1. Cumplimiento normativo

Definición y alcance de la ciberseguridad

# 1. Seguridad

* **fisica**

**Protege la organización frente a:**

* **accesos no autorizados**
* **ataques físicos a equipos e instalaciones**

**Finalidad: Proteger los bienes y recursos que tiene una organización.**

* **logica**

**Protege la información en su uso:**

* **Limita el acceso a programas o ficheros (dota privilegios a los usuarios)**
* **Gestiona la autorización de los usuarios en el acceso a la información**
* **Controla la información que entra y sale del sistema de información**

**Finalidad: Proteger de cómo los empleados o usuarios van a estar utilizando la información bajo una serie de reglas y consideraciones.**

**2. Ciberseguridad:**

**Conjunto de medios y técnicas para proteger de ataques maliciosos, a PC 's , servidores, redes y datos.**

**Seguridad lógica + Protección de Ataques**

**Datos: el activo más importante que tiene actualmente una organización.**

**Finalidad: Desarrollar acciones y normas que minimicen riesgos de un ataque:**

* **A la infraestructura que soporta la información**
* **A los usuarios que explotan la información**
* **A la información --> principal activo de las organizaciones.**

# **Protección de la Información**

**1. Las salvaguardas o controles de ciberseguridad.**

**Son las medidas que se aplican en una organización y materializan las dimensiones de seguridad de la información.**

**Los controles afectan:**

* **al personal técnico de la organización**
* **a los empleados (concienciación)**
* **a la organización de la empresa**

**2. Factores previos a la elección de controles.**

**Cuando se va a elegir un control, hay que buscar un equilibrio entre coste-beneficio y la usabilidad.**

***Por ejemplo*: no se puede arrancar una máquina y tener que pasar por 10 autenticaciones, por lo que hay que partir de la premisa que no hay que molestar para trabajar.**

**Para la elección de los controles a aplicar se debe tener en cuenta:**

**1. Identificar y clasificar los activos de información:**

**No todos los activos tienen la misma importancia, por lo que se estudiará dónde poner los mayores esfuerzos.**

**Los activos más importantes son aquellos de los que depende el negocio de la organización.**

**2. Determinar la naturaleza de los controles a aplicar:**

* **Controles técnicos y procedimentales**
* **Controles organizativos: determinar los responsables de los activos**
* **Controles de ámbito legal: cumplimiento de la LOPDGDD (*Ley Protección de Datos y Garantía de Derechos Digitales*)**
* **Controles físicos: ubicación y vigilancia de los equipos**

**3. El coste de las salvaguardas:**

**Valorar el coste económico y humano --> no sólo el dinero sino cuántas personas están involucradas en mantenerlo, gestionarlo y que funcione correctamente**

**Si el coste es superior al impacto --> buscar una alternativa más económica.**

**Las salvaguardas deben tener un coste inferior al valor del activo.**

**3. Controles básicos a implantar:**

**Se derivan de la política de seguridad, que está plasmada en el documento que realiza el responsable de seguridad en donde se determina cómo se aplican los diferentes niveles de seguridad en la empresa y serán de obligado cumplimiento para toda la organización.**

* **De acceso a la información**
  + **Utiliza el principio del mínimo privilegio.**
  + **Los empleados sólo acceden a la información para desarrollar su actividad laboral**

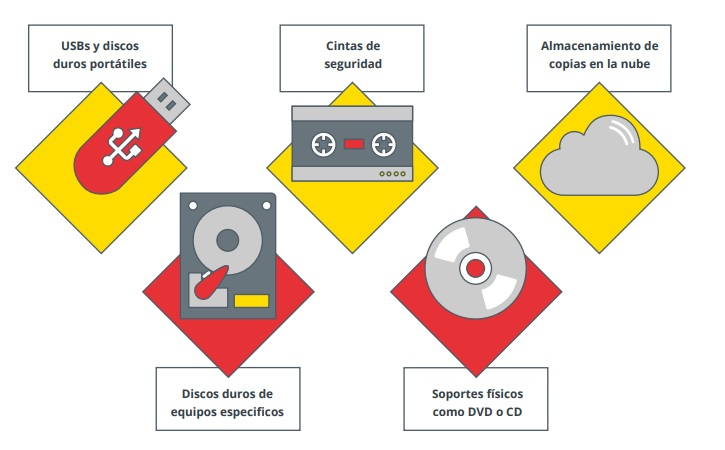
****

****

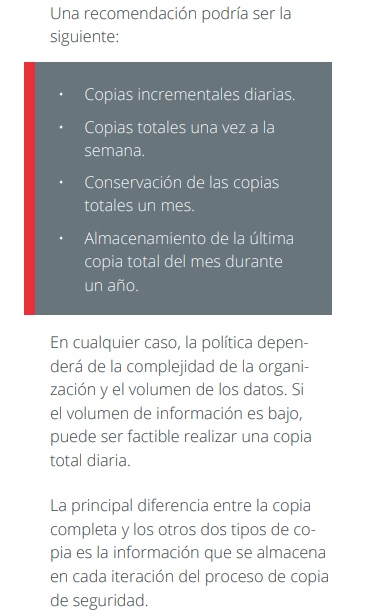
* **Copias de seguridad**

**Supone elaborar un procedimiento de copias de seguridad periódicas.**

**Los empleados/as o usuarios/as deben realizar el procedimiento según se lo indiquen.**

****

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

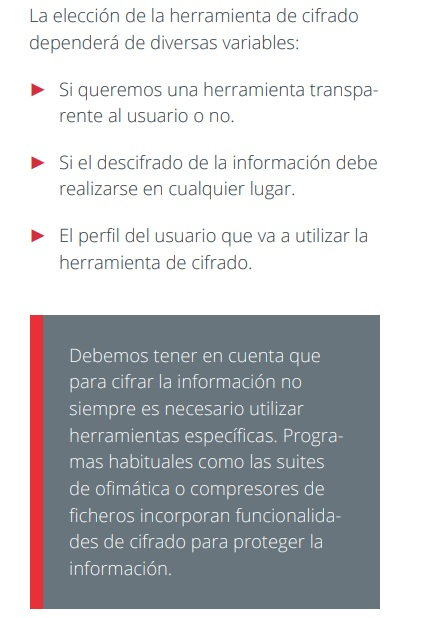
****

* **Criptográficos**

**Permite que la información sea accesible sólo por el personal autorizado.**

**Se aplica a la información sensible, almacenada en un servidor, cifrada y en tránsito.**

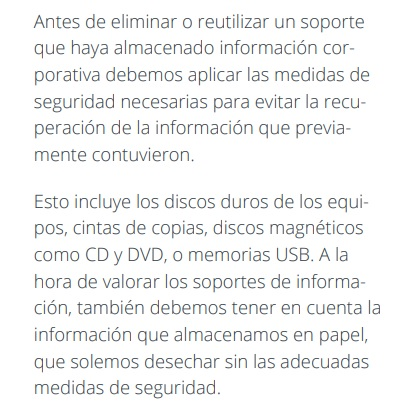
**Ejemplo: nuevos desarrollos, prototipos, datos importantes para el negocio, etc...**

****

* **Borrado seguro**

**Finalizado el ciclo de vida de la información, ésta debe ser destruida de forma segura.**

**Evita que otra persona pueda recuperarla.**

****

**La mejor opción es la destrucción física del soporte, nos asegura que no será posible recuperar la información.**

* **Almacenamiento**

**Supone establecer un procedimiento en la empresa, para no caer en el error en que cada empleado/a tenga la información en su máquina.**

**Si se decide en la nube, hay que especificar las acciones permitidas, bajo qué circunstancias, quiénes acceden,....**

**Almacenamiento en la nube:**

**Sus características básicas son la transparencia para el usuario y el acceso remoto desde cualquier lugar y dispositivo.**

**Proporciona varias ventajas:**

**- Reduce la necesidad de inversión en infraestructura propia.**

**- Permite delegar en terceros algunos aspectos que no forman parte de nuestro núcleo de negocio, como las copias de seguridad, su disponibilidad o la implantación de medidas de  
 seguridad. (Acuerdo de servicios con proveedores con penalización si existe incumplimiento).**

**- Si contratamos este tipo de servicio para el almacenamiento para datos de carácter personal, seguimos siendo responsables del tratamiento de los mismos y debemos cumplir lo especificado por la legislación de protección de datos.**

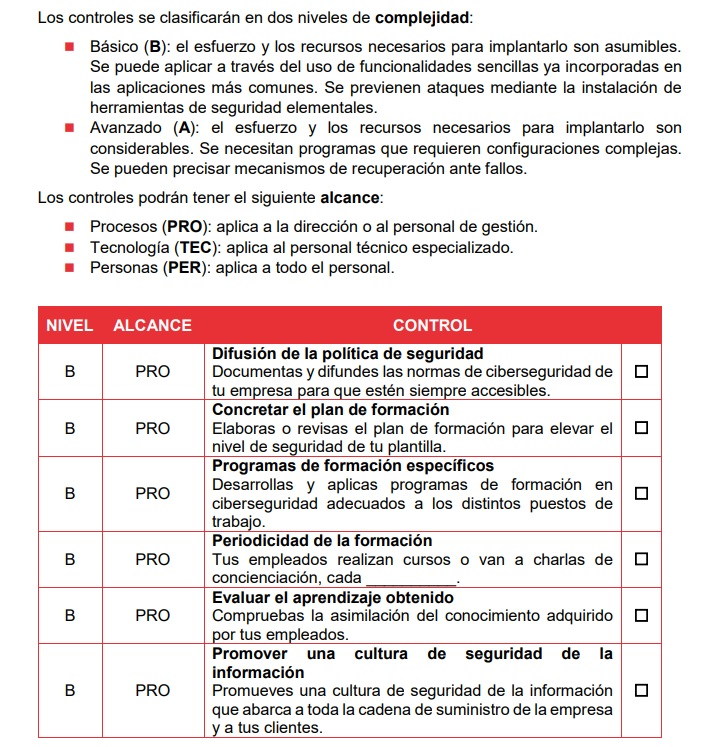
**- Existen servicios que permiten cifrar la información antes de "subirla a la nube", con las claves del servidor, a las que el usuario no tiene acceso para evitar que el proveedor o un atacante que comprometa la plataforma cloud tengan acceso a ella.**

**- Formacion y concienciación**

**Dirigida a los empleados y empleadas de la empresa.**

**Son el eslabón más importante y más débil de la cadena de seguridad.**

**Es necesario que los empleados y empleadas conozcan y apliquen buenas prácticas en el uso de todo tipo de dispositivos (de escritorio, portátiles, móviles, pendrives,…) y soluciones tecnológicas (página web,  
servicios en la nube, redes sociales, correo electrónico,…) para lo cual se debe proporcionar formación en ciberseguridad adecuada a su puesto, ya que de este modo se pueden prevenir la mayoría de los incidentes.**

* **La formación debe ser una actividad continua que ha de repetirse y revisarse periódicamente, para que surta su efecto preventivo de incidentes y esté adaptada a las nuevas tecnologías que inevitablemente iremos utilizando.**
* **Ejemplo de informe detallando los controles para revisar el cumplimiento de la política de seguridad:**
* ****

# Concienciación en Ciberseguridad

## Actividades de concienciación en la empresa.

Los protagonistas de la seguridad son los usuarios y usuarias finales, que gestionan y utilizan los sistemas de información de la organización, explotan toda la información de la organización.

Los empleados y empleadas son la primera línea de defensa contra la ciberdelincuencia, por lo que es vital que estén equipados y equipadas con todos los conocimientos y habilidades necesarias para proteger la organización.

**Objetivo:**  conseguir que tomen conciencia de los riesgos y amenazas que pueden sufrir en materia de Ciberseguridad y cómo protegerse y actuar frente a ellos.

**Actividades de concienciación:**

### El factor humano

El usuario/a es el eslabón más débil de la cadena de seguridad.

Es necesario invertir en formación y concienciación en seguridad, ya que la experiencia demuestra que es uno de los eslabones más importantes y débil de la cadena de seguridad.

**Perfiles de comportamiento frente a la seguridad:**

* Apáticos y escépticos: creen que las amenazas a la ciberseguridad están sobrevaloradas y que los mecanismo implementados inhiben su rendimiento. Como consecuencia se saltan las políticas.
* Con falta de conciencia: esperan que la empresa se ocupe de la seguridad y no asumen responsabilidad personal de protección de datos corporativos.
* Bienintencionados: tratan de cumplir las políticas de seguridad pero no lo hacen con constancia.
* Conscientes de las amenazas: son conscientes de los riegos de seguridad e intentan mantenerse seguros.

**Los empleados y empleadas deben adquirir conocimientos en ciberseguridad:**

- Que les permitan trabajar, aplicando normas de seguridad en su rutina

- Desarrollar una capacidad de respuesta ante un incidente.

### - La cultura de seguridad

Desarrollar e integrar una cultura de seguridad en la organización es complejo.

Su aplicación requiere:

- Plazos de tiempo amplios

- Y acciones continuadas en el tiempo

Finalidad: conseguir que los empleados interioricen la cultura de seguridad en sus quehaceres.

Problema: los empleados y empleadas ven los procedimientos de seguridad de la organización una complicación, un incordio o molestia. La seguridad es incómoda y dificulta sus actividades cotidianas.

Es necesario revertir esa visión negativa mediante una cultura de seguridad para garantizar el cumplimiento de la legislación y de las políticas de seguridad.

### Acciones de formación y concienciación

**Personal técnico:**  Precisa formación en materia de seguridad con un mayor grado de especialización. Se deben facilitar recursos y mecanismos para formarles en ciberseguridad, dirigida a los sistemas y aplicaciones que soportan los procesos de negocio de la organización fundamentalmente. Además este personal es asesor de los usuarios en la tecnología y su seguridad.

**Usuarios y usuarias finales:** la gran mayoría trabajan con ordenadores o dispositivos móviles que conectan desde el exterior a los sistemas corporativos. La ciberseguridad no se limita a los aspectos técnicos sino que incorpora otros ámbitos como el organizativo y el legal, si la empresa tiene como clientes a personas físicas se debe formar al empleado/a en la protección de datos de carácter personal. Además deben ser formados/as en :

- Reconocer un ataque de ingeniería social y evitarlo

- Proteger el puesto de trabajo (Antivirus, actualizaciones, correo electrónico…)

- Manejar con seguridad dispositivos móviles corporativos

- Entender los riesgos del acceso y navegación

### - Establecer una cultura de seguridad

La ciberseguridad se plasma en políticas, nomas y procedimientos. Son protocolos de actuación a seguir dentro de la organización.

Las actividades de ciberseguridad hay que formalizarlas:

- Documentando la ciberseguridad a aplicar

- Especificando lo que se puede o no se puede hacer en la organización: Incluir los usos permitidos de los recursos corporativos y las sanciones a aplicar.

Las normas y procedimientos se derivan de **Política de Seguridad:**

* Recoge los objetivos de la organización en ciberseguridad
* Debe ser formalmente aprobada por la Dirección

Aprobadas las normativas de uso de los recursos corporativos, se comunican a los empleados y empleadas para alcanzar al concienciación.

### Supervisar las buenas prácticas

Una vez definido el marco de trabajo y trasladado a las partes afectadas, Es necesario comprobar que se está aplicando.

El administrador de seguridad es el encargado de velar:

* La vigencia y actualización de las normas y procedimientos definidos, atendiendo a la detección de nuevas situaciones y cambios organizativos.
* La implantación de la normativa.
* La verificación de su cumplimiento por los empleados.

Se deben disponer mecanismos para comprobar que se siguen los procedimientos (auditorías internas o externas, herramientas que registren operaciones de los usuarios y usuarias y su trazabilidad...).

* Concienciación en ciberseguridad para empleados y directivos

**EMPLEADOS y EMPLEADAS:**

* Para que la ciberseguridad se integre en la cultura de la empresa, la Dirección debe asegurarse la implicación de los empleados y empleadas.
* Deben ser conscientes de la importancia de la información que manejan, la propia y la de terceros/as con los que hacen negocios (clientes y clientas, proveedores y proveedoras...)
* Deben conocer los riesgos a los que están expuestos/as y saber reaccionar.
* Si los empleados y empleadas no se consideran parte fundamental de este proceso, el fracaso está garantizado.

**DIRECTIVOS y DIRECTIVAS:**

* Desarrollar acciones de concienciación sobre el acceso a información de carácter sensible.
* Las acciones se deben centrar en un enfoque personalizado, considerando su problemática, su entorno de trabajo y los riesgos específicos asociados.
* Estas acciones deben adaptarse a las características del trabajo del directivo, con propuestas y medidas de seguridad para éste y su entorno.

### Técnicas de concienciación para contener incidentes

**De protección del puesto de trabajo:** consiste en realizar acciones a convertir en hábitos: bloquear el terminal, despejar la mesa, proteger las contraseñas, controlar los pendrives, destruir de forma segura lo que ya no se use...

**De prevención:** respetar los procedimientos y políticas que la empresa establece: la actualización de equipos y aplicaciones, instalación de aplicaciones, configuraciones permitidas, el uso de los navegadores, dispositivos externos en el trabajo…

**De defensa:** la fuga de información, salida no controlada de información de la empresa. Es esencial clasificar la información y seguir los procedimientos para proteger la información sensible. Sospechar de los mensajes no solicitados y lo que puedan suplantar a clientes y clientas, bancos o responsables de sistemas. No difundir datos personales y confidenciales, teniendo presente los acuerdos de confidencialidad firmados.