acuerdo al Reglamente. Y eso teniendo en cuenta que hemos tenido dos años para adaptarnos.

La propia Agencia Española de Protección de Datos ya informó, semanas antes del 25 de mayo, que no habrá ningún tipo de moratoria y que iniciaría inmediatamente planes de inspección para empresas de sectores críticos: salud, instituciones financieras y empresas de telecomunicaciones.

Si tu empresa todavía no cumple con el nuevo RGPD no lo dejes más. Trabajarás mejor y evitarás sanciones.

6. PLAN DE SEGURIDAD: PREVENCIÓN, AUDITORÍA Y PROTECCIÓN.

Todas las empresas deberían tener un Plan de Seguridad, pero muy pocas lo tienen. En él se deben identificar las amenazas que nos acechan, los riesgos que asumimos y el impacto que provocaría en nuestra actividad el que se materializara uno de esos riesgos.

Además, se identificarán las medidas de prevención que implantaremos, las auditorías, internas o externas, que desarrollaremos de forma periódica y como nos protegeremos cuando suframos un incidente de seguridad, definiendo lo que se denomina Plan de Respuesta ante Incidentes.

Sólo existen dos tipos de empresas: las que han sido atacadas y lo saben y las que han sido atacadas y no lo saben.

Ante esta afirmación sólo nos queda asumir que en cualquier momento podemos sufrir un incidente que pueda poner en peligro la continuidad de nuestra actividad y debemos prepararnos para recuperar esa actividad en el menor tiempo posible y con el menor impacto posible.

Las causas de estos incidentes, como ya hemos ido dejando entrever en este manual, pueden ser:

- Directas, por lo que podríamos preverlas y mitigarlas:
    - Daños materiales:
        - Inundaciones.
        - Incendios.
        - Fallos eléctricos
    - Errores humanos, en un porcentaje muy elevado de las ocasiones.
    - Robos/fugas de información.
    -
- Ajenas, por lo que debemos estar atentos y a la espera de que se produzcan en el momento más inesperado:
    - Infecciones por Malware.
    - Ataques dirigidos.
    - Ocasionados por nuestros proveedores y/o colaboradores.

Los planes de respuesta ante incidentes, también denominados planes de continuidad de negocio, nos van a permitir tener previstas las acciones a llevar a cabo cuando se produzca un incidente que tengamos catalogado y tienen que tener en cuenta dos aspectos importantes:

- El tiempo que tardaríamos en recuperar el sistema.
- El tiempo máximo que podríamos soportar la caída del servicio, parcial o totalmente.

Estos dos factores condicionarán, en gran parte, las medidas que deberemos implantar. No serán las mismas para una empresa que se puede permitir el lujo de estar un día entero sin sistemas informáticos que aquellas empresas que no pueden parar más de dos horas.

Por otro lado, no pienses que esto son consideraciones que sólo deben realizarse en grandes empresas. Al igual que comentábamos cuando nos referíamos al cambio de mentalidad que exige el nuevo RGPD, teniendo que ser proactivos y no reactivos cuando hablamos de seguridad, deberemos entender que este tipo de acciones nos permitirán ser más eficientes y resilientes, obteniendo un impacto positivo para la empresa de cara a clientes y proveedores.

La creación de estos planes debemos realizarlos atendiendo a nuestra realidad, es decir, las medidas a adoptar deben ser proporcionales a nuestras necesidades y se basarán en la definición de objetivos y procesos.

Los objetivos, habitualmente, se centran en la recuperación del sistema, en un periodo mínimo de tiempo, manteniendo el nivel de servicio en los límites que hayamos establecidos como asumibles.

Los procesos seguirán las siguientes fases, siempre teniendo en cuenta la idea de mejora continua, es decir, una vez que lleguemos a la fase final volveremos a la primera para mejorar continuamente nuestro plan.

Ten en cuenta que las empresas y sus infraestructuras son dinámicas y esto influye en nuestros planes de seguridad ya que, seis meses, o un año después de haber definido objetivos y procesos, es posible que, por la prestación de un nuevo servicio o la incorporación de nueva tecnología en nuestra infraestructura, el plan anterior no se ajuste a la realidad de este momento, dejando inútiles los objetivos y procesos establecidos.

Las fases que definen nuestro plan se deben ajustar a las siguientes:

- En la fase de Análisis, evaluamos las amenazas, riesgos e impacto, a corto y medio plazo.
- En la fase de Diseño, definiremos las medidas que vamos a aplicar y los procedimientos de respuesta.
- En la fase de Implementación, gestionaremos la incorporación de las medidas seleccionadas y estableceremos un calendario de programas de formación/concienciación para nuestros trabajadores.
  Siendo el trabajador interno el eslabón más débil de la seguridad, es muy importante que entiendan los riesgos y las consecuencias que supone utilizar de forma inapropiada la tecnología que se le proporciona para desarrollar su actividad.
- En la fase de Verificación debemos asegurarnos de que lo que hemos planteado en la teoría funcionará correctamente el día que suframos un incidente.
  En ocasiones, volveremos a las fases de diseño o implementación si se observa en esta última fase que las medidas diseñadas no son tan efectivas como creíamos.

Una vez lleguemos a la última fase volveremos a la fase de diseño para volver a empezar, incluso aunque nuestros procesos productivos, servicio y tecnología no hayan cambiado. Cada poco tiempo aparecen nuevas vulnerabilidades que nos afectan y debemos estar atentos a los nuevos riesgos que nos acechen.

Todo esto se puede apoyar con la realización de auditorías internas y, eventualmente, externas. De vez en cuando es interesante que algún consultor externo nos permita tener una visión diferente a la nuestra, muchas veces condicionada. Eso de, cuatro ojos ven más que dos, también se aplica en estas situaciones.

Estas auditorías deben combinarse con la realización de simulacros que nos permitan estar preparados el día que tengamos que llevar a la práctica todos estos procedimientos que estamos desarrollando.

Por otro lado, es importante definir claramente cuales son los activos que queremos auditar, si serán todos o sólo una parte.

En definitiva, nuestro Plan de seguridad debe tratar todas y cada una de las siguientes medidas:

- Medidas aplicadas a desastres naturales.
- Medidas aplicadas a problemas estructurales de nuestras instalaciones.
- Medidas aplicadas a problemas de Hardware.
- Medidas aplicadas a problemas de los Sistemas Operativos: clientes/servidores.
- Medidas aplicadas a problemas de Software.
- Medidas aplicadas a problemas de la red interna y las comunicaciones externas.
- Medidas aplicadas a problemas de las copias de seguridad.
- Medidas aplicadas a problemas con la información (CIA).
- Medidas aplicadas a problemas con el personal interno y colaboradores externos.
- Medidas aplicadas a problemas con el patrimonio.
- Medidas aplicadas al cumplimiento normativo y legal vigente.
- Medidas aplicadas a problemas provocados por otros riesgos.

Como ves, buscamos minimizar las posibilidades de sufrir un incidente y definir cómo reaccionar cuando lo hemos sufrido y, aunque sea un poco simplista, podemos decir que una buena seguridad se basa en tres aspectos fundamentales:

- El usuario debe tener mínimos privilegios de acceso. Es decir, sólo podrá acceder a aquellos recursos que estén directamente relacionados con la actividad que desarrolle.
- Mínima exposición, es decir, sólo tener activo aquellos servicios informáticos que realmente ofrezco interna y/o externamente.
- Tendremos un sistema de copia de seguridad, actualizado, que combine el almacenamiento local de esas copias con un sistema de backup en cloud, redundante, que nos permita tener fuera de la empresa la información.

Aunque son situaciones un poco extremas, piensa en lo que sucedió en los atentados del 11 de septiembre en Estados Unidos, o el incendio del Edificio Windsor en Madrid.
Las empresas que no tenían copia de seguridad fuera de las oficinas que estaban en esos edificios no pudieron seguir desarrollando su actividad, ante la imposibilidad de recuperar su activo más valioso.

Si controlamos estos tres aspectos reduciremos enormemente la posibilidad de sufrir un incidente y, si lo sufrimos, el tiempo de reacción y vuelta a la normalidad. El resto de los factores a tener en cuenta descritos anteriormente, no menos importantes, deben estar alineados con estos tres.

En definitiva: no desatiendas la seguridad informática de tu empresa. Evitarás pérdidas económicas, pérdidas de reputación y dolores de cabeza.

CAPÍTULO 2. SEGURIDAD CLOUD PARA PYMES Y AUTÓNOMOS.

1. SERVICIOS DISPONIBLES EN LA NUBE.

Cuando decimos que utilizamos servicios en la nube, o en cloud, lo que estamos queriendo decir es que estamos utilizando servicios, bajo demanda, en una infraestructura qué habitualmente no es nuestra, y qué habitualmente se encuentra en Internet.

Todos usamos servicios cloud desde hace tiempo cuando usamos los servicios gratuitos o de pago, de Google o Microsoft, entre otros proveedores. Por ejemplo: servicios como el correo electrónico, el almacenamiento de información en los drives de ambos proveedores, herramientas como Skype o Hangouts, para realizar video llamadas, aplicaciones ofimáticas como procesadores de texto, hojas de cálculo o aplicaciones para generar presentaciones vistosas, y muchas más, algunas prácticamente desconocidas para el público en general.

La nube está empezando a revolucionar los espacios de trabajo y en 15 años, poco más o menos, habrá cambiado completamente nuestras empresas y oficinas.

¿Recuerdas como era tu oficina hace 15 ó 20 años? ¿A qué ha cambiado?

Pues en los próximos 15 ó 20 va a cambiar más aún, fundamentalmente porque habrá sacado de nuestras empresas la infraestructura que ahora mantiene operativos nuestros negocios.
Piensa en oficinas en las que los servidores, el almacenamiento, el backup, los sistemas de seguridad, las aplicaciones, … ya no estén físicamente en el mismo sitio en el que están ahora, dejando únicamente terminales, prácticamente tontos, que se conectarán a todos estos servicios online, y algún equipo de impresión para poder imprimir los pocos documentos que se imprimirán en papel. A fecha de hoy ya hay un importante número de empresas que prácticamente no imprimen nada, utilizando estos dispositivos para digitalizar documentos.

¿Por qué se va a producir este cambio, que ya ha empezado a materializarse?

Fundamentalmente porque nos va a costar menos pagar por su uso, a modo de alquiler que adquirir los equipos y mantenerlos.
Al igual que ocurre cuando te compras un coche, hay unos gastos importantes, en los que habitualmente no reparamos.

Es evidente que no todas las empresas tienen las mismas necesidades, pero ¿te has parado a pensar alguna vez lo que cuesta la infraestructura tecnológica que necesita una empresa?

- Las salas que debemos tener preparadas para ubicar nuestra infraestructura más crítica, con techos y suelos técnicos.
- Sistemas de refrigeración y sistemas antiincendios.
- Sistemas de identificación de acceso.
- Armarios y cabinas.
- Los propios servidores: controladores de dominio, servidores de bases de datos, de almacenamiento, de backup, …
- Todo el equipamiento de comunicaciones y su seguridad: Routers, Firewalls, IDS/IPS, …
- Las garantías de todos estos equipos.
- La energía necesaria para mantener encendido todo esto las 24 horas del día.
- Personal que lo mantenga operativo y securizado.
    - Y además cumpliendo todas las normativas vigentes para cumplir la ley y evitar posibles sanciones.

¿De verdad piensas que es más económico comprar que pagar por uso? Pues en este momento ya no lo es, pero dentro de unos años, cuando el mercado de este tipo de servicios se haya asentado, será mucho más económico ir a la nube que quedarse en tierra.

Si el aspecto económico nos agrada, siempre solemos poner el reparo de nuestra información no está en nuestro poder, la almacenamos en máquinas de un proveedor de servicio del que nos tenemos que fiar.

Y la pregunta es ¿de verdad crees que tu información y servicios van a estar más seguros en tus instalaciones que si los tienes en los centros de datos de empresas como Amazon, Google, Microsoft, IBM, …? Es evidente que las instalaciones de estos, los sistemas de redundancia, … serán inalcanzables para nosotros. Docenas de CPDs ubicados por todo el planeta replicando nuestra información para que, en caso de desastre en cualquiera de ellos, la información esté distribuida en el resto y nuestro servicio no se vea afectado por una falta de disponibilidad de la misma.

Aun fijándonos en las innumerables ventajas que aporta este sistema, debemos reconocer que puede haber un pequeño tipo de empresas a las que este servicio no les encaje por su idiosincrasia.

Por ello debemos realizar un estudio previo para identificar si nuestro negocio se puede ver beneficiado si adopta este tipo de servicio y, en el caso de que así sea, dimensionemos en condiciones nuestra necesidad. Y esto no es trivial.

Por otro lado, la flexibilidad y escalabilidad de estos servicios y la posibilidad de acceder a los recursos desde cualquier sitio, en un momento en el que la movilidad se ha vuelto imprescindible para la gestión de nuestros negocios, son otros de los motivos para decidirse a dar el salto a la nube.

Pero ¿a qué nos referimos cuando hablamos de flexibilidad y escalabilidad?

Fundamentalmente a la capacidad de dimensionar mi infraestructura atendiendo a mis necesidades en cada momento, de una forma casi inmediata.

Supón que adquieres un servidor para un nuevo servicio que necesitas prestar a tus trabajadores. 6 meses más tarde necesitas incrementar la plantilla en un número de trabajadores con los que no habías contado cuando dimensionaste el servidor que compraste y necesitamos ampliarlo porque nos hemos quedado cortos.

En una situación tradicional, tendríamos que ponernos en contacto con uno o varios proveedores, solicitar un presupuesto, realizar el pedido, esperar varios días a que llegara el material adquirido e instalar la memoria, procesador o disco duro que hayamos adquirido. Esto, en máquinas de gama media va a suponer parar el servidor, instalar el nuevo hardware, reconfigurarlo y volver a poner en marcha la máquina.

En lo que hemos leído la explicación que acabamos de dar, habríamos realizado una ampliación de los recursos de nuestras máquinas en la nube, pagando a partir de ese momento por el servicio recibido.

Ahora bien, imagínate que tiempo después, el personal incorporado deja de ser necesario, porque había sido contratado para una campaña concreta. En este momento no puedo ponerme en contacto con el proveedor que me ha suministrado el equipamiento para devolvérselo porque ya no lo necesito. Sin embargo, en el tiempo que hemos tardado en leer esta nueva explicación, habríamos redimensionado de nuevo nuestros equipos, a la baja, pagando a partir de ese momento por la nueva configuración que estamos usando.

Otra situación, que por desgracia ocurre con frecuencia, se da cuando hemos adquirido un equipamiento que pagamos a través de un crédito, un renting o un leasing y se da la circunstancia de que tenemos que cerrar nuestra actividad. En este caso, tenemos que terminar de pagar el equipamiento adquirido sin poder recuperar la invertido porque el valor del producto se ha devaluado de tal forma que no vale si quiera lo que se debe. Sin embargo, si utilizamos servicios en nube y se da una situación como la descrita, le decimos al proveedor que ese mes va a ser el último que le pagamos y se acaba el problema.

Uno de los principales obstáculos que podemos encontrar a la hora de implementar estas soluciones se debe a la necesidad de tener una muy buena conectividad para poder acceder a los servicios. Si no hay conexión a Internet, no hay servicio.

Es cierto que en los núcleos urbanos esto no es problema, pero cuando sales 25 kilómetros de las ciudades, tener acceso a una conexión de fibra óptica no es tan sencillo y económicamente suele ser bastante más costoso.

Para poder tomar una decisión al respecto necesitamos conocer los tipos de nubes que existen y el tipo de servicios que se puede contratar.

Tipos de nubes

- Públicas:
  Aquellas que proveen proveedores como Telefónica, Amazon, Microsoft, Google, …
  Toda la infraestructura está en sus instalaciones y la compartimos con otros clientes
- Privadas:
  Aquellas que adquiero e instalo en mis propios CPDs para prestarnos a nosotros mismos el servicio. El problema es que suelen ser bastante caras.
- Híbridas:
  En entornos corporativos grandes, tanto públicos como privados, están muy extendidas. Una parte de la infraestructura la tenemos nosotros mismos y otra parte está alquilada en un proveedor externo, buscando redundancia y tolerancia a fallos.

Tipos de Servicios:

- IaaS: Infrastructure as a Service
  Con este tipo de servicio, lo que el proveedor nos ofrece son Máquinas Virtuales en las que vamos a poder colocar nuestros servidores, nuestros equipos de comunicaciones, nuestros sistemas de seguridad, balanceadores de carga, …
- SaaS: Software as a Service.
  Con este tipo de servicio, lo que proveemos a nuestros usuarios es el Software (CRM, ERP, …), escritorios virtuales, correo electrónico en nube, …
- PaaS: Platform as a Service
  Con este tipo de servicio adquirimos plataformas como servicio, para despliegue de aplicaciones como servidores web, bases de datos, sistemas de big data, …

Una cosa que nos debe quedar clara es que la seguridad de los servicios suele estar repartida entre el proveedor y el cliente. La administración, gestión y securización de estos entornos hay que contratarlos a parte de la infraestructura que contratemos. Esto es así porque nos podría interesar usar la infraestructura en la nube, pero ser nosotros mismos los que la gestionáramos. Por tanto, el proveedor del servicio nos lo podrá ofrecer siendo nosotros los que tomemos la decisión de gestionarlo nosotros mismos o externalizarles a ellos la administración de nuestra infraestructura en la nube.

2. RIESGOS Y AMENAZAS.

Utilizar servicios en la nube exige un cambio de mentalidad, ya que nuestra infraestructura deja de estar bajo nuestro "estricto" control, como ha estado hasta ahora.

Aunque ya hemos comentado las ventajas económicas, de flexibilidad y escalabilidad, de las que nos beneficiamos al utilizar servicios cloud, no es todo oro lo que reluce y debemos tener en cuenta los riesgos que asumimos y las amenazas a las que nos vemos expuestos:

- No solemos tener acceso a las instalaciones físicas de nuestros proveedores cloud. Sin embargo, debemos conocer la ubicación real de nuestras máquinas virtuales.
- Debemos tener muy claros los contratos que vinculan nuestra relación y en los que se incluirá:
  - Qué servicios se prestan y cuáles no.
  - Qué tiempos de respuesta máximos nos afectarán.
  - Las responsabilidades que asume el proveedor, exigiendo cláusulas de confidencialidad y seguridad de los datos ya que debemos cumplir las leyes de protección de datos vigentes en cada momento.
- Como hemos indicado antes, una pérdida de conectividad puede paralizar la actividad de mi empresa.
- Tendremos que mantener las políticas de seguridad que afectaban a los servicios que hemos trasladado a la nube.

Las amenazas estarán directamente vinculadas al tipo de servicio contratado y al contrato de servicios firmado, teniendo especial impacto quien debe encargarse de gestionar y administrar los servicios.

Si no tenemos controlados todos estos aspectos podemos vernos afectados por:

- Fugas de información.
- Suplantación de identidad.
- Accesos no autorizados.
- Incumplimiento normativo.
- …

3. CONSIDERACIONES LEGALES.

Si debemos tener en cuenta la legislación vigente que nos afecta, en todo momento, más aún debemos tenerla en cuenta cuando nos decidamos a contratar servicios en cloud.

En España nos afectaba la Ley Orgánica de Protección de Datos (LOPD) pero, desde el pasado 25 de mayo, nos regimos por el nuevo Reglamento General de Protección de Datos (RGPD) europeo, con el que se pretende unificar criterios respecto a la protección de datos personales, en el ámbito europeo.

El RGPD es una norma directamente aplicable, que no requiere de normas internas de trasposición ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación. Por ello, los responsables deben ante todo asumir que la norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta ahora.

En cuanto a los servicios cloud, el principal aspecto que tenemos que tener en cuenta es el de la ubicación de nuestros datos, es decir, las máquinas en las que almacenamos nuestros datos o nuestro correo electrónico deben estar dentro del ámbito territorial permitido en el RGPD.

Para cumplir las obligaciones impuestas por el Reglamento Europeo debemos atender:

- A la protección desde el diseño y por defecto, no solo con la obligación de garantizar la seguridad de los datos personales, si no que se deberá tener en cuenta también la forma del almacenamiento de la información para atender el derecho de acceso, el de rectificación y limitación al tratamiento, el derecho al olvido y sobre todo el nuevo derecho a la portabilidad de los datos.

- Cumplimiento proactivo, disponiendo de todas las medidas técnicas y organizativas apropiadas para poder demostrar, en cualquier momento, que los tratamientos de datos son conformes con este Reglamento.

    - En caso de manejar información de carácter personal, el Reglamento exige que el proveedor contratado ofrezca garantías suficientes en cuanto a su cumplimiento, es decir, que disponga y pueda demostrar, que cuenta con todos los medios necesarios para cumplir sus obligaciones como encargado en el manejo de los datos personales de su cliente. Para ello el responsable de los datos personales no solo deberá firmar el contrato con el proveedor del Cloud, donde se establezcan sus obligaciones en el manejo de los datos, si no que deberá establecer, en el proceso de selección del proveedor, mecanismos para poder determinar si éste cuenta con estas garantías

suficientes para cumplir el Reglamento y la protección de los derechos de los interesados.

- Evaluaciones de impacto para ciertos tratamientos de datos, como en la elaboración de perfiles o cuando se manejen a gran escala datos de categoría especial, que son los relativos al origen racial, religión, afiliación sindical, genéticos y de salud. Con ello se determinará que riesgos existirán para los derechos de las personas en el tratamiento de sus datos personales.

- En cuanto a las medidas de seguridad a implantar sobre los datos, éstas deben estar ajustados al riesgo, pudiendo incluir seudonimización y cifrado (tanto en tránsito como mientras permanece almacenada en mis equipos informáticos), para garantizar la confidencialidad, integridad, resiliencia de los sistemas y servicios, la capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida. Pero los riesgos para el responsable de los datos y la empresa que presta el Cloud pueden no ser iguales, dado que dependerán estos riesgos de los tratamientos de datos que se lleven a cabo cada uno de ellos. Por lo que convendrá acordar en el contrato con el proveedor cual serán estos riesgos y las medidas que deban implantarse.

    - En el caso de producirse una violación de la seguridad en los datos, y exista riesgo para los derechos y libertados de las personas, es obligatorio notificarlo a la Agencia Española de Protección de Datos, en el plazo de 72 horas desde que se haya tenido conocimiento.

    - Deberemos tener claro quién es el responsable del incidente, el proveedor o nosotros. Si la brecha de seguridad es atribuible al proveedor cloud, este deberá notificárnoslo para posteriormente notificarlo nosotros a la Agencia. Para atender a esta obligación, deberemos establecer algún procedimiento que determine que violaciones de seguridad se notificarán, el mecanismo para notificarla.

Deberemos informar, incluso, a los interesados, cuando sus datos hayan sufrido un alto riesgo desde el punto de vista de sus derechos y libertades, teniendo entonces que incorporar en este procedimiento de notificación de violaciones de seguridad a la Agencia Española de Protección de Datos, el mecanismo para comunicarlo a las personas, tras determinar si se produjo un alto riesgo, como decíamos, para sus derechos y libertades.

CAPÍTULO 3. ¿ESTÁS PREPARADO PARA UN CIBERATAQUE?

1. INFECCIÓN POR RANSOMWARE.

1.1. QUÉ ES EL RANSOMWARE.

El Ransomware es un Malware (software malicioso) que bloquea nuestro dispositivo, pudiendo llegar a cifrar el contenido del disco duro. Una vez que hemos perdido el control sobre nuestro equipo nos reclaman el pago de un rescate que habitualmente se solicita en criptomonedas, bitcoins por ejemplo.

Hoy día hay Ransonware tanto para equipos de sobremesa y portátiles como para dispositivos móviles (smartphones y tablets).

El Ransomware llega oculto dentro de otro archivo o programa y se activará en el momento que hagamos doble click sobre el archivo.

Podemos infectarnos desde archivos que recibimos en como adjuntos en correos electrónicos o que recibimos como adjuntos en aplicaciones de mensajería instantánea como WhatsApp o Telegram. Tanto para dispositivos móviles como si usamos las aplicaciones web que nos permiten usar el servicio en un ordenador de sobremesa o portátil.

También podemos infectarnos visitando páginas de dudoso origen: pornográficas o de descargas de películas o música e, incluso, al realizar el proceso de actualización de sistemas operativos y software legítimo, como Microsoft Windows o Adobe Flash, si no lo hacemos desde las webs oficiales de los fabricantes.

Una vez que ha penetrado en el ordenador, el malware se activa y provoca el bloqueo de todo el sistema operativo y lanza el mensaje de advertencia con la amenaza y el importe del “rescate” que se ha de pagar para recuperar toda la información. El mensaje puede variar en función del tipo de ransomware al que nos enfrentemos: contenido pirateado, pornografía, falsos virus, …

1.2. ¿CÓMO EVITAMOS INFECTARNOS?

Para evitar infectarnos por un Ransonware debemos seguir las siguientes pautas, pautas que por otro lado son de sentido común:

- Mantener nuestro sistema operativo y nuestras aplicaciones actualizadas, evitando así que el atacante se aproveche de vulnerabilidades ya identificadas.
- Disponer, por lo menos, de un antivirus siempre actualizado.

- No abrir correos electrónicos o archivos con remitentes desconocidos. Nos intentarán engañar enviándonos correos electrónicos con un gancho para que piquemos.
- Evitar navegar por páginas no seguras o con contenido no verificado.
- Tener un sistema de copia de seguridad y un procedimiento de recuperación definido que nos permitan recuperar el sistema en el menor tiempo posible sin pérdida de información.

1.3. UNA VEZ INFECTADOS, ¿CÓMO LO ARREGLAMOS?

Pues realmente no es sencillo. Las autoridades y el propio INCIBE insisten en no pagar el rescate porque nadie te garantiza que vayas a recuperar el acceso a la información. Por otro lado, aunque la recuperes es casi seguro que quedará infectada con algún otro tipo de malware.

La mejor solución sería recuperar una copia de seguridad, lo más reciente posible, pero en muchas ocasiones no disponemos de ella.

En otras ocasiones y si el ransomware ya está identificado y analizado, es posible que exista algún tipo de procedimiento de recuperación.

En caso contrario, podemos recurrir:

- Al servicio antiransomware de INCIBE https://www.incibe.es/en/node/5139
- Al grupo de delitos telemáticos de la Guardia Civil https://www.gdt.guardiacivil.es/webgdt/home_alerta.php
- A la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional. http://www.policia.es/org_central/judicial/udef/bit_alertas.html

1.4. COMPORTAMIENTO DEL RANSOMWARE AL INFECTAR EL SISTEMA.

Durante estos últimos años hemos sufrido numerosos ataques de tipo ransomware y podemos calificar los ataques de:

1. Bloqueo del Sistema. “Virus de la Policía”.
2. Cifrado de Información. CTB-Locker.
3. Bloqueo y cifrado del sistema. Segunda variante de Petya | Bad Rabbit.
4. Bloqueo y malware que habla para pedir el rescate. Jisut.
5. Cifrado y robo de información o billeteras virtuales. Cerber.
6. Ransomware PUBG. MSIL/Filedecoder.HD
7. Pago con fotos íntimas. nRansom.
8. Ransomware en dispositivos IoT
9. Ransomware en smartphones o tablets.
10. Ransomware para fugas de información.

2. ATAQUE POR PHISHING.

2.1. ¿QUÉ ES EL PHISING?

¿Alguna vez has recibido un correo electrónico de alguien en el que te piden que sigas un enlace que te lleva a una página web donde tienes que realizar algún tipo de revisión vinculada a tus datos personales? ¡Mucho cuidado! Es muy posible que estés siendo víctima de un ataque de tipo phishing.

El phishing es una técnica utilizada por ciberdelincuentes para, haciéndose pasar por una entidad o persona de confianza, a través del correo electrónico u otros canales de comunicación, robarnos información confidencial como nombres de usuario, contraseñas y datos de tarjetas de crédito, entre otras, mientras accedemos a un servicio web que creemos seguro y legítimo.

Aunque podemos ver phishing en otros escenarios, el más frecuente está asociado con la clonación de una página web para hacer creer al visitante que se encuentra en el sitio web al que quería acceder, cuando en realidad es falso.

El usuario creerá que está accediendo a la web legítima e introducirá sus credenciales de acceso sin darse cuenta de que en realidad está enviándoles sus datos al atacante. Una vez introducidos los datos, y otra vez sin darse cuenta, será redirigido automáticamente hacia la página legítima a la que quería acceder.

El phishing es el origen del 90% de los ciberataques. Es por eso por lo que la inversión en la concienciación para prevenirlos tiene que ser cada vez más elevada, sin olvidar que los ciberdelincuentes buscaran nuevos métodos de engaño.

La consecuencia es que los usuarios desconocen que el sitio web donde están ingresando información confidencial está controlado por estos ciberdelincuentes.

2.2. TIPOS DE PHISHING.

- **DECEPTIVE PHISHING**: es el más común y ya descrito anteriormente. Busca conseguir nuestras credenciales de acceso a un servicio web (usuario y contraseña, habitualmente).
  Por ejemplo: Intento de phishing con Carrefour.

Fuente: Guardia Civil

- **MALWARE-BASED PHISHING**: son aquellos ataques en los que el phishing busca que el usuario descargue y/o ejecute un archivo o visite una página web desde dónde se le infectará con un Malware.
- **DNS-BASED PHISHING:** También conocido como Pharming. El ataque consiste en modificar los archivos hosts de una empresa o el sistema de nombres de dominio de la misma, para que las solicitudes de URL devuelvan una dirección falsa y las comunicaciones sean dirigidas a un sitio web falso. Este tipo de ataques se podrían mitigar si las contraseñas de los administradores de los routers que nos dan servicio a internet se cambiaran una vez instalados, algo que, en el entorno de las PYMEs, Micropymes o Profesionales, no hace prácticamente nadie.
- **CONTENT-INJECTION PHISHING:** en estos ataques se sustituye parte del contenido de un sitio legítimo con contenido falso diseñado para engañar o desviar al usuario a dar su información confidencial.
- **SEARCH ENGINE PHISHING:** mediante esta técnica podemos infectarnos simplemente haciendo una búsqueda en Google o Bing, ya que se los enlaces maliciosos están indexados en los motores de búsqueda de los propios buscadores, ofreciéndose los resultados en una búsqueda normal y corriente. Uno de los casos más recordados fue el sufrido por el Banco Sabadell. Durante un tiempo aparecieron dos anuncios patrocinados en las dos primeras posiciones de los resultados de búsqueda de Google. Cuando se pinchaba en ellos, la víctima era redirigida a una página web fraudulenta que solo se diferenciaba de la oficial en la URL.

- **MAN-IN-THE-MIDDLE-PHISHING:** es el más difícil de detectar, ya que el ciberdelincuente se coloca entre el ordenador del usuario y el servidor, grabando, así, la información que se transmite entre ambos.

2.3. ¿CÓMO PODEMOS EVITAR EL PHISHING?

- No conteste ningún correo que solicite información personal o financiera. Recuerda que ningún banco, u otras entidades, solicitan información confidencial a través de canales no seguros y en ningún caso lo hacen a través de correo electrónico.
- Nunca haga click en el enlace que te invitan a visitar. En todo caso escribe tú mismo la dirección en tu navegador de Internet.
- Comprueba que la página utiliza el protocolo HTTPS para proteger la autenticación y la comunicación. En los navegadores aparecerá un pequeño candado cerrado. Si la dirección comienza por http:// no sigas adelante.
- Activa con tu entidad bancaria el sistema, disponible en casi todos, que obliga a que te avisen cuando se realice cualquier tipo de trasferencia desde tus cuentas.
- Usa sistemas anti-spam.

3. FUGA DE INFORMACIÓN.

En el año 2010 se produjo, la que está considerada hasta la fecha, como la mayor filtración de información de la historia. Wikileaks, una organización sin ánimo de lucro publicó un total de 250.000 documentos que se habían enviado entre el Departamento de Estado Estadounidense y sus embajadas repartidas por todo el mundo. Las consecuencias ya las conocemos todos.

Todos los incidentes de fuga de información nos constatan lo difícil que es proteger la confidencialidad de la información, por otro lado, el activo más valioso de cualquier organización.

Denominamos incidentes de **fuga de información** a aquellos incidentes que ponen en poder de una persona ajena a la organización, información confidencial.

El incidente puede ser interno o externo y podría ser provocado o no intencionado.

Algunos ejemplos de fuga de información pueden ser:

- Un empleado vendiendo información confidencial a la competencia (incidente interno e intencional).
- Un administrativo que pierde un documento en un lugar público (incidente interno y no intencional).
- La pérdida de una portátil, tablet, smarphone o *pendrive* (incidente interno y no intencional).
- El acceso desde el exterior a una base de datos de la organización (incidente externo e intencional).
- Un equipo infectado con un Spyware que envíe información al exterior sin que seamos conscientes de ello (incidente externo e intencional).

La intencionalidad del incidente determina el impacto de la fuga de información. En el caso de que el incidente sea no intencionado es muy probable que no ocurra nada, sin embargo, en los incidentes provocados, el impacto es evidente y dependerá de qué información se haya visto afectada.

Independientemente de que el origen sea intencionado o inintencionado, la realidad es que el incidente es difícilmente reparable pudiendo llegar a provocar desde pérdidas económicas a pérdidas reputacionales o de imagen.

Impacto global

- Daño de imagen.
- Consecuencias legales.
- Consecuencias económicas.
- Otras consecuencias que suponen un impacto negativo en ámbitos muy diversos, como, por ejemplo, el ámbito institucional, político, diplomático o gubernamental, entre otros.

Otros factores que tener en consideración, sobre el impacto global, tiene que ver con el tipo de información que ha sido sustraída:

- Si son datos de carácter personal o no.
- Si los datos son internos a la organización o son externos.

4. ATAQUE POR INGENIERÍA SOCIAL.

La ingeniería social, que no es otra cosa que conseguir engañar a alguien con el objetivo de conseguir de ellos lo que se desee, se ha convertido en uno de los principales vectores de ataque a las empresas. Fundamentalmente porque a partir de este ataque, a un trabajador, como se inician ataques como los descritos anteriormente: malware, ransomware, …, llegando incluso a las temidas APTs o Amenazas Persistentes Avanzadas.

El término saltó a la fama tras la publicación, por parte de The New York Times, del ataque realizado por una unidad militar china (conocida como APT1) contra las redes de diferentes medios, mediante una campaña de spearphishing y malware.

Las APTs son, probablemente el ataque más sofisticado que nos podemos encontrar y al que más recursos va a destinar el ciberdelincuente. A diferencia de lo visto hasta ahora, son ataques dirigidos contra compañías concretas, no ataques

CAPÍTULO 4. RELACIÓN SEGURA CON PROVEEDORES Y CLIENTES.

1. INTRODUCCIÓN.

Toda empresa necesita relacionarse con sus proveedores y clientes para que la actividad que desarrolla genere los beneficios deseados.

En relación a nuestros clientes, en primer lugar, debemos cumplir con la legislación vigente, LOPD/RGPD, para garantizar que los datos que almacenamos de ellos están a buen recaudo y lejos del alcance de un ciberdelincuente.

A parte de los datos personales, prácticamente toda nuestra relación con ellos es ya digital. Pedidos, albaranes, facturas, informes, …, se envían por email, utilizamos herramientas de mensajería instantánea como WhatsApp o Telegram, o guardamos la información que queremos enviar en un espacio en la nube, como Drive de Google, Onedrive de Microsoft, Dropbox, … enviándoles el enlace de acceso a los mismos.

Que nuestros clientes confíen en nosotros es fundamental, y no sólo respecto a los servicios que nos contratan, sino también al tratamiento que hacemos de su información. Por otro lado, ya es muy frecuente que nuestros grandes clientes nos obliguen a implementar medidas de seguridad tecnológica que asegure que no van a tener problemas ocasionados por unas deficientes medidas de seguridad tecnológicas por nuestra parte.

Respecto a nuestros proveedores, estamos en la misma posición que nuestros clientes con nosotros. Debemos exigirles lo mismo que nos exigimos a nosotros mismos con nuestros clientes: unas medidas de seguridad informática suficientes y un tratamiento de nuestros datos acorde a la legislación vigente.

Todas las empresas contratan servicios con terceros, fundamentalmente porque no pueden tener contratado un especialista en todas las áreas que son necesarias para gestionar la actividad empresarial.
Por ejemplo:

- El asesoramiento laboral, jurídico o fiscal.
- El proveedor de informática: sistemas/comunicaciones internas, copiadoras, …
- El proveedor de comunicaciones: voz, datos e internet.
- Y dependiendo de nuestra actividad, nos relacionaremos con otros muchos proveedores.

Por otro lado, cada vez es más frecuente la contratación de servicios cloud (en la nube) para alojar nuestras máquinas o nuestros datos. Dependiendo de que sólo contratemos la infraestructura o nos presten un servicio completo de gestión y administración, deberemos exigirles por contrato que cumplen la ley y que tengan implementadas las medidas de seguridad necesarias para garantizar nuestra actividad o para recuperarla en caso de un incidente.

Con todos ellos, clientes y proveedores, debemos sentarnos a discutir los términos de nuestra relación y cómo nos afecta mutuamente la tecnología con la que nos comunicamos, para garantizar que no surjan problemas operativos o legales para ambas partes, cada uno en su rol oportuno.
Respecto a ese cumplimiento legal o legislativo que comentamos, el pasado 25 de mayo se comenzó a aplicar el Reglamento General de Protección de Datos europeo, que ya estaba en vigor desde el 27 de abril de 2016. Este nuevo reglamento tiene especial impacto en las relaciones que tenemos con nuestros proveedores y clientes y viene a unificar criterios en todos los estados miembro, prácticamente sustituyendo a las normativas nacionales que estaban vigentes en cada estado. En nuestro caso, la Ley Orgánica de Protección de Datos (LOPD).

Según los últimos informes publicados, el 65% de las empresas no están preparadas para cumplir con el RGPD, a pesar de que han tenido dos años para adaptarse.

¿Por qué debes cumplir con el RGPD?

- En primer lugar, porque es de obligado cumplimiento, independientemente del tamaño de la empresa.
- En segundo lugar, porque las sanciones pueden llegar al 4% de nuestra facturación, en casos muy graves.
- En tercer lugar, porque no puedo exigirle a un cliente o proveedor que proteja mi información si yo no me molesto en proteger la suya.
- En cuarto lugar, porque el pasado 10 de abril, la Agencia Española de Protección de Datos, informó de que tenía abierta su sede electrónica para que, empresas y administraciones públicas, obligatoriamente informen de quien va a ser su Delegado de Protección de Datos.
- En quinto lugar, porque implementar las medidas de seguridad activa que propone el reglamento nos va a hacer trabajar de una forma más segura minimizando el riesgo de sufrir un incidente o ciberincidente.

Que no se te olvide: la protección de datos personales según el RGPD no sólo sirve para evitar sanciones, sirve para conseguir una ventaja competitiva ante la competencia.

Evidentemente hay una diferencia importante entre una gran empresa y una pyme a la hora de implementar las medidas exigidas, sin embargo, como hemos dicho antes, es de obligado cumplimiento para todos y, mientras que las grandes empresas llevan años tratando los datos acorde a la ley, más o menos, las pymes están a años luz. Como dicen algunos, no están maduras. Y el problema está en que vamos a tener que madurar a una velocidad de vértigo.

El punto de inflexión va a darse en el momento en el que se empiece a sancionar a las empresas.

La propia directora de la Agencia, **Mar España**, lo ha dejado claro en sus recientes intervenciones, indicando que no habrá ningún tipo de moratoria a este respecto, por lo que a partir del 25 de mayo todas las organizaciones debemos cumplir con el Reglamento y estar en condiciones de demostrarlo. Es más, ha indicado que los planes de inspección de la Agencia van a focalizarse en tres sectores concretos: salud, instituciones financieras y empresas de telecomunicaciones, comenzando inmediatamente a la fecha de obligada aplicación, es decir, a partir del 25 de mayo.

2. RIESGOS EN LA RELACIÓN CON PROVEEDORES.

Tenemos que tener en cuenta que, en España, un país en el que más del 95% de las empresas son pymes, y de estas en un porcentaje similar son micropymes y profesionales, por lo general tenemos una economía de pequeñas empresas prestando servicios a empresas pequeñas.

Este modelo económico plantea problemas sobre todo en las épocas de crisis como las que estamos padeciendo (y digo padeciendo porque todavía hay muchas empresas que no han acabado de superar la crisis), por la imposibilidad de mantener las plantillas, lo cual afecta negativamente al servicio que prestamos o nos prestan.

La gestión de riesgos permite controlar la incertidumbre que afecta a una amenaza. Para ello identificamos, evaluamos y tratamos esos riesgos y valoramos el impacto de la exposición a una amenaza, junto a la probabilidad de que esta se materialice.

Para evitar riesgos, debemos estar muy atentos a si los servicios que contratamos los recibimos con una calidad suficiente. Debemos evaluar a nuestros proveedores periódicamente ya que una parte importante de nuestro éxito depende directamente de ellos.

Por ello, debemos acostumbrarnos a gestionar a los proveedores más allá de la firma del contrato:

- Si un contrato estándar no se ajusta a nuestras necesidades debemos negociar contratos y SLAs (acuerdos de servicio) alineados con nuestros intereses y necesidades.

- Evaluar el servicio que recibimos periódicamente, para:
    - Minimizar los riesgos de seguridad evitando así:
        - Por un lado, sanciones.
        - Por otro, que seamos incapaces de prestar nuestros servicios, lo que provocaría, aparte de pérdidas económicas, que nuestra reputación e imagen se vean afectados de cara a nuestros clientes.
    - Evitar robos o fugas de información.
    - Tener la capacidad de respuesta necesaria en aquellos excesos puntuales de demanda de trabajo.

Cuando nuestros servicios se apoyan en proveedores cloud debemos asegurarnos de que cumpla la ley e implemente medidas de seguridad activas: seguridad física y lógica, backups, monitorización de sus sistemas, …

Ten en cuenta que, aunque hayamos alquilado la infraestructura, soy el responsable de su seguridad, bien porque la gestione yo o porque hayamos externalizado esa gestión en el proveedor, en cuyo caso debo estar vigilante para que el proveedor cumpla sus contratos y SLAs y no nos ocasione alguno de los perjuicios que ya hemos comentado. Por lo tanto:

- Debemos definir nuestras medidas de seguridad y los riesgos que somos capaces de asumir y los que debemos evitar.
- Siempre que sea posible debemos conocer las instalaciones donde van a prestarnos el servicio.
- Debemos exigir que nos presenten periódicamente informes en los que se haga referencia a la eficacia de los controles implementados.

3. ACUERDOS CON PROVEEDORES Y COLABORADORES.

Debemos integrar a nuestros proveedores en el desarrollo de nuestras operaciones. Una estrecha colaboración con nuestros proveedores nos permitirá minimizar riesgos y optimizar costes y plazos. Para ello emplearemos cuatro directrices básicas que nos permitan definir la relación con y reforzar la estrategia:

- Externalización de aquellos servicios que no estén en el core de nuestro negocio.
- Rodearnos de los mejores nos permitirá ser mejores y estar más cerca de conseguir la tan ansiada diferencia competitiva con nuestra competencia.
- Siempre que se pueda es mejor tener al proveedor cerca. La colaboración se vuelve más estrecha.
- Integración de los proveedores en nuestras operaciones diarias. Implicarles en nuestra operativa permitirá generar sinergias beneficiosas para ambas partes.

Por otro lado, como indicábamos anteriormente, no debemos conformarnos con un acuerdo estándar si no se ajusta a nuestras necesidades. En estos contratos debemos incluir cláusulas que hagan referencia a:

- Acuerdos de Confidencialidad, es decir, el compromiso que debe adquirir el proveedor de no difundir la información a la que haya tenido acceso durante la prestación de su servicio, llegando incluso a exigirles cláusulas de Propiedad Intelectual si fuera necesario.
- Que la información esté cifrada, tanto mientras se encuentra en sus equipos como cuando está en tránsito. Este es un requisito del nuevo RGPD para empresas de determinados sectores.
- La protección de datos personales.
- Penalizaciones por incumplimientos del contrato.

4. USO SEGURO Y RESPONSABLE DEL CORREO ELECTRÓNICO Y SERVICIOS DE MENSAJERÍA INSTANTÁNEA.

Como indicábamos en la introducción, prácticamente toda nuestra relación con nuestros proveedores y clientes es digital.

Para comunicarnos con ellos utilizamos tanto el correo electrónico como herramientas de mensajería instantánea como WhatsApp.

Precisamente 3 servicios vulnerables y habitualmente utilizados para atacarnos desde el exterior. Probablemente sean el principal vector de ataque en la actualidad, ya que al igual que la comunicación evolucionó desde un correo postal tradicional a los mensajes electrónicos, las estafas y engaños también lo han hecho, aprovechándose de usuarios ingenuos o con escasa concienciación en ciberseguridad.
En todos los casos debemos utilizar servicios diferentes en el ámbito personal y en el ámbito profesional. Mezclar estos ámbitos nos puede crear más de un dolor de cabeza.

Tipos de problemas que aprovechan de estas tecnologías:

- Hoax o falsas noticias.
- Estafas.
- *Spam*: **mensajes masivos, anónimos y no deseados.**
- Phising.
- Distribución de Malware.
- Y un larguísimo etc …

Respecto al uso del correo electrónico como medio de transmisión en campañas de email marketing, hay que tener mucho cuidado:

- En primer lugar, suelen tener muy bajo rendimiento porque la mayoría de la gente no lee emails publicitarios.
- En segundo lugar, porque nuestro correo podría ser considerado como spam y esto podría provocar que nuestro correo no llegará sus destinatarios al ser bloqueado por los filtros antispam:
    - Filtros Bayesianos.
    - Listas negras.
    - Filtros challenge/response.
    - Filtros firewalls.
    - Filtros que se basan en la reputación del dominio desde el que se envían.
    - …

Hay informes que dicen que más del 75% del correo que se envía a diario es correo basura. Teniendo en cuenta la gravedad del asunto y la facilidad con la que el spam puede ocasionarnos serios problemas, no dejan de surgir herramientas para combatirlo. Una de las más utilizadas es el spam score, uno de los tests de spam más potentes del momento.

Los filtros antispam condicionan el spam score y podrían ser detenidos antes de llegar a su destinatario si el índice que asigna a nuestros correos es alto, al ser marcados como maliciosos.

Esto puede provocar un problema muy serio, ya que podría impedir que nos comunicáramos a través del correo electrónico durante una temporada, y de difícil solución a corto plazo.

Para envíos masivos de correos se utilizan otros sistemas.

Por otro lado, una buena concienciación, de nuestro personal, sobre el uso correcto de estas herramientas de comunicación nos permitirá evitar que los ciberdelincuentes los utilicen para perjudicarnos:

- Debemos ser capaces de identificar correos maliciosos.
- No dejarnos engañar por phishing.
- No responder a mensajes que puedan ser spam ni hacer click en enlaces que desconozcamos.
- No descargar archivos adjuntos recibidos desde correos electrónicos de desconocidos.
- Utilizar contraseñas seguras y cambiarlas con cierta periodicidad.
- No enviar correos en cadena.
- Usar sistemas de seguridad como antivirus y antispam para correo electrónico.
- En definitiva, usar el sentido común.

Respecto a las herramientas de mensajería instantánea, también hay que tener mucho cuidado. Nuestros smartphones se pueden infectar de una forma muy sencilla a través del envío de imágenes o archivos que recibimos, sobre todo, por WhatsApp. Una vez infectado el smartphone, no tardaremos mucho en enchufarlo un día al ordenador o portátil para cargar porque se está quedando sin batería y, en ese momento se infectará el ordenador.

A efectos de la normativa de protección de datos, el Grupo de trabajo del artículo 29 (GT 29) ha llegado a la conclusión, a través de una carta emitida el pasado mes de octubre de 2017, de que Whatsapp no puede recabar el consentimiento de los usuarios a través de una casilla ya marcada por defecto para ceder nuestros datos personales a Facebook. Esto se debe a la ambigüedad de los términos y condiciones que utiliza, los cuales hacen que la forma de prestar el consentimiento sea totalmente contraria a lo establecido en el nuevo Reglamento General de Protección de Datos (RGPD).

Podríamos llegar a decir que WhatsApp se ha olvidado de todo aquello que tiene que ver con una “manifestación de voluntad, libre, inequívoca, específica e informada”. No sólo porque la casilla

aparece premarcada, sino porque no informa de los datos personales que se cederán ni tampoco de su finalidad.

En definitiva, para las autoridades de control de protección de datos, WhatsApp no cumple los requisitos de consentimiento e interés legítimo en la cesión de datos a Facebook con su política de "take it o leave it" ("lo tomas o lo dejas").

El GT29 está formado por un representante de la autoridad de protección de datos de cada Estado miembro de la Unión Europea, el Supervisor Europeo de Protección de Datos y la Comisión Europea.

Socios del proyecto

Associação Empresarial do Alto Tâmega (ACISAT) *http://acisat.pt*

Câmara de Comercio de Zamora *http://www.camarazamora.com/*

Instituto Politécnico de Bragança (IPB) *https://portal3.ipb.pt/index.php/pt*

Diputación de Ávila https://www.diputacionavila.es/

Más información del proyecto:

Web: http://competic-poctep.com

Email: info@competic-poctep.com

Parque Tecnológico de Boecillo

C/Luis Proust 17

47151 Boecillo – Valladolid