LA INFORMACIÓN

El activo imprescindible de tu organización

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CIBERSEGURITY INSTITUTE
www.incibe.es

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. La importancia de la información *pág. 03*

2. Los tres pilares de la seguridad *pág. 07*

3. La privacidad y la Ley *pág. 10*

4. Referencias *pág. 12*

ÍNDICE DE FIGURAS.

Ilustración 1 Los tres pilares de la seguridad de la información *pág. 09*

1. LA IMPORTANCIA DE LA INFORMACIÓN

La información en la empresa es esencial para llevar a cabo los distintos procesos de negocio: compras, contratación, contabilidad, ventas, etc. El almacenamiento, tratamiento y gestión de la información, en formato digital o en otros formatos son las actividades que conforman los llamados **sistemas de información** de la empresa que soportan estos procesos. Estos sistemas incluyen también los datos, los recursos materiales (tradicionales, como el bolígrafo y el papel, o tecnológicos) y las personas necesarios para realizar esas las actividades.

Compras

Contratación

Contabilidad

Ventas

Actividades de los sistemas de información

Almacenamiento

Tratamiento

Gestión

La información también es un activo de la empresa: tangible e intangible

INTANGIBLE

- *Know-How*
- Reputación
- Propiedad Intelectual

Si hablamos de los activos que componen estos sistemas de información, es fácil identificar, en primer lugar, aquellos más tangibles como ordenadores, dispositivos de almacenamiento, teléfonos móviles, etc. Sin embargo, no se debe olvidar que existen otros **activos de información, también esenciales para la empresa, que son intangibles** como el *know-how* de los empleados, la reputación, el *software*, la cartera de clientes, las tarifas o la propiedad intelectual.

TANGIBLE

- Ordenadores
- Dispositivos de almacenamiento
- Teléfonos móviles

1.

Es lógico pensar que la información es un recurso esencial para aquellas empresas cuyo negocio se basa en ella, como las que se dedican a publicidad, prensa, contenidos multimedia, etc. Pero, **todas las empresas deben preocuparse por su información**, pues de no estar disponible, alterarse o difundirse sin consentimiento podría afectar a la buena marcha de la empresa. Si nuestros diseños, la cartera de clientes o las tarifas internas cayeran en manos de la competencia las consecuencias podrían ser muy negativas para nuestro negocio y nuestra reputación.

Todas las empresas deben preocuparse por su información

1.

A la protección de los activos de información frente a las amenazas que puedan afectar a su disponibilidad, integridad o confidencialidad la denominamos **seguridad de la información**. Los incidentes de seguridad que afectan a la información de la empresa pueden ser:

Accidentales:

Los sucesos no intencionados son la causa de muchos incidentes. Algunos ejemplos son: borrado de un archivo que pensabas que ya no servía, enviar un correo a un destinatario erróneo o sencillamente una avería en el disco duro.

Intencionados por parte de empleados o *insiders*:

En ocasiones son los propios empleados los que deciden llevarse información de la empresa, causar infecciones o facilitar el acceso a tercero. Lo hacen por motivos propios, como en el caso de empleados insatisfechos o bajo la influencia o el soborno de ciberdelincuentes. Un *insider* puede causar muchos incidentes pues tiene fácil acceso a la información de la empresa. En particular, los robos o fugas de información son fáciles de realizar dado el reducido tamaño de los dispositivos de almacenamiento extraíble y su creciente capacidad, la accesibilidad a los servicios de almacenamiento en la nube o debido al acceso generalizado al correo electrónico.

Causados por ciberdelincuentes

Utilizando códigos maliciosos o *malware* que introducen aprovechando debilidades de nuestros sistemas y en ocasiones nuestra ingenuidad o falta de preparación, como cuando utilizan ingeniería social para conseguir el acceso. El *malware* puede robar información como es el caso de los troyanos o hacerla inaccesible para su propietario al que extorsionan pidiendo un rescate como hacen los llamados *ransomware* **[Ref. - 1]**, o hacer que nuestro equipo esté a las órdenes de una *botnet* que realiza cualquier actividad delictiva.

Por tanto, es muy importante que se adopten las decisiones y medidas necesarias antes de que se produzca un incidente de seguridad que afecte a la información de tu empresa.

2. LOS TRES PILARES DE LA SEGURIDAD

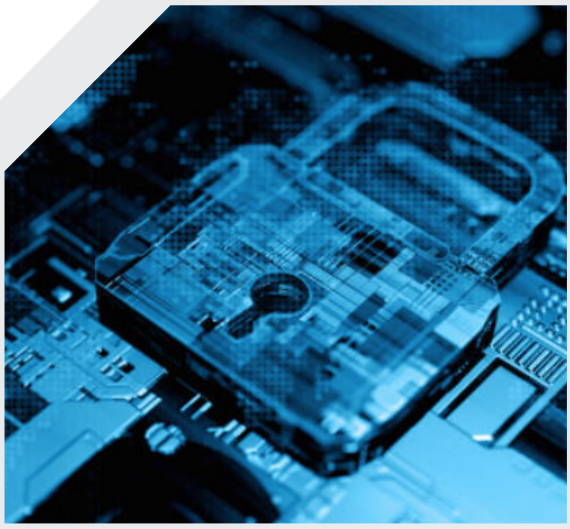
La seguridad de la información consiste en conservar y proteger tres propiedades de la información: disponibilidad, integridad y confidencialidad.

Disponibilidad

Es la propiedad que hace referencia a que la **información esté accesible cuando la necesitemos**. Por ejemplo, un fallo de disponibilidad ocurre cuando es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de *ransomware*, en el que los archivos son cifrados impidiéndonos el acceso a los mismos.

Integridad

Es la característica de la **información que protegemos para que esté libre de modificaciones y errores que impliquen cambios en su contenido**. Existe un fallo de integridad cuando la información, por ejemplo la de un informe de ventas, ha podido ser alterada intencionadamente y podemos basar nuestras decisiones en ella. Otros ejemplos de fallos de integridad son el borrado parcial, ya sea accidental o no, de bases de datos, archivos o programas.



Confidencialidad

Es la propiedad por la que **la información no se pone a disposición o no se revela a individuos, entidades o procesos no autorizados**, es decir, la información confidencial es aquella que debemos proteger del acceso de personas no autorizadas. La difusión intencionada o accidental de esta información se protegerá mediante contratos de confidencialidad con empleados o con terceros que tengan acceso a ella. Tanto a clientes, como a proveedores no les gustaría que información suya fuese expuesta sin su consentimiento y perderíamos su confianza.

La información confidencial puede encontrarse en formato digital, pero también en formato físico (papel y otros soportes) o ser parte del conocimiento de las personas. Independientemente del formato en que se encuentre, se debe proteger. Es responsabilidad de los empleados conocer qué información es confidencial y a quién puede o no comunicarse. Hay distintos tipos de información confidencial:

- la que es crítica para la empresa;
- la información especialmente sensible que puede interesar a otras empresas;
- la información protegida por la legislación como los datos personales o la propiedad intelectual;
- la que, aun no siendo datos personales, afecta a clientes, proveedores o socios y no debe caer en manos de terceros.

En función de los activos de información que tenga la empresa se deben seguir una serie de recomendaciones para que su seguridad sea lo más alta posible. Por ello, es importante identificarlos para los distintos procesos de negocio o los distintos servicios a los que pertenecen en un inventario de activos. A estos activos tenemos que asignarles la importancia en estas tres propiedades. Con estos datos podremos priorizar y diseñar su protección.

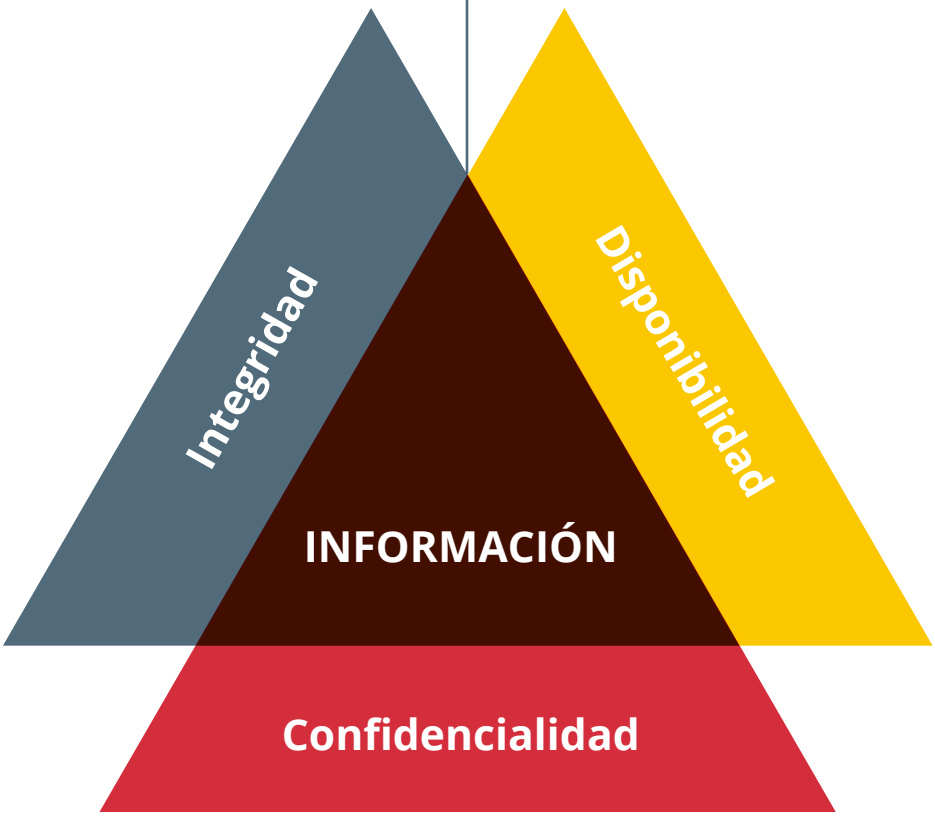


Ilustración 1 Los tres pilares de la seguridad de la información

3. LA PRIVACIDAD Y LA LEY

Los datos personales y su privacidad se han convertido en una prioridad para la sociedad y para todas las empresas. Gran empresa o pyme, independientemente del tamaño deben examinar su situación en cuanto a la protección de datos personales, pues están en juego factores como la confianza de los clientes o la competitividad.

Se considera **dato de carácter personal** «cualquier información concerniente a personas físicas identificadas o identificables», es decir, un DNI es un dato de carácter personal, una fotografía es un dato de carácter personal, e incluso el dato de la estatura de alguien es un dato de carácter personal, si podemos, de alguna forma, saber a quién pertenece.

3.

Desde el Parlamento Europeo se elaboró el Reglamento General de Protección de Datos o RGPD **[Ref. - 2]**. Su adaptación al derecho español se hizo por medio de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales o LOPDGDD.

Esta ley es aplicable a empresas, sociedades, comunidades y autónomos que realicen algún tipo de tratamiento de datos personales. Para cumplir con la ley es importante conocerla, siendo el empresario quien proporcionará la formación específica a sus empleados. Así, todos los que manejan datos personales estarán preparados para garantizar los derechos y libertades de las personas desde que se comienza a realizar cualquier tipo de tratamiento sobre sus datos. Llevar a cabo un tratamiento incorrecto sobre los datos personales que gestiona la empresa, puede suponer graves consecuencias para esta y su continuidad en el tiempo. Para ello:

Identifica si realizas tratamientos de alto riesgo, con datos especialmente protegidos o a gran escala

- Si consideras que no son tratamientos de alto riesgo, deberás justificar tu decisión.

Garantiza los derechos y libertades de los afectados

- Infórmales de forma visible, accesible, sencilla y transparente.
- Obtén el consentimiento inequívoco o expreso.
- Permite que puedan ejercer sus derechos «acceso, rectificación, supresión, limitación, portabilidad, oposición y derecho a no ser objeto de decisiones individualizadas».
- Infórmales en caso de violaciones de seguridad que pudieran afectarles.

Garantiza la confidencialidad, integridad y disponibilidad de los tratamientos y datos personales.

Permite que las autoridades puedan verificar que el tratamiento de datos se realiza de forma correcta a su nivel.

REFERENCIAS

1. INCIBE - Protege tu empresa – Herramientas - Servicio AntiRansomware - https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

2. INCIBE - Protege tu Empresa - RGPD para pymes - https://www.incibe.es/protege-tu-empresa/rgpd-para-pymes

3. INCIBE - Protege tu Empresa - ¿Qué te interesa? - Protección de la información - https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

4. Agencia Española de Protección de Datos - https://www.aepd.es/index.html

5. INCIBE - Protege tu Empresa – Blog – Artículos filtro: Protección de la información - https://www.incibe.es/protege-tu-empresa/blog/filtro/proteccion-informacion

6. INCIBE - Protege tu Empresa – Guías - Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

7. INCIBE - Protege tu Empresa – Blog - Historias reales: mi trabajo robaron y mi proyecto plagiaron - https://www.incibe.es/protege-tu-empresa/blog/historias-reales-mi-trabajo-robaron-y-mi-proyecto-plagiaron

LA INFORMACIÓN

El activo imprescindible de tu organización.

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CIBERSEGURITY INSTITUTE
www.incibe.es
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD