GRUPOLAE

EMPRESAS

SEGURIDAD

MANUAL DE BUENAS PRÁCTICAS

INTRODUCCIÓN

La evolución de las tecnologías de la información y comunicación nos ha permitido automatizar y optimizar muchas de las actividades que se llevan a cabo en nuestra organización. Estas tecnologías han ido ocupando un lugar cada vez más importante, hasta el punto de que hoy en día, sin ellas, muchos de nuestros procesos de negocio no serían posibles.

La información es un activo importante para las empresas, es fundamental para el negocio: facturas, informes, bases de datos de clientes, pedidos, etc. Podemos decir que las empresas basan su actividad en sistemas de información con soporte tecnológico (ordenadores, tabletas, página web, etc.).

Por eso proteger los sistemas de información es proteger el negocio. Para garantizar la seguridad de la información del negocio se necesita llevar a cabo una gestión planificada de actuaciones en materia de Ciberseguridad, tal y como se realiza en cualquier otro proceso productivo de la organización.

¿Qué ocurriría si nuestra empresa se encontrase en alguna de las siguientes situaciones?

- Sufrimos los efectos de un virus informático y no sabemos cómo reaccionar.
- Se produce una pérdida de datos y no tenemos copias de seguridad o no podemos recuperar la información.
- Perdemos o extraviamos un disco duro portátil con información sensible.
- Nuestra página de comercio electrónico es el objetivo de un ataque de denegación de servicio, dejándola inoperativa.
- Se nos estropea algún servidor o elemento de red, que nos impide el uso del correo electrónico, la conexión a Internet o el uso de una aplicación crítica.

Si las herramientas tecnológicas y la información que dan soporte a los servicios y procesos productivos de la organización son de gran valor para nuestra organización, debemos empezar a pensar en poner en práctica un Plan de Seguridad Informática.

¿Qué es un **Plan de Seguridad Informática**?

Un **Plan de Seguridad Informática** consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial. Es fundamental para la realización de un buen Plan Director de Seguridad, en adelante PSI, que se alinee con los objetivos estratégicos de la empresa, incluya una definición del alcance e incorpore las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización, así como terceros que colaboren con ésta.

Principios básicos de las medidas de seguridad

El RGPD señala como piedra angular el principio de la seguridad proactiva (accountability).

Al respecto, el Grupo de Trabajo del art. 29 realiza sugerencias en lo concerniente a la seguridad para garantizar que el principio de responsabilidad aporte seguridad jurídica, dejando a la vez margen para su modulación progresiva (que permita disponer la aplicación de medidas concretas en función del riesgo del tratamiento y de la naturaleza de los datos).

Los principios básicos de la gestión de la seguridad de la información obrante en la Sociedad se estructuran desde las siguientes dimensiones:

- Seguridad strictu sensu: referida a la seguridad proporcionada para evitar el acceso de terceros no autorizados, su alteración o pérdida por actuaciones maliciosas efectuadas sobre la información protegida.

- Confidencialidad: entendida como aquella información fuera del alcance público o de terceros a la que solo las personas autorizadas pueden acceder. La información confidencial debe ser declarada como tal por las personas responsables de la misma y dotarlas de la seguridad necesaria de forma diligente.

- Integridad: garantizando que no se producen alteraciones o manipulaciones no autorizadas sobre la información.

- Autenticidad: de forma que se pueda concluir sin duda alguna, que la información no ha sido manipulada y que se conoce la autoría, de forma que no puede ser repudiada por el autor.

- Trazabilidad: la cual permite establecer un histórico sobre el acceso a la información, el itinerario o recorrido que ha tenido, su posible alteración y concluir quien ha sido el autor de cada acción efectuada sobre ésta.

Conforme a lo establecido en el RGPD, el Responsable de Seguridad (con la colaboración, coordinación y supervisión necesarias del Delegado de Protección de Datos) aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Medidas de Seguridad

Con la nueva regulación introducida por el RGPD, se abandona el sistema de medidas de seguridad tasadas en pro de un sistema menos reglado en el que cada responsable del tratamiento debe valorar qué medidas son las más apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

ALCANCE DEL PLAN DE SEGURIDAD INFORMÁTICA

El responsable del cumplimiento del Plan de Seguridad Informática será siempre la empresa o profesional propietario de la información.

Sus obligaciones serán velar por el cumplimiento del PSI y salvaguardar la seguridad de la información y del sistema informática para evitar los riesgos de fuga o pérdida de información.

LA EMPRESA pretende establecer un Plan de Seguridad Informática para todos los procesos de la empresa y en particular aquellos que puedan almacenar datos confidenciales de clientes, proveedores, empleados.

Normativa interna:

LA EMPRESA tiene que informar al empleado de los usos aceptados y no aceptables, por ejemplo con políticas, normativas y buenas prácticas.

Cumplimiento legal:

Las normativas legales que toda empresa debe cumplir. Leyes y demás normativa aplicable a toda empresa que opera en territorio europeo y que están relacionadas con la gestión y protección de la información de sus usuarios y clientes, así como los sistemas informáticos que la tratan. Las principales leyes y normativas aplicables son:

- Reglamento Europeo de Protección de datos (RGPD): Es el reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica de Protección de Datos (LOPD): Es una ley que afecta a la gran mayoría de empresas y vela por la seguridad de los datos y ficheros de datos de carácter personal que gestionan las empresas. Esta ley obliga a implantar diferentes medidas de seguridad según la sensibilidad de la

información. Próximamente se verá derogada por la Ley Orgánica de Protección de Datos y Garantías de Derechos digitales.

- Directiva sobre privacidad y comunicaciones electrónicas: garantiza la protección de los derechos y libertades fundamentales, en particular el respeto de la vida privada, la confidencialidad de las comunicaciones y la protección de los datos personales en el sector de las comunicaciones electrónicas. También garantiza la libre circulación de datos, equipos y servicios de comunicaciones electrónicas en la Unión. Próximamente se derogará por el Reglamento sobre la Privacidad y las Comunicaciones Electrónicas (E-Privacy).
- Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI): Esta ley a las empresas dedicadas a actividades lucrativas o económicas, que permitan la contratación online de servicios, ofrezcan información de productos a través de páginas web, o que se dediquen al comercio electrónico.
- Ley de Propiedad Intelectual (LPI): Esta ley protege los proyectos, desarrollos u obras fruto de la actividad empresarial.

Seguridad con terceros:

Se hace referencia a los contratos celebrados con los proveedores en relación con servicios externos prestados a LA EMPRESA. De cara a la seguridad, en estos acuerdos de nivel de servicio se deben contemplar:

- Los activos cuya seguridad vigilara el proveedor.
- Las tareas de seguridad (parcheado, actualización, etc.) que realizara el proveedor y realizara LA EMPRESA.
- Una clasificación de incidentes con sus objetivos de tiempos de respuesta o recuperación.
- Las obligaciones contractuales, por ejemplo, compensaciones financieras por pérdidas, etc.

Seguridad interna con los empleados:

En la relación con empleados y colaboradores LA EMPRESA ha de garantizar la confidencialidad de la información de los proyectos y datos personales de los clientes. De no hacerlo puede suponer un incumplimiento desde el punto de vista legal sujeto a sanciones económicas importantes. Por ello LA EMPRESA ha de elaborar acuerdos de confidencialidad con los que regulara los aspectos relativos a la prestación del servicio, incluyendo las sanciones en caso de incumplimiento. Los empleados aceptaran y firmaran por escrito estos acuerdos, que tendrán en cuenta aspectos cómo los siguientes:

- Quien interviene y a qué servicio va asociado el acuerdo de confidencialidad.
- Que se considera información confidencial.
- A que se comprometen las partes que intervienen en el acuerdo.
- Auditoria y legislación aplicable.

PROCEDIMIENTOS INTERNOS DE SEGURIDAD

El compromiso con la seguridad se demuestra definiendo, documentando y difundiendo una política de seguridad que defina cómo se va a abordar la seguridad. También se concreta con el desarrollo de normativas y procedimientos internos que recojan las obligaciones a las que están sujetos los usuarios en lo que respecta al tratamiento y seguridad de la información. En los siguientes epígrafes desarrollamos las políticas internas de LA EMPRESA en torno a:

- **Política de seguridad en el puesto de trabajo**

Los ordenadores, servidores y conexiones de LA EMPRESA tendrán que disponer de sistemas mínimos de seguridad.

A modo de recomendación identificamos la necesidad de disponer de licencias oficiales de hardware y software.

Los riesgos de un ataque de seguridad informática crecen de forma exponencial si los usuarios disponen de versiones no oficiales, además del delito recogido en el Código Penal, tanto en hardware y software.

En el caso de LA EMPRESA, se recomienda que preste especial atención en la renovación de las siguientes herramientas utilizadas:

Sistemas Operativo PC y Servidor	Uso
Windows	General

Herramienta de Correos electrónicos	Uso
Outlook	Gestión de correos electrónicos
Gmail	Gestión de correos electrónicos

Herramienta de Ofimática	Uso
Office (Excel, Word, Access, etc)	Administración
Adobe (PDF)	Administración

- **Política de uso de dispositivos personales**

Trabajar con dispositivos móviles conlleva una serie de riesgos importantes para la seguridad de las empresas como, por ejemplo:

- Pérdida o robo de información.
- El mal uso que se pueda hacer de los dispositivos.
- Robo de dispositivos.
- Robo de credenciales.
- Utilización de sistemas de conexión no seguros.

Por todo esto, LA EMPRESA de establecer políticas y mecanismos adecuados de seguridad para los dispositivos móviles personales que permitan su gestión. LA EMPRESA debe establecer políticas internas que implanten configuraciones de seguridad específicas, y adapten los dispositivos personales a las medidas de seguridad corporativas ya existentes en la empresa (para los dispositivos móviles de uso profesional). No basta con que el dispositivo esté personalizado y securizado según las preferencias personales del usuario, sino que debe cumplir una serie de requisitos que hagan su uso compatible con las políticas de seguridad de la empresa. Para ello se recomienda a la empresa formalizar y firmar la política de uso de los dispositivos móviles en entornos profesionales.

- **Política de utilización de navegadores de internet:**

LA EMPRESA debe controlar el acceso a páginas web que resulten ofensivas o atentatorias contra la dignidad humana o los derechos fundamentales o que estén protegidos por derechos reconocidos en las leyes como los de propiedad intelectual.

- **Política de uso de wifis externas o de conexión desde el exterior**

La configuración de la red wifi pues puede permitir el acceso a la red corporativa a personas ajenas.

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

- LA EMPRESA debe cambiar el usuario y la contraseña de acceso a la configuración del router, pues suelen ser contraseñas por defecto que son de conocimiento público.

- LA EMPRESA debe Modificar, y cambiar regularmente, la contraseña de acceso a la red wifi que viene configurada de fábrica en el router, por otra personalizada que cumpla los requisitos mínimos de seguridad.

- LA EMPRESA debe ocultar el nombre de la red wifi (SSID) de la empresa, para que esta no sea «visible» por dispositivos ajenos a la empresa. De esta forma dificultamos los intentos de conexión indeseados.

- LA EMPRESA protege la red wifi utilizando cifrado en las comunicaciones (activando cifrado WPA/ WPA2).

- LA EMPRESA debe permitir acceder a la red únicamente a los dispositivos de trabajo (esto se puede hacer activando el filtrado de direcciones MAC).

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

- **Utilización de redes inalámbricas**

En referencia a la utilización de tecnología Bluetooth y Zigbee es necesario que LA EMPRESA establezca una serie de medidas de seguridad:

- Activarlos solo cuando se vayan a utilizar

- No aceptar ninguna conexión desconocida y requerir siempre autenticación.
- Configurar los dispositivos para que no resulten visibles a terceros y revisar periódicamente la lista de dispositivos de confianza registrados.
- Asignar nombres a los dispositivos que no reflejen marcas ni modelos.
- Mantener actualizado el software del *smartphone*

➢ **Utilización de equipos informáticos**

LA EMPRESA debe establecer la prohibición del acceso o entrada por cualquier medio en los sistemas informáticos de otros usuarios utilizando una clave de identificación personal (login) o contraseña (password) de otro usuario, salvo autorización expresa.

Se recomienda que siempre que, por cualquier motivo, un trabajador abandone su puesto de trabajo bloquee su sistema para evitar que terceros puedan acceder a los recursos y aplicaciones a las que él.

➢ **Utilización de los programas y archivos informáticos**

La información de carácter confidencial, no debe enviarse a través de ningún medio a terceras personas u organizaciones distintas de las receptoras de la información.

Los programas y archivos informáticos puestos a disposición de los trabajadores de LA EMPRESA deben estar destinados a la actividad empresarial.

Todos los equipos utilizados para la prestación del servicio, deben tener instalado un programa antivirus. No obstante, dado que estos programas de antivirus no eliminan por completo el riesgo de generar y propagar un virus informático, el trabajador deberá tener la máxima diligencia a la hora de ejecutar archivos procedentes de fuentes no conocidas y tener la autorización expresa de Sistemas de Información.

LA EMPRESA no debe permitir la desactivación del antivirus y el firewall sin la autorización del departamento informático o responsable de seguridad de la empresa.

Se debe realizar las actualizaciones de seguridad y mantenimiento de forma periódica. Las actualizaciones son añadidos o modificaciones realizadas sobre los sistemas operativos o aplicaciones que se tienen instaladas en los dispositivos y cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad.

Si no se mantienen los equipos al día la empresa se expone a todo tipo de riesgos: robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, etc.

- LA EMPRESA debe vigilar el estado de actualización de todos los dispositivos y aplicaciones.
- LA EMPRESA debe elegir la opción de actualizaciones automáticas siempre que esté disponible.
- LA EMPRESA debe Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- LA EMPRESA debe evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.

➢ **Política de acceso a la red corporativa:**

LA EMPRESA debe implantar y establecer una política de seguridad que tenga en cuenta las características especiales de los dispositivos y las redes que utilizan para conectarse, así como en las modalidades de teletrabajo y acceso remoto:

- Restringir al máximo los accesos a la red.
- Deshabilitar las conexiones por defecto y habilitar solo los accesos necesarios.
- Configurar correctamente cualquier nuevo equipo o dispositivo para conectarlo a la red corporativa. Asimismo, habrá que asegurarse que hay un software antimalware actualizado.
- Controlar y gestionar el uso de dispositivos móviles y medios de almacenamiento externo como USB, discos duros portátiles, etc.
- Limitar la navegación por Internet para evitar la exposición a amenazas. Es importante prestar atención a las conexiones a redes sociales.
- Eliminar las cuentas y contraseñas por defecto.
- Monitorizar todas las actividades de la red.
- Definir responsabilidades y procedimientos de trabajo para la gestión del equipamiento de red.

➢ **Políticas de almacenamiento (local, dispositivos externos y en la nube)**

Servidores: El Centro de procesamiento de datos (CPD) debe estar acondicionado con un sistema de refrigeración y disponer de medidas de alarma de incendios conectada a un disparador de gas especial para apagar fuegos. El acceso al CPD está restringido al personal de encargado de sistemas y permanecer cerrado con llave cuando no hay nadie en él.

Dispositivos de almacenamiento: Por motivos de seguridad y confidencialidad, es aconsejable eliminar la posibilidad de que el personal de LA EMPRESA descargue en dispositivos de almacenamiento electrónico (USB, pen drive, etc.) la documentación contenida en los sistemas informáticos de la empresa.

Ordenadores en la nube:

El cloud computing, o computación en la nube, es un modelo de trabajo que permite al proveedor tecnológico ofrecer servicios informáticos a través de internet. (Dropbox, Google Drive, One Drive, etc.)

Una parte importante de la seguridad de cualquier servicio cloud recae sobre la empresa proveedora pues será la encargada de garantizar la seguridad física en sus centros de procesos de datos y es importante por parte LA EMPRESA verificar que este proveedor cumpla con unos requisitos de seguridad. Una mala contratación puede tener efectos muy negativos en LA EMPRESA. A continuación, se exponen una serie de amenazas y riesgos a tener en cuenta por parte del empresario:

a) **Amenazas**:

- Accesos no autorizados: Si el proveedor y el cliente no toman conjuntamente las medidas de seguridad adecuadas, no habrá posibilidad de controlar los accesos a la información de la empresa. Los accesos no autorizados pueden provocar robo de datos, inyección de código malicioso, etc.
- Amenazas internas: empleados insatisfechos o exempleados pueden provocar situaciones de riesgo si no se gestionan los permisos y privilegios de acceso. Por ejemplo cuando algún

trabajador que usa un servicio en la nube deja la empresa (por fin de contrato o despido), se debe notificar al proveedor de servicios cloud su baja para evitar que sigan teniendo acceso a la información.

- Interfaces inseguras: si las interfaces que proporciona el proveedor para acceder a la plataforma en la nube no son del todo seguras, estos pueden ser explotados por terceros para acceder a nuestra información.

- Problemas derivados de uso de las tecnologías compartidas: Contratar una infraestructura compartida existe la amenaza de que por un fallo de seguridad usuarios de otras empresas puedan acceder a la información de LA EMPRESA.

- Fuga de información: Como resultado de un ataque informático, el delincuente puede acceder a información confidencial. También en el caso de que las operaciones de transferencias de datos no estén cifradas puede producirse una fuga de información.

- Desconocimiento del entorno: Como no saber manejar la plataforma por parte de los empleados.

b) Riesgos:

Las amenazas pueden transformarse en incidentes si se dan las circunstancias para ello, provocando daños en la reputación y pérdidas económicas. Para ser consciente de estas circunstancias es necesario realizar una evaluación de riesgos.

De las características de los servicios en la nube y conociendo las amenazas, se derivan estos riesgos que se han de valorar:

- Acceso de usuarios con privilegios: este riesgo parece cuando un empleado con privilegios de administrador accede cuando no debería o actúa de forma maliciosa alterando datos o configuraciones. También es posible que se den privilegios por error a empleados que no deban tenerlos y estos por desconocimientos provoquen daños.

  Mitigación: LA EMPRESA ha de consensuar con el proveedor para que los usuarios que tienen privilegios sean solo los que deban tenerlos.

- Falta de aislamiento de los datos: en los servicios en los que la empresa comparte la infraestructura en la nube con otras es necesario que el proveedor gestione que los datos de las distintas empresas no se mezclen y que cada empresa solo tenga accesos a los suyos.

  Mitigación: LA EMPRESA debe garantizar que los datos estén aislados y los procedimientos de cifrado se ejecuten por personal experimentado. Es responsabilidad del empresario saber dónde está localizada la información más sensible para su negocio y exigir que se adoptan las medidas de seguridad oportunas ante el proveedor de alojamiento de la información.

- Indisponibilidad del servicio en caso de desastre o incidente: Si el proveedor sufre un incidente grave o un desastre y no tiene un plan de continuidad, por ejemplo: los servicios y los datos replicados en otro centro de datos, no nos podrá seguir dando servicio.

- Mitigación: LA EMPRESA ha de exigir a los proveedores la capacidad de recuperación de los datos y el tiempo estimado. Asegurándose que estas condiciones quedan establecidas en el contrato. Adicionalmente, es recomendable tener los datos replicados en otra plataforma (Servidores o equipos propios)

Como en todo acuerdo empresarial, la relación entre el proveedor de servicios en la nube y el cliente debe estar regulada por un contrato. En el contrato se fijará el servicio contratado, su duración, condiciones de finalización y desistimiento, precio y otras condiciones. Aspectos a tener en cuenta:

- Disponibilidad, tiempo de respuesta, capacidad de soporte en caso de incidente.

- Seguridad: Verificar previamente si se utilizan medidas como: autenticación y autorización, copias de seguridad, gestión de incidentes, monitorización y registro de actividad (Logging).

- Privacidad: Verificar que la empresa proveedora se acoge a códigos de conducta o dispone certificados amparados por la autoridad de control competente en materia de protección de datos. (Agencia Española de Protección de Datos o la Comisión Europea de Protección de Datos).

➢ **Política de uso del correo electrónico**

El correo electrónico es una herramienta que ofrece muchas posibilidades, tanto en el trabajo como en el ámbito privado, pero se ha de actuar con cautela cuando se use, por tanto, es aconsejable poner en práctica una serie de pautas y medidas de seguridad tanto en el ámbito de la privacidad como en el de la seguridad informática.

- LA EMPRESA ha de utilizar una contraseña robusta y se esté utilizando para acceder a ningún otro servicio.

- LA EMPRESA siempre que un servicio lo proporcione, activara la verificación en dos pasos para añadir una capa extra de seguridad en el proceso de autenticación.

- LA EMPRESA evitara facilitar información que pueda comprometer la privacidad, en caso de que no haya otra elección, cifrar o comprimir los ficheros con alguna contraseña que sólo conozca el destinario y el emisor del email.

- LA EMPRESA no debe abrir correos de usuarios desconocidos y eliminarlos: podrían contener ficheros con malware, enlaces a páginas maliciosas o que suplantan la identidad de alguna entidad.

A continuación, se exponen **las consecuencias de un acceso ilegitimo al correo electrónico**:

A) Pérdida de privacidad:
   - Las conversaciones privadas quedarán expuestas.
   - Las personas sin autorización tendrán acceso a los contactos y documentación importante enviada/recibida por email: Facturas, Nóminas, DNI, Fotografías, Vídeos Etc.

B) Problemas de seguridad:

Un acceso ilegítimo puede acarrear la pérdida de acceso a la cuenta si modifican la contraseña de acceso o los métodos de recuperación alternativos (otra dirección de email, número de teléfono, etc.)

Otros servicios que pueden verse afectados son aquellos que estén vinculados a la dirección de email (PayPal, Amazon, Facebook, Dropbox, etc.)

C) Suplantación de la identidad:

Un acceso ilegítimo puede provocar la suplantación de identidad del propietario de la cuenta de correo electrónico con las siguientes posibles consecuencias:

- Daño de reputación
- Ciberacoso a otras personas, clientes o proveedores.

- Envío de correos fraudulentos: phishing, malware, spam, etc.
- Puesta en circulación de bulos/spam/publicidad no deseada.

Por ello es fundamental llevar una **política de contraseñas robusta y ágil**.

➢ Política de contraseñas:

Las contraseñas son las llaves que dan acceso a los servicios y por ende a la información personal, por lo que si alguien las consigue podría comprometer la privacidad.

A) Contraseñas Robustas

Crear contraseñas fuertes o robustas de al menos 8 caracteres y compuesta por:

- Mayúsculas (A, B, C…)
- Minúsculas (a, b, c…)
- Números (1, 2, 3…) y caracteres especiales ($, &, #...)
- NO utilizar contraseñas fáciles de adivinar como: "12345678", "qwerty","aaaaa", nombres de familiares, matrículas de vehículos, etc.
- NO compartir las contraseñas. Si se hace, dejará de ser secreta y se estará aumentando la visibilidad de tu privacidad.
- NO usar la misma contraseña en varios servicios.

B) Utilizar patrones para crear y recordar tus claves

C) Uso de gestores de contraseñas

Los gestores de contraseñas son programas de cómputo que se utilizan para almacenar una gran cantidad de parejas "usuario/contraseña". La base de datos donde se guarda esta información está cifrada mediante una única clave (contraseña maestra; en inglés, master password), de forma que el usuario solo tenga que memorizar una clave para acceder a todas las demás. Esto facilita la administración de contraseñas y fomenta que los usuarios escojan claves complejas sin miedo a que no podrán recordarlas posteriormente

Características optimas:

- **Acceso online y offline**

No todos los gestores soportan sincronización en la nube, aunque posiblemente esa sea una característica que haga desconfiar a los más recelosos con su privacidad, sin embargo, es extraño ver un servicio que la utilice sin cifrado. Por su parte, los gestores offline gestionan las contraseñas localmente en el disco o en un dispositivo USB.

- **Autenticación en dos pasos**

La autenticación en dos pasos es muy importante en la actualidad y sería muy recomendable activarla al menos para las principales cuentas que utiliza el usuario, entre ellas, como no, la perteneciente al gestor de contraseñas.

- **Integración con los navegadores**

Ayuda a minimizar la interacción con las contraseñas y automatizar el proceso de acceso.

- **Captura automática de la contraseña**

Esta característica está relacionada con la anterior y hace referencia a que el gestor detecta cuando una nueva contraseña es introducida para preguntarle al usuario si quiere guardarla. Algunos gestores también son capaces de detectar las que son actualizadas.

- **Alertas automáticas de seguridad**

Algunos gestores avisan al usuario cuando uno de los servicios que utiliza o uno de los sitios web en los que está registrado ha recibido un ataque que ha podido comprometer las contraseñas.

- **Que sea portable y con soporte para móviles**

Lo ideal sería que el gestor fuese portable, pudiéndose llevar en un pendrive y sin requerir instalación. Que soporte plataformas móviles es otra característica recomendable para gestionar las contraseñas desde cualquier lugar.

- **Auditoría de seguridad**

Algunos gestores permiten realizar auditorías de seguridad sobre la propia base de datos de contraseñas, detectando las que sean débiles o repetidas, entre otros problemas.

- **Contraseñas de un solo uso**

Un sistema de usar y tirar permite designar contraseñas para que sean de un solo uso. Esto abre la puerta incluso a usar el gestor sobre un sistema comprometido debido a que la contraseña para acceder solo puede usarse una vez.

- **Compartir contraseñas**

Algunos gestores permiten compartirlas de forma segura. Esta función puede servir con un amigo o bien en entornos laborales.

Mejores soluciones de gestor de contraseñas

- **LastPass**: es posiblemente la solución más conocida dentro de su segmento. Es un servicio bien presentado, con una interfaz sencilla, sincronización en la nube, auditoría de seguridad y es totalmente multiplataforma, funcionando sobre Windows, macOS, Linux, Android e iOS.
- **KeePass**: es el gestor de contraseñas Open Source por excelencia, ya que está certificada por al Open Source Initiative y su código está publicado bajo la licencia GPLv2. Debido a esto, existen muchas reimplementaciones disponibles para todos los sistemas operativos y hasta una extensión llamada CKP. Es conocido sobre todo entre los usuarios de Linux.
- **Dashlane**: es un gestor de contraseñas que maneja un concepto similar al de LastPass. Resulta sencillo de utilizar y ofrece sincronización en la nube, aunque sus planes de pago son más caros que los de su competidor. Anteriormente era una aplicación que solo soportaba los sistemas operativos mayoritarios (Windows, macOS, iOS y Android), pero recientemente ha añadido a Linux y Chrome OS a modo de extensiones para Chrome y Firefox.
- **Bitwarden**: Una alternativa Open Source y gratuita a LastPass con extensiones para Firefox, Chrome, Opera y Edge, además de aplicaciones para iOS y Android.
- **Encrypt**: Consiste en una aplicación que se instala a nivel del sistema operativo, soportando Windows, Mac, Linux, Android e iOS. Al igual que Bitwarden, es Open Source y presume de ser fácil de usar.

➢ **Política de utilización de redes sociales**

- **Control de las publicaciones**

Cada vez que se publique algo en una red social se pierde el control sobre ese contenido. Aunque se borre, quedará como mínimo registrado en los servidores de la red social y cualquiera que lo haya visto puede haber hecho uso de esa información, ya sea difundiéndola o copiándola.

Se ha de valorar previamente qué que se quiere publicar, especialmente teniendo en cuenta configuración de la privacidad y en consecuencia quién podrá ver toda esa información.

- **Recabar previamente todos los derechos de imagen, de propiedad intelectual e industrial antes de colgar contenidos en la red social**

Es común incluir imágenes de trabajadores en redes sociales sin su consentimiento. El derecho a la propia imagen está reconocido en el artículo 18.1 de la Constitución, junto al derecho al honor y el derecho a la intimidad, y goza de un nivel de protección extraordinario. Por tanto, hay que tener muy claro que no se puede ilustrar una página web de una de una empresa, un blog, un cartel de publicidad con el retrato de una persona sin su autorización previa y expresa. La persona fotografiada debe ceder el derecho de uso de su imagen por escrito y siempre antes de la publicación. Luego si se va a hacer uso de alguna fotografía en este sentido, es extremadamente recomendables utilizar un documento de cesión del uso de la imagen, a afectos de no incurrir en responsabilidad.

Incluir fragmentos de obras ajenas con efectos comerciales (Canciones, Fotografías o fragmentos literarios o videos) requiere de la obtención de los derechos a través de una firma de la oportuna licencia. Las redes sociales no se hacen responsables de este tipo de infracciones al aceptar las condiciones y términos de uso. En la misma línea con la utilización de marcas y productos de otras empresas.

- **Elaborar perfiles profesionales y no personales**

Es un error bastante común, sobre todo en pequeñas y medianas empresas, no tener clara la diferencia entre una página profesional y un perfil personal. Algunas empresas u organizaciones crean un perfil en lugar de una página, sin saber que están por un lado incumpliendo una norma del uso de la red social y, por otro, desaprovechando oportunidades muy valiosas que estarían a su alcance si tuvieran una página creada correctamente.

- **Política de copias de respaldo y de recuperación**

La seguridad de los datos no sólo supone la confidencialidad de los mismos, sino que también conlleva la integridad y disponibilidad de éstos.

Para garantizar dichos aspectos será necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del Sistema Informático, permitan recuperar y en su caso reconstruir los datos que se conservaban en los ficheros de LA EMPRESA.

El Responsable de Seguridad es quien se encargará de:

- Obtener periódicamente una copia de seguridad de los distintos ficheros, a efectos de respaldo y posible recuperación en caso de fallo, siguiendo el procedimiento de backup establecido.
- Revisar la ejecución de los procedimientos de backup y notificar cualquier incidencia al respecto.

Estas copias de deberán realizarse con una periodicidad, al menos, semanal, salvo en el caso de que no se haya producido ninguna actualización de los datos.

El caso de fallo del Sistema con pérdida total o parcial de los datos de datos existirá un procedimiento mediante el que sea posible, partiendo de la última copia de respaldo, reconstruir los datos al estado en que se encontraban en el momento del fallo.

Será necesaria la autorización por escrito del responsable de tratamiento, para la ejecución de los procedimientos de recuperación de los datos; deberá dejarse constancia en el Registro de Incidencias de

las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

Para datos a los que corresponda un nivel de seguridad superior al estándar, la copia de respaldo y procedimientos asociados deben almacenarse en un lugar separado al de ubicación del fichero que contiene esos datos y que reúna las medidas de seguridad apropiadas.

Descripción del proceso de realización de copias de seguridad.

Medidas de seguridad aconsejables en relación con las copias de seguridad:

- Realizar copias de seguridad de forma semanal.
- Al final de cada mes realizar una copia completa que se conserve, al menos, durante dos años.
- Al final de cada año realizar una copia completa que se conserve de forma indefinida.
- Al final de cada año se deben desecharán los juegos de copias semanales y serán sustituirlas por nuevas
- Las copias se deben almacenar en una ubicación diferente a la del Servidor de la Aplicación y, a ser posible, en armario ignífugo o fuera de las instalaciones.
- Para proceder a la recuperación de datos o archivos, será imprescindible la autorización del responsable del tratamiento.

- **Control de Accesos**

La normativa vigente en materia de protección de datos personales y demás legislación complementaria establece que el acceso a los sistemas de información por parte de los usuarios de LA EMPRESA debe corresponderse con la adecuación a perfiles de usuario, con las jerarquías pertinentes, debe adoptar las medidas de seguridad prescritas por la normativa y debe garantizarse el nivel de seguridad correspondiente al tipo de dato personal objeto de tratamiento. Se debe distinguir los siguientes conceptos antes de proceder a llevar un control de accesos:

- **Accesos autorizados**: autorizaciones concedidas a un Usuario para la utilización de los diversos Recursos.

- **Autenticación**: procedimiento de comprobación de la identidad de un Usuario.

- **Contraseña**: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la Autenticación de un Usuario.

- **Control del acceso**: mecanismo que en función a la Identificación ya autenticada permite acceder a datos o recursos.

- **Identificación**: procedimiento de reconocimiento de la identidad de un Usuario.

- **Incidencia**: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- **Recurso**: cualquier parte componente de un sistema de información.

- **Responsable de Tratamiento:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

- **Usuario**: sujeto o proceso autorizado para acceder a datos o recursos.

Por cuestiones de seguridad, debe quedar prohibida en LA EMPRESA la entrega y/o comunicación de Identificaciones y Contraseñas que permitan acceder a los sistemas de información a personas no autorizadas. Las Identificaciones y Contraseñas son de carácter exclusivo y confidencial. Queda prohibida su comunicación a terceros.

Los responsables de seguridad debe ser el responsable para entregar Identificaciones y Contraseñas a los trabajadores para que accedan a los sistemas de información de LA EMPRESA

El responsable de seguridad de LA EMPRESA debe disponer de unas Identificaciones y Contraseñas genéricas, guardados en sobres numerados y sólo accesibles por éste que anotará en un registro informático o físico, relacionándolo con el trabajador al que le haga entrega, de forma que quede registro de quien dispone de cada Identificación y Contraseña.

El responsable de seguridad de LA EMPRESA es el encargado de entregar y registrar en el modelo de registros, las Identificaciones y Contraseñas que precisen los trabajadores a su cargo, así como tramitar de forma inmediata las peticiones de altas y bajas a los sistemas de información de la organización.

El responsable de seguridad de LA EMPRESA ha de velar porque ningún Usuario de los sistemas de información de la organización acceda y/o trate información, especialmente datos de carácter personal, que no precise para el ejercicio de sus funciones además de verificar que ningún usuario de los sistemas de información de la organización acceda a estos sin estar debidamente identificado y registrado.

- **Actualizaciones**

LA EMPRESA ha de mantener una adecuada planificación de la seguridad de las aplicaciones que manejan la información.

Cualquier aplicación es susceptible de tener fallos de seguridad en su diseño, es decir, vulnerabilidades, por lo que el fabricante va lanzando actualizaciones y parches que corrigen estos fallos. LA EMPRESA como usuaria de aplicaciones y de programas informáticas he de actualizar e instalar estos parches.

Los atacantes escanean las redes en busca de equipos desactualizados para averiguar por donde atacarlos, aprovechando sus fallos del software. También se aprovechan de defectos en la configuración.

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

LA EMPRESA debe realizar un inventario de todos los activos y dispositivos informáticos de la empresa, donde se incluyan las características técnicas de los equipos, los sistemas operativos, versiones, licencias y aplicaciones instaladas con todas sus características. Para ello LA EMPRESA puede ayudarse de una base de datos de la gestión de configuración, que permite inventariar servicios, hardware, redes, documentación, licencias, etc.

- **Registro de actividad**

Es preciso recabar toda la información posible sobre todas las actividades de los distintos procesos y actividades llevas a cabo en ello. Para ello LA EMPRESA debe monitorizar y analizar constantemente todos estos elementos.

Este proceso de monitorización pasa por las fases de:

- Recolección de la información y datos.
- Detección de posibles anomalías.

- Análisis de la información.

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

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

Los sistemas de monitorización deben contemplar también los problemas físicos y de rendimiento de los sistemas como el nivel de funcionamiento de un SAI (Fuente de alimentación en caso de apagón), la temperatura de los servidores y sistemas corporativos para detectar problemas de seguridad, rendimiento o funcionalidad permitiendo, de forma proactiva, programar cambios o sustituciones de los equipos susceptibles de antes de que ocurra cualquier problema.

GRUPOLAE

EMPRESAS

SEGURIDAD

SISTEMA PARA LA GESTIÓN DE LA PRIVACIDAD Y LA

INTRODUCCIÓN

LA EMPRESA tiene establecido, implementado y mantenido un sistema para la gestión de la privacidad y la protección de datos, de acuerdo con los requisitos establecidos en el Reglamento Europeo 2016/679 relativo a la protección de las personas físicas en los que respecta al tratamiento de datos personales y a cualquier otra normativa aplicable relacionada con la protección de los datos personales.

Este sistema describe y define las medidas, normas, procedimientos, reglas, controles y estándares de seguridad que LA EMPRESA acomete sobre el ámbito de aplicación de cualquier tipo de soporte, tanto si es informatizado como si no, para garantizar la seguridad de los datos de carácter personal que se almacenan y gestionan en la LA EMPRESA, evitando su alteración, pérdida, difusión, tratamiento o acceso no autorizado.

La documentación del sistema se mantendrá en todo momento actualizada y deberá ser revisada siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

DESCRIPCIÓN DEL ALCANCE DEL MATERIAL: SISTEMAS DE INFORMACIÓN

El ámbito material de aplicación incluye las aplicaciones informáticas, bases de datos, sistemas operativos, sistemas de soporte, servidores, equipos, sistemas de comunicaciones y usuarios que componen la infraestructura de la informática de la LA EMPRESA y que se utilizan para el tratamiento de datos de carácter personal, así como los locales en los que se ubican.

1. UTILIZACIÓN DE EQUIPOS INFORMÁTICOS

Equipos informáticos	**Medidas de seguridad**
LA EMPRESA pone a disposición de sus empleados equipos informáticos (Torres y/ ordenadores portátiles).	LA EMPRESA debe llevar a cabo controles de acceso y bloqueo de los equipos informáticos.

2. USO DE NAVEGADORES

Navegadores utilizados	**Medidas de seguridad**
LA EMPRESA navegadores de búsqueda en Internet tales como Safari, Windows Edge, Firefox, Google Chrome, Internet Explores u otros.	LA EMPRESA debe emplear controles de acceso a páginas web que resulten ofensivas o atentatorias contra la dignidad humana o los derechos fundamentales o que estén protegidos por derechos reconocidos en las leyes como los de propiedad intelectual o Industrial.

3. POLÍTICAS DE ALMACENAMIENTO (LOCAL, DISPOSITIVOS EXTERNOS Y EN LA NUBE)

- **SERVIDORES:**

Uso	Medidas de Seguridad
Administración	Los servidores de LA EMPRESA deben tener acceso limitado por usuario y contraseña y estar filtrado por necesidades y privilegios.

- **DISPOSITIVOS DE ALMACENAMIENTO ELECTRÓNICO**

Utilización de dispositivos de almacenamiento electrónico	Medidas de seguridad
LA EMPRESA permite la utilización de dispositivos de dispositivos de almacenamiento electrónico.	LA EMPRESA debe eliminar la posibilidad de que el personal de la empresa descargue en dispositivos de almacenamiento electrónico (USB, pen drive, etc.) la documentación contenida en los sistemas informáticos de la empresa.

4. POLÍTICA DE USO DE CORREO ELECTRÓNICO

Utilización de cuentas de correo electrónico	Medidas de seguridad
LA EMPRESA utiliza cuentas de correo electrónico para la realización de la actividad empresarial	LA EMPRESA debe poner en práctica una serie de pautas y medidas de seguridad tanto en el ámbito de la privacidad como en el de la seguridad informática (Ver Anexo I).

5. POLÍTICA DE CONTRASEÑAS

Utilización de Usuarios y Contraseñas	Medidas de seguridad
LA EMPRESA utiliza cuenta de usuarios y contraseñas	LA EMPRESA debe utilizar contraseñas robustas (Alfanuméricas, no conceptuales o genéricas) o gestores de contraseñas

6. UTILIZACIÓN DE PROGRAMAS Y ARCHIVOS INFORMÁTICOS

Programas y archivos informativos	Medidas de seguridad
LA EMPRESA pone a disposición de sus empleados el uso de programas y archivos informáticos.	LA EMPRESA debe emplear controles de seguridad (Firewall y Antivirus) y limita el uso de programas informáticos únicamente a la actividad empresarial.

- **SOFTWARE UTILIZADO EN LA EMPRESA**

SOFTWARE	FUNCIONALIDADES
MS OFFICE	**EXCEL** Aplicación para manejar hojas de cálculos. **OUTLOOK** Programa de agenda ofimática y cliente de email que puede ser utilizado como aplicación independiente, o junto con Microsoft Exchange Server para dar servicio a múltiples usuarios dentro de una organización tal como buzones compartidos, calendarios comunes, etc. **POWER POINT** Es un programa diseñado para hacer presentaciones con texto esquematizado, fácil de entender, animaciones de texto e imágenes, imágenes prediseñadas o importadas desde imágenes del ordenador. Se le pueden aplicar distintos diseños de fuente, plantilla y animación. Además, se puede realizar muchos tipos de productos relacionados con las presentaciones: transparencias, documentos impresos para los asistentes, notas y esquemas para el presentador, o diapositivas estándar de 35mm. **WORD** Procesador de textos.
ADOBE	**ACROBAT READER DC** Permite "navegar" a través de documentos PDF para visualizar su contenido, así como imprimirlos o compartirlos tal y como fueron creados por su autor. También permite descargar PDFs encriptados y desbloquearlos. Se integra perfectamente con el Internet Explorer de Microsoft y con el Navigator de Netscape.

7. USO DE WIFI y REDES INHALÁMBRICAS

EMPLEO DE RED WIFI	Medidas de seguridad
LA EMPRESA utiliza conexión Wifi	LA EMPRESA debe emplear buenas prácticas para aumentar la seguridad de la red Wifi corporativa (Ver Anexo I)
LA EMPRESA permite la utilización de la tecnología inalámbrica como Bluetooth y/o Zigbee.	LA EMPRESA debe establecer una serie de medidas de seguridad en la utilización de las redes inalámbricas (Ver Anexo I).

8. POLÍTICA DE ACCESOS A LA RED CORPORATIVA

Acceso a la red corporativa	Medidas de seguridad
LA EMPRESA pone a disposición de sus empleados el acceso a la red corporativa.	LA EMPRESA debe implantar y establecer una política de seguridad que tenga en cuenta las características especiales de los dispositivos y

	las redes que utilizan para conectarse (Ver Anexo I).

9. POLÍTICA DE COPIAS DE RESPALDO Y DE RECUPERACIÓN

Realización de copias de seguridad externas o internas	Medidas de seguridad
LA EMPRESA realiza copias de seguridad	LA EMPRESA debe realizar copias de seguridad con periodicidad semanal internamente o a través de otra empresa (Hosting Externo o Cloud)

10. ACTUALIZACIONES Y REGISTRO DE ACTIVIDADES

LA EMPRESA debe actualizar el software de forma periódica y monitoriza las actividades dentro de su actividad empresarial.

CONCLUSIONES FINALES

LA EMPRESA debe estar preparada para prevenir, protegerse y reaccionar ante incidentes de seguridad que puedan afectar a su negocio. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permita a LA EMPRESA recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. De esta forma se garantiza poder dar respuesta de forma planificada ante cualquier fallo de seguridad a través de un sistema para la gestión de seguridad informática.