OFICINA Acelera pyme

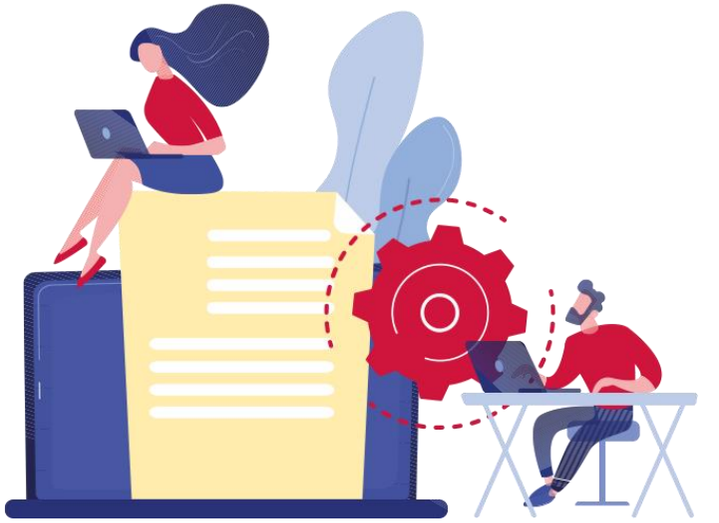
Protección de la información en las empresas

03 de maro de 2022

ISOTADER

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Índice



ISOTADER

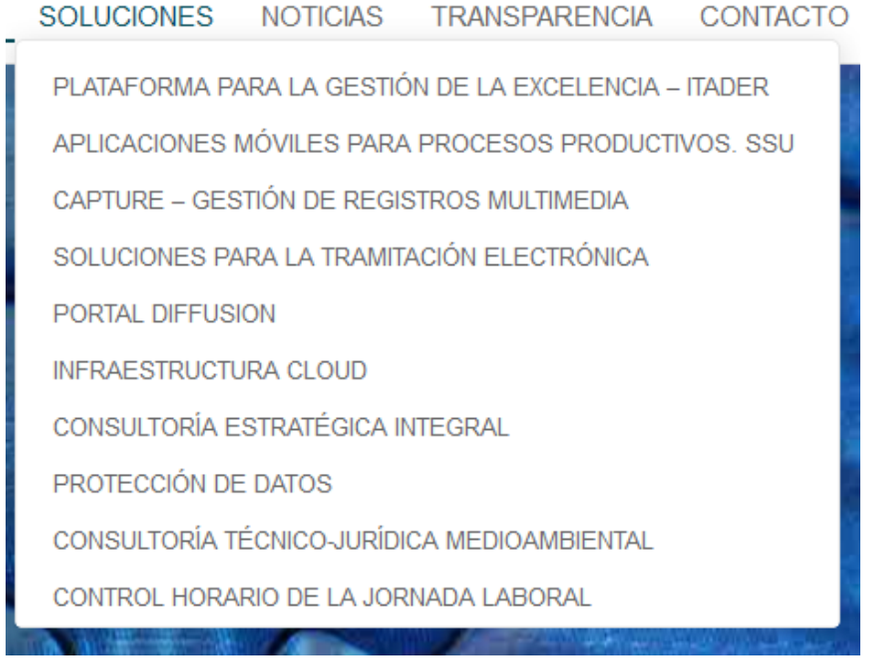
https://www.isotader.com/

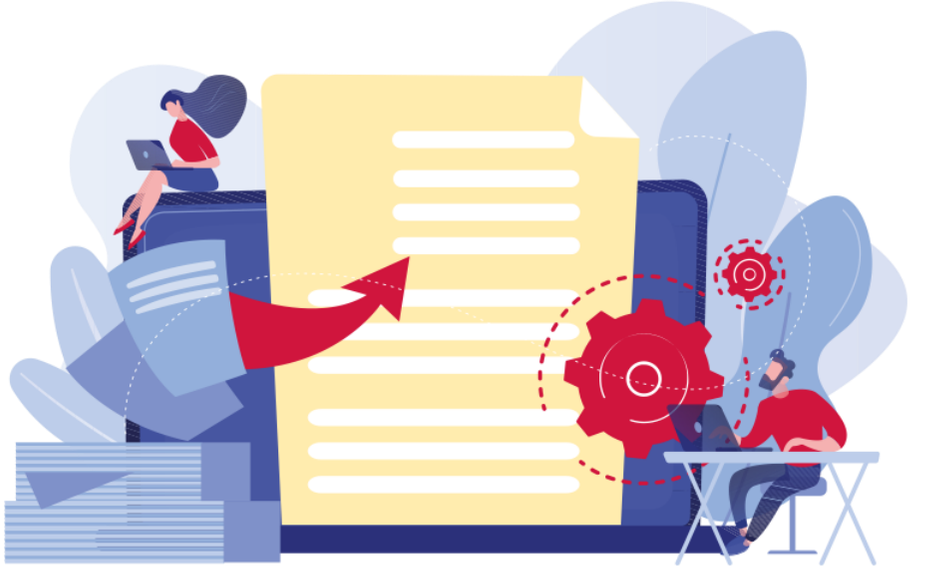
1.1 QUIENES SOMOS

ISOTADER nació hace más de una década como Isotader Calidadg. Una consultoría cuyo objetivo era cubrir las necesidades del mercado en relación con la calidad y el medio ambiente aportando soluciones informáticas. El enfoque inicial pronto fue ampliado con nuevos objetivos, alcances y actividades.

Más de DIECIOCHO años de trabajo y mejora continua han permitido a nuestro equipo diseñar y recomendar las soluciones adecuadas con el compromiso de la creación de valor para nuestros clientes. Lo que nos ha permitido desarrollar una gran tipología de proyectos así como la expansión internacional en México, Chile y Colombia.

1.2 QUÉ HACEMOS





1.2 QUÉ HACEMOS

CONSULTORÍA DE PROTECCIÓN DE DATOS LOPDGDD LEY 3/18

- **Implantación RGPD, EVALUACIÓN RIESGOS, EIPD, VIDEOVIGILANCIA, INFORMACIÓN A LOS EMPEADOS, REVISIÓN DE CUMPLIMIENTO DE LAS WEBS, etc**

ACTUAR COMO DELEGADO DE PROTECCIÓN DE DATOS

- **Apoyo al DPD interno**
- **Actuar como DPD, registrado en la AEPD**

CANAL DENUNCIAS INTERNO WISTLEBLOWING Directiva (UE) 2019/1937

- **Acceso a un canal propio en sus instalaciones o en la nube**
- **Ejecutar y gestionar los procedimientos de denuncias**

1. Introducción

Introducción

La información de nuestra empresa y constituyen uno de los activos más importantes de nuestra organización.

Es un error común pensar que en el ámbito de una pequeña empresa no es necesaria la protección de la información:

- las tarifas o las ofertas que presentamos a nuestros clientes, las cuales nos permiten posicionarnos en el mercado o frente a la competencia,
- o en nuestros planes estratégicos para el crecimiento de nuestro negocio.
- Las consecuencias que tendría la pérdida de la contabilidad de la organización,
- la cartera de clientes, la información confidencial que tenemos sobre nuestros clientes como sus cuentas bancarias
- o las propiedades intelectuales de nuestra empresa.

Todos estos ejemplos forman parte de la información de nuestra empresa, lo que la convierte en un activo vital que debe protegerse adecuadamente. Esto es lo que conocemos

como seguridad de la información.

2. Descripción del Problema

Descripción del Problema

Gracias al uso de la tecnología, el procesamiento y almacenamiento de grandes volúmenes de datos se ha vuelto muy sencillo.

En una memoria USB se podría almacenar, sin autorización para ello, una gran cantidad de información confidencial de una empresa de tamaño mediano e incluso
a través de correo electrónico se podría enviar información confidencial de la empresa como la base de datos de clientes, con fines distintos a los permitidos

Aunque la tecnología es un elemento indispensable de cualquier organización, debe utilizarse de forma adecuada para evitar riesgos en la gestión de la información. Por tanto, es de extrema
importancia que se adopten las decisiones y medidas necesarias antes de que se produzca un incidente de seguridad de la información

Los Errores más comunes en el tratamiento de la información en la empresa.

Descripción del Problema: Errores comunes

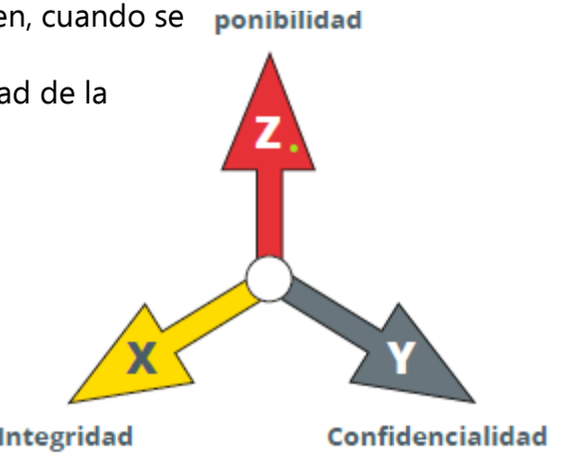
ERRORES	CÓMO EVITARLOS
Información importante de la que no se realiza copia de seguridad.	Para evitar cometer este error tendremos que asegurarnos que tenemos una copia de seguridad actualizada de la información, al menos de aquella más crítica. Y comprobaremos que sabemos y que podemos recuperarla.
Carpetas de red compartidas sin control de acceso. Usuarios que no saben dónde está la última versión de un documento. Usuarios que tras un cambio de puesto conservan acceso a información que, por el nuevo tipo de trabajo que van a desempeñar, no es necesaria.	Estos errores se pueden evitar si hacemos que la información sólo sea accesible a quien la necesita y esté autorizado para ello. Es decir implantar un **«control de accesos»**.
Presencia de discos duros portátiles sin que la organización conozca y tenga inventariados quién los utiliza y qué información pueden tener almacenada. Falta de formación de los usuarios en las herramientas que utilizan. Dejar que los empleados utilicen almacenamiento en la nube y su correo personal para actividades profesionales	Si no se **limita el uso de aplicaciones no corporativas** (correo personal, almacenamiento en la nube) y se **controla el uso de los dispositivos externos** ni los usuarios tienen la adecuada formación, cometeremos estos errores.
Tirar los ordenadores y discos a la basura sin ningún control previo de su contenido.	Tener controlados los soportes y los equipos es esencial pues algún día dejan de ser útiles, por obsoletos o por desgaste. Es el momento de deshacerse de ellos, **borrar toda la información** que tenían, de forma que no quede ni rastro de su uso previo.

3. Dimensionoes de la seguridad de la información

Dimensiones de la seguridad de la información

La seguridad de la información se articula sobre tres dimensiones, que son los pilares sobre los que aplicar las medidas de protección de nuestra información:

►► **La disponibilidad de la información,** hace referencia a que la información esté accesible cuando la necesitemos
Algunos ejemplos de falta de disponibilidad de la información son:
cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de denegación de servicio,
en el que el sistema «cae» impidiendo accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información.



►► **La confidencialidad,** implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este
término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso.
Ejemplos de falta de confidencialidad,
son el robo de información confidencial por parte de un atacante a través de Internet, la divulgación no autorizada a través de las redes sociales de información
confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener acceso.

►► **La integridad de la información** hace referencia a que la información sea correcta y esté libre de modificaciones y errores.
La información ha podido ser alterada intencionadamente o ser incorrecta y nosotros podemos basar nuestras decisiones en ella.
Ejemplos de ataques contra la integridad de la información
- son la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas por un empleado malintencionado o por error humano.
- desastres como tornados, inundaciones y tormentas, pueden ser suficientes para eliminar una empresa en cualquier lugar del mundo. Incluso, un simple incendio localizado puede destruir todos los datos si no se ha preocupado de realizar una relocalización de sus copias de seguridad en una ubicación remota.

Dimensiones de la seguridad de la información

►► Fallos y errores humanos involuntarios,

Los fallos de equipamiento e infraestructuras pueden ser otro de los ejemplos de incidentes de seguridad de la información. Se realizan casi a diario, pueden estar producidos por cortes de energía, caídas de vínculos de internet, etc.

Todas las situaciones que se puedan dar suelen tener dos cosas en común:
- La consecuencia, que es que se perderán todos los datos o no se podrá acceder a ellos.
- Este tipo de incidentes suelen darse con mucha facilidad.

La evaluación de los activos de información de la organización en relación a estas tres dimensiones ,

La evaluación de los activos de información de la organización en relación a estas tres dimensiones de la seguridad determina la dirección a seguir en la implantación y selección de medidas, también denominadas controles o salvaguardas.

También debemos tener en cuenta que la adopción de un determinado control para mejorar la seguridad en una dimensión, puede afectar de forma negativa o positiva a otra de las dimensiones, por ello, es esencial conocer cuál de estas dimensiones es más importante proteger en cada sistema de información. Por ejemplo, implantar un control de acceso para proteger la confidencialidad en un aparato médico de una sala de operaciones, puede producir un retardo en el acceso a la información afectando a su disponibilidad, lo cual no sería lo más adecuado

4. Selección de Salvaguardas

Selección de Salvaguardas

Las salvaguardas son las medidas necesarias para proteger la información de nuestro negocio.
Para la selección de estas medidas tendremos que fijarnos en los siguientes aspectos:

►► **El sector de negocio ,**
Determinar la importancia de la información que manejamos. **El sector de negocio** puede afectar a la naturaleza de la información que tratamos, en particular en lo relativo a la privacidad de los datos personales de nuestros usuarios y por la existencia de información confidencial, cuya pérdida o deterioro pueda causar graves daños económicos o de imagen a la empresa..

►► **Identificar, Clasificar y Valorar**, la información según las dimensiones de seguridad son los pasos previos que van a dirigir la selección de las salvaguardas.
Así, algunos activos de información serán muy confidenciales (estrategias, contraseñas,...), mientras que otros, como la página web o la tienda online, no podremos
permitir que no estén disponibles.

►► Tendremos también que conocer la **naturaleza de los controles** que podemos implantar. No sólo tendremos que considerar medidas técnicas como la instalación de un cortafuegos, sino que consideraremos también medidas organizativas, por ejemplo, implantar un plan de formación, establecer responsables de los activos o adaptarnos para cumplir con la legislación.

►► **El coste** de las medidas será también un factor a considerar, pues ha de ser proporcional al riesgo que se quiere evitar.

4.1 Importancia de la información para la empresa

La importancia de la información que manejamos será, en gran medida, relativa a nuestro sector de negocio,

En el **ámbito sanitario** se maneja un gran volumen de información personal de pacientes, a la que se deben aplicar todas las medidas de seguridad para evitar que se pierda, modifique o se acceda a ella sin autorización. Además suele ser necesario llevar un registro de los accesos y modificaciones.

En **sectores industriales o de desarrollo de productos** es importante velar por la confidencialidad de los procesos y procedimientos que nos pueden aportar una mejora de productividad sobre la competencia.

En **hostelería y restauración** se maneja, además de un volumen de datos de carácter personal muy significativo, información sobre reservas, cuya pérdida nos podría poner en una situación muy complicada con nuestros clientes.

En el **sector financiero** se maneja información confidencial tanto de clientes como de operaciones financieras de compras y ventas de activos cuya difusión puede suponer una importante pérdida económica o un perjuicio para nuestros clientes.

4.2 Pasos previos a la selección de salvaguardas

La clasificación de la información,

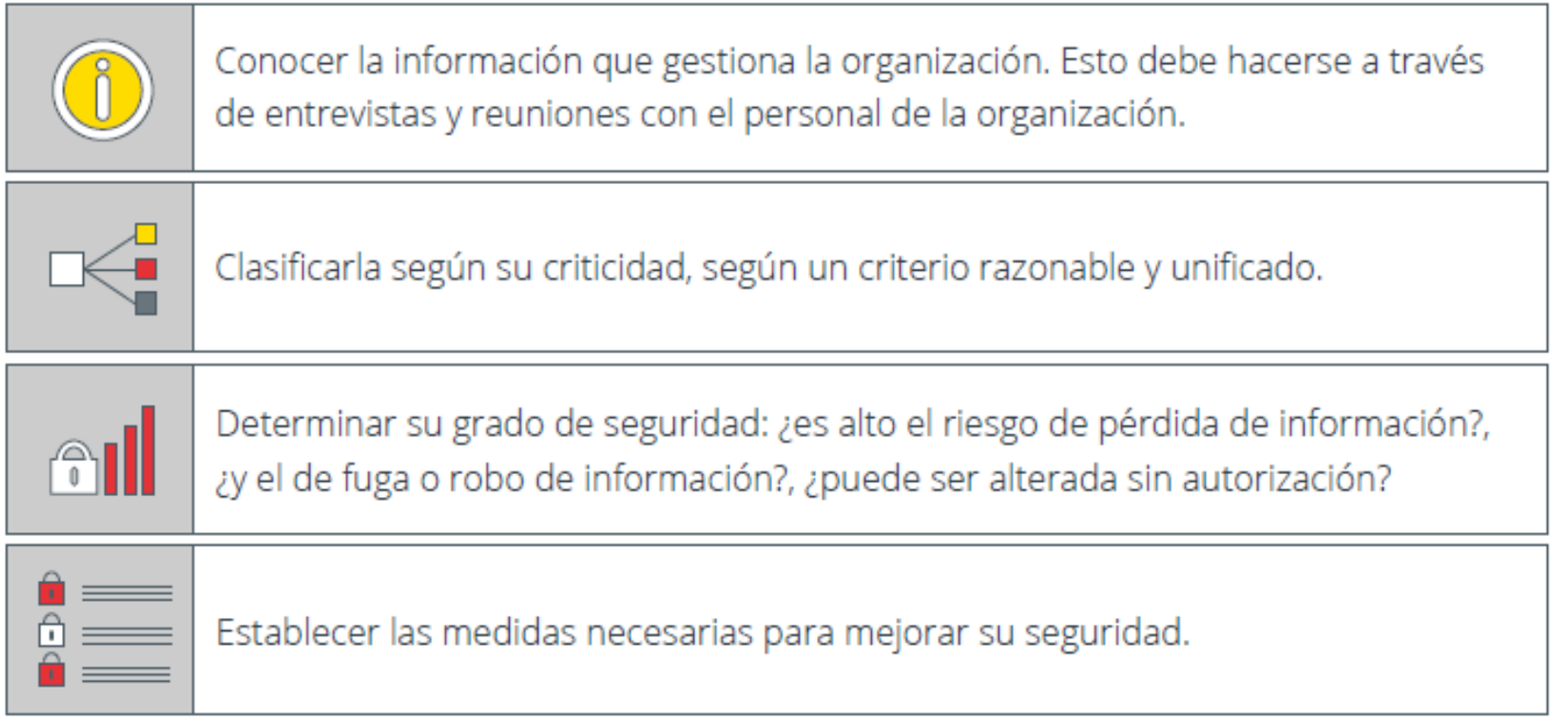
En primer lugar revisaremos qué información tratamos (bases de datos, archivos, aplicaciones, programas,…) y seleccionaremos la más crítica, la que está sujeta a la ley, la que si nos faltara, por su confidencialidad o si se corrompiera, paralizaría nuestra actividad y nos acarrearía pérdidas de imagen o económicas. En esta clasificación de la información podemos establecer varios niveles en función de su importancia para la empresa.

CATEGORÍA	DEFINICIÓN	TRATAMIENTO
Confidencial	Información especialmente sensible para la organización. Su acceso está restringido únicamente a la Dirección y a aquellos empleados que necesiten conocerla para desempeñar sus funciones. También datos de carácter personal, en particular los de categorías especiales.	Esta información debe marcarse adecuadamente. Se deben implementar todos los controles necesarios para limitar el acceso a la misma únicamente a aquellos empleados que necesiten conocerla. En caso de sacarla de las instalaciones de la empresa en formato digital, debe cifrarse. Para los datos de carácter personal, se deben tener en cuenta la protección y garantías indicadas en la legislación sobre la materia.
Interna	Información propia de la empresa, accesible para todos sus empleados. Por ejemplo, la política de seguridad de la compañía, el directorio de personal u otra información accesible en la intranet corporativa.	Esta información debe estar adecuadamente etiquetada, y estar accesible para todo el personal. No debe difundirse a terceros salvo autorización expresa de la dirección de la empresa.
Pública	Cualquier material de la empresa sin restricciones de difusión. Por ejemplo, información publicada en la página web o materiales comerciales.	Esta información no está sujeta a ningún tipo de tratamiento especial.

4.2 Pasos previos a la selección de salvaguardas

Criticidad,

Una vez hayamos clasificado y valorado la criticidad de la información, debemos determinar su riesgo específico para así enfocar las medidas a evitarlo o subsanarlo. Así, serán diferentes las medidas para evitar riesgos de fuga de información, de las necesarias para evitar que sea alterada por personas no autorizadas..
En este punto se puede realizar **un análisis de riesgos**



4.3 Naturaleza de los controles

Naturaleza

Otro aspecto importante a considerar en la selección e implantación de controles es su tipología o naturaleza. Ésta puede ser:

- **Técnica:** medidas de carácter tecnológico dentro del ámbito de la seguridad. Son medidas técnicas: antivirus, cortafuegos o sistemas de copias de seguridad.
- **Organizativa:** medidas que se centran en la mejora de la seguridad teniendo en cuenta a las personas, por ejemplo: **formación** en seguridad, identificación de **responsables** o implantación de **procedimientos** formales de alta y baja de usuarios.
- **Física:** medidas físicas para proteger nuestra organización. Como por ejemplo, acondicionar adecuadamente la sala de servidores frente a riesgos de incendio, inundaciones o accesos no autorizados, establecer un sistema de control de acceso para entrar en las oficinas, poner cerraduras en los despachos y armarios o guardar las copias de seguridad en una caja ignífuga.

4.4 Resumen de criterios de selección

El coste de la implantación de la medida de seguridad.

- Coste económico de la medida.
- Coste en el tiempo y recursos humanos empleados.
- Coste de las posibles medidas alternativas.
- Coste de las pérdidas económicas que supondrías no tener implantada la medida.

La importancia de cada sistema de información en la organización.

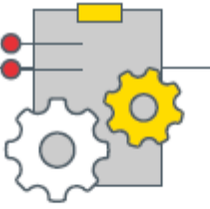
- Identificar los activos más críticos e importantes a proteger.
- Contemplar las particularidades de cada sector de negocio.

Ámbito sanitario

Ámbito financiero

Ámbito industrial

Ámbito hostelería



Las necesidades de cada sistema de información.

-Determinar cuál de las dimensiones de seguridad, confidencialidad, integridad o disponibilidad es más importante proteger.

5. Salvaguardas básicas

5.1 Control de Acceso a la información

Por defecto, toda organización debe **seguir el principio del mínimo privilegio**. Este principio se traduce en que un usuario sólo debe tener acceso a aquella información estrictamente necesaria para desempeñar sus funciones diarias. Para conseguir este objetivo, previo a la implement

Asignar permisos individualmente a cada usuario puede ser un método más flexible pero con mayor dificultad de gestión a medida que el número de usuarios crece.

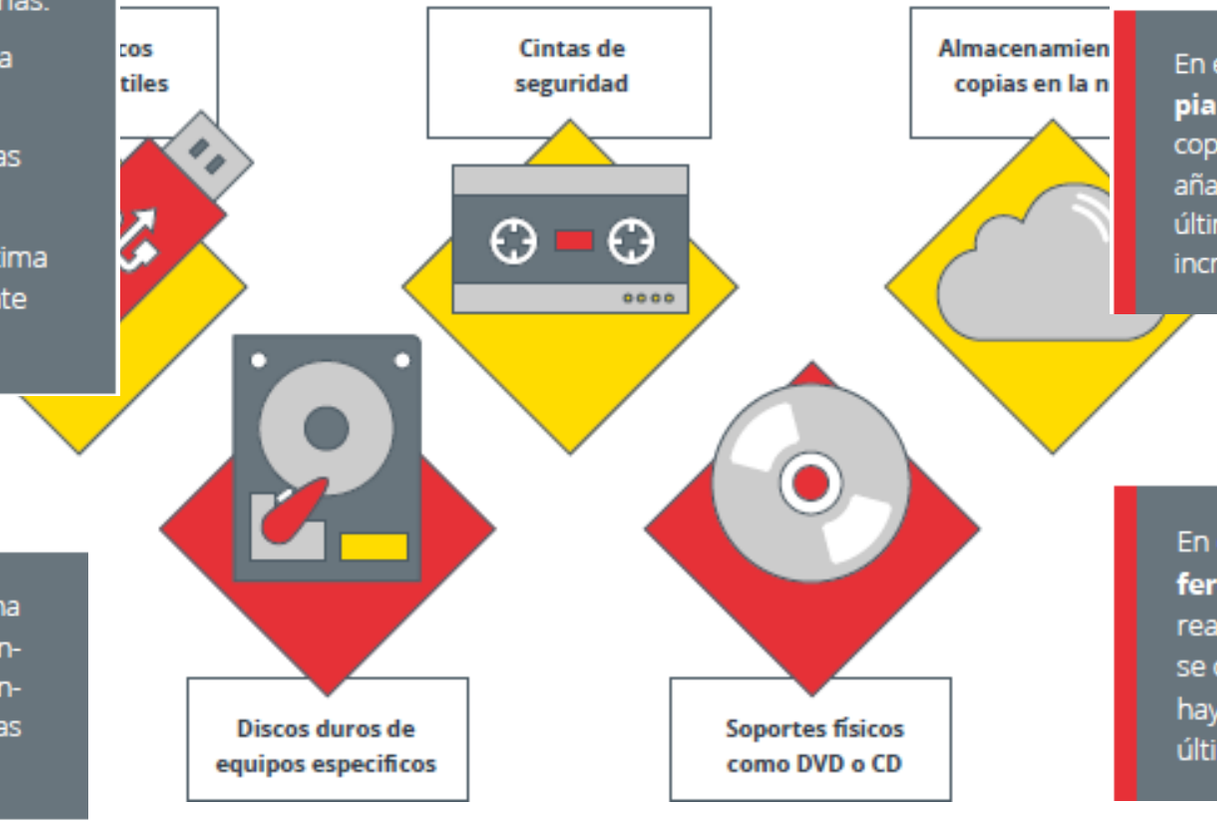
	PERFILES DE LA INFORMACIÓN				
	Personal de administración	Personal de informática	Perso opera		
Servidor	✓	✓	✓		
Pedidos	✓	✓	✗	✗	
Almacén	✓	✓	✗	✗	
	✓	✓	✗	✓	
	✗	✗	✗	✓	✗

Si optamos por asignar permisos según perfiles de usuario, será necesario llevar a cabo un mayor trabajo inicial para determinar a qué accede cada perfil y qué perfil tiene cada usuario, pero tras esta tarea inicial, la gestión de permisos es más rápida y eficiente, permitiendo una trazabilidad completa de los accesos de cada empleado.

5.2 Copias de seguridad

- Copias incrementales diarias.
- Copias totales una vez a la semana.
- Conservación de las copias totales un mes.
- Almacenamiento de la última copia total del mes durante un año.

El primer pas
los sistemas y
configuracione
en smartphones



En **la copia total**, se realiza una copia completa y exacta de la información original, independientemente de las copias realizadas anteriormente.

En el caso de los sistemas de **copia incremental**, únicamente se copian los archivos que se hayan añadido o modificado desde la última copia realizada, sea total o incremental.

copia, así como
aspectos como las

En el **sistema de copias diferenciales** cada vez que se realiza una copia de seguridad, se copian todos los archivos que hayan sido modificados desde la última copia completa.

Deben hacerse pruebas de restauración periódicas, para garantizar que no se producirán problemas en caso de necesitar recuperar la información. Esto es especialmente importante si no se solicitan restauraciones con frecuencia. Los sistemas de copia o los soportes pueden fallar
y es fundamental detectarlo antes de que sean necesarios.

5.3 Cifrado de información

El cifrado consiste en ofuscar la información mediante técnicas de codificación, evitando que los datos sean legibles por cualquier persona que desconozca la clave de decodificación. Estas técnicas son la mejor opción para el almacenamiento y transmisión de información sensible, especialmente a través de soportes
y dispositivos móviles, ya que:

- **permiten controlar el acceso a la información;**
- **limitan la difusión no autorizada en caso de pérdida o robo de soportes.**

Sin embargo, hay que tener en cuenta una serie de aspectos:

- la clave debe ser robusta para que dificultar el acceso no autorizado a la información;
- la pérdida de la clave de acceso imposibilita el acceso a la información;
- cuando ocurre un error físico no es posible la recuperación de la información, indepe a o no.

Debemos tener en cuenta que para cifrar la información no siempre es necesario utilizar herramientas específicas. Programas habituales como las suites de ofimática o compresores de ficheros incorporan funcionalidades de cifrado para proteger la información.

5.4 Desechado y reutilización de soportes y equipos

Antes de eliminar o reutilizar un soporte que haya almacenado información corporativa debemos aplicar las medidas de seguridad necesarias para evitar la recuperación de la información que previamente contuvieron.

- Si vamos a **reutilizarlo, venderlo, regalarlo o prestarlo**, debemos realizar un **borrado seguro** del soporte. Es frecuente pensar que el borrado de la información o el formateo del disco duro elimina los datos, cuando no es cierto. Al eliminar archivos utilizando la función suprimir habitual del sistema operativo, éste se limita a marcarlo como eliminado. Pero los datos no han sido eliminados realmente. Siguen estando en el disco aunque el espacio que ocupaban aparezca como disponible. Y seguirán estando ahí hasta que nuevos datos ocupen esa zona de memoria.

Existen multitud de herramientas que nos permiten borrar de forma segura los dispositivos. Estas herramientas de borrado seguro, además de marcar el espacio como vacío, escriben en él datos aleatorios un número determinado de veces. De este modo, si se intenta obtener el contenido anterior del disco duro lo que se encontrará serán datos aleatorios y no la información original.

En general, la mejor opción es la **destrucción física del soporte**. Para los soportes menos robustos (CD/DVD, papel) podemos utilizar una destructora de papel (o de soportes magnéticos). Para otros medios, podemos optar por una destrucción manual o recurrir a empresas especializadas en la destrucción certificada de información.

- Si por el contrario vamos a **desechar el soporte**, debemos garantizar que nadie puede utilizarlo posteriormente, y que la información que contiene no puede ser recuperada. Los soportes se pueden desechar por múltiples motivos, como pueden ser mal funcionamiento, poca capacidad, antigüedad o porque ya no es útil

5.5 Almacenamiento en la nube

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. Estos aspectos se controlan mediante los acuerdos de servicio con los proveedores que suelen incluir penalizaciones en caso de incumplimiento.

RIESGOS

▶▶ No debemos utilizar servicios en la nube sin haber **estudiado detenidamente las condiciones de uso** en lo referente a las garantías de disponibilidad y confidencialidad de la información. Debemos informarnos sobre dónde acudir en caso de fallo del servicio, medidas de protección de la información, o los tiempos de indisponibilidad permitidos por contrato.

▶▶ Se debe **evitar el uso sin control de estos servicios por parte de los empleados**, mediante una política corporativa y medidas técnicas. El uso de estos entornos dificulta o imposibilita el control sobre la información que se almacena en el servicio, ya que las medidas de seguridad (control de acceso, claves utilizadas, registro de accesos) no están bajo el control de nuestra organización.

▶▶ En caso de manejar los datos de carácter personal, en particular si son datos especialmente protegidos, debemos tener en cuenta que **tendremos que firmar con nuestros proveedores en la nube contratos de tratamiento de datos de conformidad con el RGPD**

▶▶ Intentar **evitar servicios en la nube que sean gratuitos**. Cuando algo es gratuito, **el producto somos nosotros**, o nuestra información. Los servicios gratuitos en la nube ofrecen a menudo acuerdos de nivel de servicio inflexibles o con cláusulas ambiguas que no dejan nada claro cuáles son las medidas de seguridad que utilizan o la responsabilidad del proveedor.

5.6 Confidencialidad en la contratación de servicios

:Cualquiera de estos servicios es susceptible de ser externalizado: creación de las copias de seguridad, almacenamiento en la nube, destrucción física de soportes, mantenimiento informático, etc. Sin embargo, esta **externalización** puede introducir nuevos riesgos para la seguridad de la información, derivados del acceso del proveedor a los datos.

Una medida que mitiga (pero no elimina) este tipo de riesgo es la **firma de contratos de confidencialidad o inclusión de este tipo de cláusulas en el contrato de servicio.** Esto compromete al prestador del servicio a no hacer un uso fraudulento de los datos, y adquiere especial relevancia si se externaliza la gestión de datos de carácter personal ya que este acuerc

6. Buenas prácticas

Buenas prácticas: recomendaciones de seguridad y protección de datos

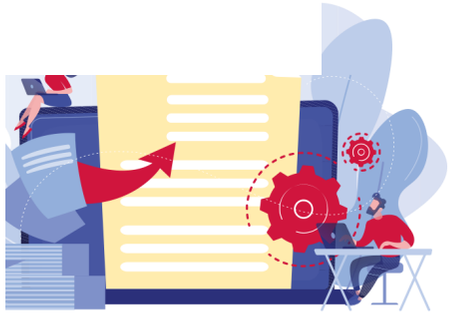
1- Actualización de los sistemas
Invierta tiempo suficiente en el mantenimiento de los sistemas para que se mantengan siempre actualizados. La aplicación Patch es simple y eficaz en la protección de la red corporativa.

2- Limitación a los usuarios
Cada usuario del sistema debe acceder solamente a aquello que requiera. ¿Para qué dejar toda la red abierta a personas que no necesitan tener acceso a documentos estratégicos por ejemplo? Limite quién puede acceder a qué..

3- Bloqueo de sistemas de salida
De la misma forma en que es importante limitar el acceso a determinados archivos, también es necesario que haya un bloqueo de aplicaciones, programas y sistemas que permitan la salida de información de la empresa. Así como nubes públicas, en las que son posibles cargar millones de archivos en diferentes formatos.

4- Separe los archivos más importantes
Es importante distinguir en la red los datos más relevantes y estratégicos de la empresa y sobre ellos hacer una barrera diferenciada de protección. Puede ser criptografía, contraseñas o inclusive firewalls para limitar el tránsito en esa parte de la red.

5- Automatización
Utilice la automatización para atenuar tareas de seguridad, disminuyendo los errores manuales.



Buenas prácticas: recomendaciones de seguridad y protección de datos

6- Monitoreo sistemático
Es fundamental que el coordinador de la red tenga una visión general sobre lo que está pasando con todo el sistema. Asegúrese de que está realizando un barrido completo por toda el área y mantenga un monitoreo constante y sistemático

7- Normas de seguridad
Una política de seguridad consiste en permitir que administradores de la red, personal de seguridad en TI y otros técnicos puedan entender las reglas y aplicarlas en la red, colaborando también con la divulgación de éstas entre los usuarios.

8- Unificación de procesos
Asegúrese de que los equipos de seguridad están alineados con los otros equipos de la empresa ligados a las operaciones y procesos de los negocios. Todos deben saber que existen reglas, y que esas reglas son para la seguridad del negocio y que deben ser cumplidas.
Al estar todos alineados no existen disculpas futuras y existe la posibilidad de mejoras a partir de feedbacks que pueden surgir de otras áreas que no se relacionen con la TI.

9- Educar
Muchas veces los datos son robados o perdidos por pura inocencia y falta de conocimiento de un usuario. Deje claro lo que es y no permitido en las máquinas de la empresa e inclusive en las prácticas de BYOD. No porque el usuario está usando su propio dispositivo hará lo que entienda con los datos de la empresa..

10- Encuentre indicadores
Defina métricas y datos capaces de evaluar su trabajo en seguridad de la información a lo largo del tiempo. Con tan frecuentes cortes de presupuesto, poder demostrar la importancia de su trabajo es algo fundamental.

Buenas prácticas: recomendaciones de seguridad y protección de datos

.

11.- No revelar información interna, principalmente de personas físicas, a terceros no identificados o que no se encuentren debidamente autorizados.
Evitar tomar fotografías en ambientes laborales, sobre todo si se quieren compartir por redes sociales o sistemas de mensajería instantánea, ya que pueden incluir vistas de pantallas, notas u otros papeles o sistemas que revelen información sensible.

12.- Almacenar la documentación importante bajo llave, y retirar cuanto antes las impresoras compartidas la documentación que se imprima..

13.- No comparta contraseñas. Jamás deberá proporcionarlas por correo electrónico e ignore cualquier mensaje de correo electrónico que solicite cambiarlas, si no viene de personal autorizado y coincide con la gestión que acaba de realizar.
Se debe asegurarse que los sitios web en los que ingrese contraseñas o datos personales cuente con el "https" al inicio de la dirección web. De esta forma toda la información que ingrese se encontrará segura.
Utilizar los sistemas informáticos con la finalidad exclusiva de cumplir con todas las funciones de su cargo. Cualquier otro uso puede considerarse indebido y, por lo tanto, puede ponerle en riesgo.

14.- Evitar utilizar memorias flash y discos duros externos para mantener respaldos. Deben hacerse por personal especializado, en ubicaciones locales o remotas, en equipos o sistemas seguros que se dedican a dicha función

Buenas prácticas: recomendaciones de seguridad y protección de datos

15.- Evitar el uso de almacenamientos en la nube que no se encuentre expresamente autorizados por la organización. La información que se encuentra almacenada en la nube no suele estar sujeta a las mismas normas legales de su país, se encuentra expuesta a ataques las 24 horas al día, y dificulta verificar con quién fue compartida y si el acceso de terceros fue retirado cuando ya no la necesitaban.

16.- Evitar el uso de dispositivos personales que no se encuentren expresamente autorizados para almacenar o procesar datos laborales. Los dispositivos personales se encuentran mucho más expuestos a robos, extravíos y roturas, y tienen un riesgo mucho mayor de contener software malicioso.

17.- No realizar cambios en la configuración estándar de los sistemas sin autorización. Las computadoras laborales son configuradas de determinada forma para que no sean evidentes para los usuarios. Los cambios indebidos en configuración, programadas o ubicación de archivos suelen implicar riesgos y costos adicionales.

OFICINA
Acelera
pyme

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

UNIÓN EUROPEA

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"