FUNDACION SER

ANEXO I
MEDIDAS DE SEGURIDAD ORGANIZATIVAS Y TECNICAS SOBRE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo,
de 27 de abril de 2016

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales
y garantía de los derechos digitales.

Versión: 01.00
Fecha última actualización: Octubre 2021

ANEXO

MEDIDAS DE SEGURIDAD ORGANIZATIVAS Y TECNICAS SOBRE TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

INDICE. **PAG.**

1. INFORMACION GENERAL

El **Reglamento General de Protección de Datos (RGPD**) **en su artículo 5.1.f** determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental.
Esto implica que hay que adoptar **medidas técnicas y organizativas** encaminadas a asegurar la **integridad y confidencialidad** de los datos personales y la posibilidad de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

1.1 SEGURIDAD DE LOS DATOS PERSONALES

El **Reglamento General de Protección de Datos (RGPD**) **en su artículo 32** establece lo siguiente:

Seguridad del tratamiento

1.Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán **medidas técnicas y organizativas** apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la **seudoanimización 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.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

El Reglamento General de Protección de Datos no establece un listado cerrado o taxativo de las medidas de seguridad que han de ser implantadas por el responsable de los tratamientos de datos de carácter personal, en consecuencia, las siguientes medidas de seguridad deben considerarse como una orientación, debiendo adoptarse aquellas medidas más adecuadas criterio del responsable, atendiendo a las necesidades o circunstancias propias de la entidad.

2. MEDIDAS ORGANIZATIVAS

Todo el personal con acceso a datos personales responsabilidad de la entidad, deberá ser informado y tener conocimiento de sus obligaciones con relación al tratamiento de los mismos.

2.1 MEDIDAS RELATIVAS A LA PROTECCION DEL PUESTO DE TRABAJO.

La gestión de la información se realiza fundamentalmente desde el puesto de trabajo, tanto desde dispositivos informáticos como de forma más tradicional en papel.

Para garantizar la seguridad de la información y los recursos gestionados desde el puesto de trabajo, debe implantarse una **política de protección del puesto de trabajo**.

La entidad debe informar a los usuarios de los datos personales sobre las obligaciones y buenas prácticas en materia de seguridad que apliquen a su puesto de trabajo. Esta normativa debe ser firmada por los empleados en su incorporación a la entidad, así como estar siempre disponible y recordar su aplicación de manera periódica.

Se establecerán las siguientes medidas de seguridad en lo relativo a **protección del puesto de trabajo**.

- Para el acceso a documentos o archivos informáticos responsabilidad de la entidad **solo se utilizarán soportes o equipos informáticos puestos a disposición por la misma** salvo que sea autorizado de manera motivada y excepcional la utilización de equipos o soportes informáticos ajenos a ella.

- El empleado o usuario debe conocer, aceptar y aplicar la **Política de uso de dispositivos móviles de la empresa**.

- **Los documentos o archivos informáticos** se **guardarán en los directorios protegidos de los servidores o equipos informáticos que sean designados para ese fin** con la finalidad de poder aplicar las medidas de seguridad que les correspondan.

- Se **deberán revisar periódicamente los equipos para detectar información sensible** en carpetas distintas a las designadas, incluida la papelera de reciclaje, y de existir, deberá ser traspasada a los directorios designados en servidores o equipos informáticos o bien destruida con las medidas adecuadas.

- **Los terminales o equipos informáticos con acceso a datos de carácter personal no se podrán tener en zonas de acceso público** como salas de espera o recepciones, salvo que estén permanentemente vigilados por personal autorizado.

- El personal informático programará un **bloqueo automático de sesión por salvapantallas** en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo. La desactivación del salvapantallas requerirá la introducción de contraseña.

- En caso de finalización de la jornada laboral se apagará el equipo.

- El personal informático aplicará la **Política de actualizaciones de software** revisando los equipos periódicamente para garantizar su actualización o activando las actualizaciones automáticas.

- El personal informático aplicará la **Política antimalware**, que incluya la instalación y actualización de herramientas antimalware en todos los equipos y sistemas, y su revisión periódica de manera que se garantice la protección antimalware.

- El personal informático **deshabilitará por defecto los puertos USB** de todos los equipos y los habilitará para aquellos usuarios que necesiten, de forma justificada y debidamente autorizada, dicha funcionalidad.

- El personal informático verificará que las impresoras y otros equipos conectados a la red o que puedan contener información de la empresa están incluidos en las Políticas de seguridad.

- Para que el empleado haga un uso correcto de los dispositivos de almacenamiento disponibles, debe conocer y aplicar la normativa corporativa relativa al almacenamiento local en el equipo de trabajo, almacenamiento en la red corporativa, en la nube y en los dispositivos extraíbles.

- **Se considerará prohibida cualquier alteración en la configuración del equipo e instalación de aplicaciones no autorizadas**. Si el usuario requiere una configuración o software específico para el desempeño de su trabajo, deberá solicitarlo formalmente al equipo informático.

- **Los documentos en papel y soportes informáticos se almacenarán en lugar seguro** como armarios o estancias cerradas bajo llave **y acceso restringido a personal autorizado** durante las 24 horas del día.

- Se deberá **evitar que en las mesas de trabajo queda expuesta documentación con datos personales** o dispositivos extraíbles, siempre y cuando no se esté trabajando con ella y en todo caso a la finalización de la jornada laboral. No se apuntarán usuarios ni contraseñas en los puestos de trabajo.

- **No se realizarán copias de documentos o ficheros temporales** que contengan datos de carácter personal, ya sea en papel o en equipos o soportes informáticos, **sin la autorización expresa del responsable del tratamiento** o de la persona en quien se delegue, siempre y cuando no sea en el ejercicio de las funciones que le han sido encomendadas.

- **En caso de realizarse, se establecerán medidas para borrar los ficheros temporales o copia de documentos** una vez que hayan dejado de ser necesarios para el trabajo y mientras estén vigentes se procederá a aplicar las medidas de seguridad adecuadas.

- Se informará a los usuarios que **después del uso de fotocopiadoras, impresoras o escáneres, deberán asegurarse que no queden en ellos documentos impresos que contengan datos de carácter personal.**

- Los documentos en papel que vayan a ser desechados, se destruirán mediante sistemas que aseguren la imposibilidad de recuperar la información que contienen, en particular:

    - Mediante destructoras de papel al servicio de los empleados;
    - Mediante un servicio externo de destrucción segura.
    - Dando a conocer los riesgos asociados a la utilización de papeleras para documentos sensibles.

- Todo usuario con acceso a datos de carácter personal estará sometido al **deber de secreto y de confidencialidad** que incluso persistirá cuando finalice su relación laboral o de cualquier otra naturaleza con la entidad.
- **No se comunicarán datos personales a terceros**, sin la autorización previa y por escrito del responsable del tratamiento, siempre y cuando no sea en el ejercicio de las funciones que le han sido encomendadas.

- Se prestará atención especial en no comunicar datos personales a terceros durante las consultas telefónicas, correos electrónicos u otros sistemas de comunicación.

- El usuario debe seguir la **Política de contraseñas** de la entidad:
    - Las credenciales (usuario y contraseña) son confidenciales y no pueden ser publicadas ni compartidas;
    - No deben anotarse las credenciales en documentos ni en cualquier otro tipo de soporte;
    - Las contraseñas deben ser robustas: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales.
    - Se deben cambiar periódicamente.

- El usuario debe conocer, aceptar y aplicar la normativa que regula el uso de Internet como herramienta de trabajo con los usos permitidos y prohibidos. También seguirá las recomendaciones de seguridad relativas a la navegación por internet como:
    - Verificar que las direcciones (URL) de destino son correctas;
    - Verificar que el certificado es válido, cuando se trate de conexiones a entornos seguros (web mail, extranet, etc.) o realicemos transacciones;
    - Comprobar que se cumple el protocolo https:// en las páginas donde trabajemos con información crítica.

- El usuario debe conocer, aceptar y aplicar la **Política de clasificación de información**, que indica qué información debe ser cifrada.

- El usuario debe advertir de cualquier incidente relacionado con su puesto de trabajo:
    - Alertas de virus/malware generados por el antivirus;
    - Llamadas sospechosas recibidas pidiendo información sensible;
    - Correos electrónicos sospechosos de contener virus;
    - Pérdida de dispositivos móviles (portátiles, *smartphones* o tabletas) y dispositivos externos de almacenamiento (USB, CD/DVD, etc.);
    - Borrado accidental de información;
    - Alteración accidental de datos o registros en las aplicaciones con información crítica;
    - Evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (CPD, despachos, almacenes…);
    - Evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros;
    - Cualquier actividad sospechosa que pueda detectar en su puesto de trabajo.

2.2 MEDIDAS SOBRE PROCEDIMIENTOS DE ATENCION DE LOS DERECHOS DE LOS TITULARES DE LOS DATOS

- Se informará a todo el personal acerca del procedimiento para atender los derechos de las personas interesadas, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:
    - La entidad dispondrá de **modelos de solicitud de ejercicio de derechos** para facilitar a las personas interesadas, si bien también pueden ser obtenidos en la página web de la Agencia Española de Protección de Datos.

- Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (personas interesadas) podrán ejercer sus derechos de acceso, rectificación, supresión y oposición, así como otros derechos que establece la normativa. El responsable del tratamiento deberá dar respuesta a las personas interesadas sin dilación indebida.

- Para el **derecho de acceso** se facilitará a las personas interesadas la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.

- Para el **derecho de rectificación** se procederá a modificar los datos de las personas interesadas que fueran inexactos o incompletos atendiendo a los fines del tratamiento.

- Para el **derecho de supresión** se suprimirán los datos de las personas interesadas cuando las personas interesadas manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.

- El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de las personas interesadas, la forma y el procedimiento en que se atenderán dichos derechos.

- El responsable del tratamiento comunicara cualquier solicitud de ejercicio de derechos de las personas interesadas al **Delegado de Protección de Datos** o **en su defecto a la consultora sobre protección de Datos** en el plazo más breve posible para poder gestionar adecuadamente el ejercicio de derechos.

2.3 VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL

2.3.1 NOTIFICACIÓN A LA AUTORIDAD DE CONTROL

- Serán notificadas por parte del responsable del tratamiento a la Agencia Española de Protección de Datos las violaciones de seguridad de datos de carácter personal que se produzcan en la entidad sin dilación indebida y de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.
- Si la notificación a la Agencia Española de Protección de Datos no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
- La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es
- Se deberá incluir en la notificación:
  - Describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de personas interesadas afectadas, y las categorías y el número aproximado de registros de datos personales afectados.
  - Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
  - Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

- Si no fuera posible facilitar la información simultáneamente, la información se facilitará de manera gradual sin dilación indebida.

- El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

2.3.2 COMUNICACIÓN AL INTERESADO

- Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

- La comunicación al interesado describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la siguiente información:
  - El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
  - Las posibles consecuencias de la violación de la seguridad de los datos personales.
  - Las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

- No será necesaria la comunicación si se cumple alguna de las condiciones siguientes:

  - El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.
  - El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.
  - Suponga un esfuerzo desproporcionado optándose por una comunicación pública o una medida semejante.

3. MEDIDAS TECNICAS

3.1 MEDIDAS RELATIVAS AL CONTROL DE ACCESO A LA INFORMACION

Se establecerá por parte del responsable del Tratamiento una **política o sistema de control de accesos** de los usuarios a los recursos o datos de la entidad y que se basará en los siguientes elementos:

- **Identificación** es el método mediante el cual decimos quienes somos, es decir, que nombre nos han puesto en el sistema, como nos reconoce.

- **Autenticación** es el método para comprobar que somos quienes decimos que somos. Esto se realiza generalmente con algo que poseemos, somos o sabemos y que previamente al darnos de alta el sistema había asociado a nuestra identidad. Es la segunda parte de las credenciales de acceso.

- **Autorización** es el mecanismo para comprobar si el usuario autenticado tiene los derechos de acceso a los recursos que quiere acceder y los privilegios para hacer con ellos lo que solicita. Si es así, le autoriza, en caso contrario no.

- **Registro de Acceso** es el mecanismo para dejar constancia de todos los eventos que tiene lugar en relación con los accesos, básicamente: **quién quiere acceder, a qué, cuándo, para qué y qué resultado tiene ese evento** (accede, no accede, el recurso no está disponible, etc.).

- Sólo se concederá acceso a aquellos datos y recursos que el usuario necesite para el desarrollo de sus funciones y haya sido expresamente autorizado por la entidad.

- **Se deberá definir con qué derechos se puede acceder**. Crear, modificar, borrar o destruir cualquier documento o fichero.

- **Sólo el personal autorizado podrá conceder, modificar o anular la autorización de acceso a los recursos**, conforme a los criterios establecidos por su responsable.

- **Se establecerán los controles para evitar que alguien acceda a recursos sin autorización** o con derechos distintos de los autorizados.

- Deberá existir una **relación actualizada de usuarios con autorización de acceso** a dichos recursos, especificando el perfil de acceso de cada uno de ellos, comprobando que es correcto.

- Esta relación se actualizará cuando exista cualquier cambio sobre las autorizaciones de acceso a los ficheros de datos.

- Deberá existir un control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.

- Los mecanismos de autenticación serán adecuados al nivel de protección requerido, pudiendo usarse los siguientes factores de autenticación:

  - **Contraseñas.**
  - **Componentes lógicos** como certificados software o dispositivos físicos.
  - **Elementos biométricos.**

- Se recomienda implantar un **sistema de autenticación de doble factor** en el acceso a servicios que contengan **información especialmente sensible o crítica**.

- **El control de acceso a los recursos informáticos mediante contraseña se realizará** de acuerdo con lo que se indica a continuación:
  - El usuario, **dispondrá de un identificador personal (nombre de usuario)** proporcionado por la entidad, que le identifique única y exclusivamente a él **y de una contraseña única, que le permita autenticarse como usuario autorizado**, tanto al Sistema Operativo como a cualquier otro programa o aplicación de gestión de ficheros.
  - Las credenciales se activarán una vez estén bajo el control efectivo del usuario y estarán bajo su control exclusivo.
  - El usuario reconocerá a través de algún sistema que deje constancia que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.

- **Las contraseñas** deberán reunir como mínimo las siguientes características y ser confidenciales:
  - **Deberán tener** una longitud mínima de **8 caracteres y que contengan números, letras, caracteres especiales y alternar mayúsculas y minúsculas.**
  - Se deberá evitar contraseñas fáciles como nombres, palabras o expresiones que coincida con el propio usuario o que coincida con contraseñas anteriores que han sido utilizadas por el usuario.

- Se cambiarán con la periodicidad marcada por la política de la organización, **no siendo superior a 12 meses.** Es recomendable implantar un sistema de solicitud de cambio de contraseña automático de la aplicación y/o el sistema operativo al cumplirse el periodo indicado anteriormente.

- La deberá establecer un número limitado de intentos de acceso a aplicaciones, bloqueándose el acceso del usuario cuando sobrepase el número máximo de intentos.

- **Las cuentas deben ser inhabilitadas en los siguientes casos**:
  - Cuando el usuario deja la organización.
  - Cuando el usuario cesa en la función para la cual se requería la cuenta de usuario;
  - Cuando la persona que la autorizó, da orden en sentido contrario.

- **Las cuentas se retendrán durante el periodo necesario** para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas.

- Los ficheros con datos de carácter personal en soportes no informáticos (papel), deberán estar siempre almacenados en archivadores (armarios o cajones) dotados de sistemas de cierre con llave u otro mecanismo de seguridad y siempre en zonas que imposibiliten el acceso no autorizado a los datos.

- Se deberá establecer un sistema de registro de accesos a los documentos de cada fichero, por medio de un registro manual donde se indique, el nombre del usuario, la fecha y hora y el documento accedido.
- Como regla general y en todo caso las aplicaciones informáticas que gestionen datos especialmente protegidos deberán disponer de un sistema que permita registrar las actividades de los usuarios de acuerdo con lo que se indica a continuación:
  - El registro indicará que usuario realiza la actividad, la fecha y la hora de acceso y sobre qué información o documento se ha accedido.

- Se incluirá la actividad de los usuarios y el tipo de acceso. (Solo Lectura, Creación, Modificación, Supresión).
- Deberá registrarse si se ha autorizado o denegado el acceso.

- De existir **personal ajeno** al responsable con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

3.2 MEDIDAS RELATIVAS A LA ACTUALIZACION DE SOFTWARE

Para garantizar la protección de los sistemas de información de la organización, es necesario mantener los sistemas, aplicaciones y soluciones de seguridad en un nivel correcto de actualización.

Se establecen las siguientes medidas de seguridad en lo relativo a la **actualización de software.**

- Se realizará un inventario de todo el software y el *firmware* instalado y que debe ser actualizado.
- El personal responsable de los sistemas aplicará la Política de actualizaciones de software, revisando los equipos periódicamente para garantizar su actualización o activando las actualizaciones automáticas.
- **Realizar revisiones** periódicas de los sitios web de proveedores de las aplicaciones y en especial, de las notificaciones de seguridad, para identificar las nuevas actualizaciones de software y los nuevos problemas de seguridad que puedan afectar a nuestros sistemas informáticos.
- **Aplicar las actualizaciones** necesarias conforme a las instrucciones del fabricante. Se deberán instalar actualizaciones provenientes de fuentes confiables.
- **Verificar** que el sistema está funcionando correctamente una vez aplicada la actualización.
- Se deberán instalar actualizaciones provenientes de fuentes confiables.
- **Se deberá disponer de un entorno de prueba donde instalar las actualizaciones**. Es obligatorio realizarlo así en las actualizaciones de aplicaciones críticas instaladas en servidores. (servidores web, servidores de correo, etc.).
- Se deberá disponer antes de cualquier cambio, de copias de seguridad recientes localizadas y probadas.
- Se realizará un registro de las actualizaciones que se han instalado en nuestros sistemas. De esta forma se tendrá en todo momento un conocimiento exhaustivo del software operativo en nuestros equipos**.**

3.3 MEDIDAS RELATIVAS A LA GESTIÓN Y CONTROL DE SISTEMAS ANTIMALWARE

En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus o antimalware que evite en la medida posible el robo y destrucción de la información y datos personales.

Las vías de contagio por malware son numerosas, destacando entre otras:

- Las descargas de ficheros de todo tipo, adjuntos en correos o desde páginas web;
- La navegación por webs de dudosa fiabilidad;
- y la utilización de dispositivos ajenos, por ejemplo, pendrives

A continuación, se establecen las siguientes medidas de seguridad en lo relativo a la **gestión y control de sistemas antimalware.**

- El personal responsable de los sistemas aplicará la **Política Antimalware** que incluya la instalación y actualización de herramientas antimalware en todos los equipos y sistemas, y su revisión periódica de manera que se garantice la protección antimalware.

- **Política general de buenas prácticas para el control de malware.** Con el fin de reforzar las medidas establecidas para el control del malware es conveniente tener concienciada a la plantilla en los siguientes aspectos:

  - **Se deben considerar todos los contenidos y las descargas como potencialmente inseguros** hasta que no sean convenientemente analizados por una herramienta de detección de malware.
  - No se ejecutarán ficheros descargados de servidores externos, de soportes móviles no controlados o adjuntos a correos, sin haber sido previamente analizados.
  - No se configurará el programa cliente de correo electrónico para la ejecución automática de contenido recibido por correo.
  - No se podrá alterar la configuración de seguridad establecida para los sistemas y equipos de tratamiento de información.
  - Debe utilizarse únicamente el software permitido por la organización. Este además debe estar convenientemente actualizado.
  - Para evitar la recepción de spam se deben seguir las directrices incluidas en la política de correo electrónico.

3.4 MEDIDAS RELATIVAS A SISTEMA DE CORTAFUEGOS O FIREWALL

Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

3.5 MEDIDAS RELATIVAS A LA GESTIÓN DE SOPORTES Y BORRADO SEGURO DE INFORMACIÓN

La gestión de soportes persigue evitar que se revele, modifique o elimine de forma no autorizada la información almacenada en los mismos**.**

Se establecen las siguientes medidas de seguridad en lo relativo a **gestión de soportes y borrado seguro de información:**

- **Inventario de activos**. Es necesario que se realice y mantenga actualizado un **inventario** en el que los activos se encuentren clasificados y gestionados de la manera correcta.
  Se debe incluir dentro del inventario:

    - Identificador interno del activo
    - Características básicas
    - Clasificación de seguridad
    - Responsable del activo.
    - Información contenida
    - Proveedor, garantía y datos de mantenimiento.
    - Ubicación física
    - Fecha de destrucción cuando sea el caso.

- **Gestión de soportes**. Se supervisarán los dispositivos que almacenan información corporativa, en particular los que se usan para realizar las copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, reparación, sustitución, etc.

- **Eliminación de la Información**. Cuando la información deja de ser necesaria para la organización, es necesario destruirla de forma segura. También debemos utilizar el borrado seguro cuando queremos:
    - Reutilizar un soporte
    - Deshacernos de un soporte que se ha quedado obsoleto

  En **soportes no electrónicos y soportes magnéticos**:
    - Para eliminar la información de este tipo de soportes se deberá utilizar la opción de triturado como modo seguro de eliminación.

  Para la **reutilización de soportes electrónicos**:
    - Si queremos reutilizar un soporte que ya contiene datos, debemos utilizar la opción de sobreescritura para garantizar un borrado total de la información.
      La sobreescritura se puede utilizar en todos los dispositivos regrabables (discos duros, memorias USB, etc.) siempre que el dispositivo no esté dañado.

  Antes de **deshacernos de soportes electrónicos**:
    - Para desechar algún soporte de almacenamiento porque ya no funcione o porque se haya quedado obsoleto se deberán utilizar los métodos de desmagnetización o destrucción física. Cualquiera de estos dos métodos imposibilita la reutilización del dispositivo.
    - Prestar una especial atención cuando queramos deshacernos de dispositivos móviles (*smartphones*, tabletas, etc.) ya que también pueden contener información confidencial.

- **Destrucción certificada**: existe la opción de contratar una empresa que realice una destrucción certificada. Esta empresa se encargará de llevar a cabo el proceso de eliminación de la información garantizando la gestión y control de recogida, transporte y destrucción del material confidencial. Después de llevar a cabo la destrucción, la empresa emite un certificado que garantiza la validez de todo el proceso.

3.6 MEDIDAS RELATIVAS AL ALMACENAMIENTO EN DISPOSITIVOS EXTRAIBLES

Los dispositivos de almacenamiento extraíbles o portátiles (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.) permiten una transferencia rápida y directa de información, pero se deben aplicar una serie de medidas de seguridad ya que son susceptibles al robo, manipulación, extravío e infección por virus.

La entidad debe decidir si se permite el uso de dispositivos de almacenamiento externo y en qué situaciones pueden utilizarse y qué tipo de información se permite guardar en ellos.

Si se necesita almacenar información sensible o confidencial se utilizarán dispositivos externos corporativos debidamente protegidos.

En el caso de que se permita el uso de dispositivos personales, se aplicarán las normas de seguridad recogidas en la política correspondiente.

En definitiva, debemos aplicar las medidas de seguridad que este tipo de dispositivos requieren, así como concienciar a los empleados para su buen uso. De esta forma protegeremos tanto la información contenida en ellos como la de los dispositivos a los que se conectan.

Se establecen las siguientes medidas de seguridad en lo relativo al **uso y gestión de dispositivos extraíbles:**

- Se deberá elaborar un protocolo que regule el uso de dispositivos extraíbles que incluya:
  - Registro de los dispositivos autorizados;
  - Registro de Usuarios.
  - Definir en qué condiciones o casos se permite su uso;
  - Definir cómo se accede y si la información debe ir cifrada;
  - Establecer las configuraciones de seguridad necesarias para poder utilizarlos, etc.

- **Se aplicarán medidas técnicas para garantizar un almacenamiento seguro de la información.** Estas medidas podrán aplicarse tanto sobre el dispositivo extraíble como sobre los dispositivos a los que se conecta o sobre los documentos. Por ejemplo:

  Sobre el dispositivo extraíble:
  - Programar cambios periódicos de contraseña de acceso al dispositivo.

  Sobre los dispositivos a los que se conectan:
  - Desactivar la opción de autoarranque en los equipos para no permitir posibles ejecuciones automáticas no deseadas cuando los dispositivos extraíbles son enchufados.
  - Deshabilitar por defecto los puertos USB y habilitarlos para el personal que necesite dicha funcionalidad.

  Sobre los documentos que se transfieren:
  - Implementar mecanismos de cifrado de la documentación para evitar el acceso no autorizado por terceros en caso de pérdida o sustracción.

- Se tendrá que comunicar esta normativa y asegurarnos de que los usuarios la conocen y se comprometen a cumplirla antes de utilizar dispositivos extraíbles en el entorno de trabajo.

- **En caso de traslado o distribución de documentos físicos o en papel**, se realizará adoptando las medidas de custodia que sean más adecuadas para evitar el acceso no autorizado por terceros en caso de pérdida o sustracción**.**
- **En caso que los documentos o archivos** con datos de carácter personal **se envíen a través de correo electrónico,** los documentos **deberán ir adjunto al correo y ser encriptados** con contraseña, para evitar el acceso no autorizado. Dicha contraseña deberá ser comunicada al destinatario de forma que solo sea conocida por él.

3.7 MEDIDAS RELATIVAS A LAS COPIAS DE SEGURIDAD

Una copia de seguridad, es un proceso por el cual se duplica la información existente de un soporte informático a otro con la finalidad poder recuperar los datos en el caso de que el sistema de información pueda verse involucrado en situaciones como robos, incendios, inundaciones, fallos eléctricos, rotura o fallo del soporte informático, virus, borrados accidentales de información, traslado de datos a otra ubicación y poder garantizar la continuidad de la actividad.

Por ello, se debe definir e implantar por parte de la entidad **un sistema para la gestión de las copias de seguridad**, incluyendo pruebas de restauración periódica para garantizar que se realizan adecuadamente.

Se establecen las siguientes medidas de seguridad en lo relativo al **gestión de copias de seguridad:**

- Se identificará toda la información necesaria a través de un inventario, para reanudar la actividad en caso de desastre o de incidente grave.

El inventario incluirá:

- Responsables de realización de las copias de seguridad.
- Contenido de las copias.
- Tipo de Copias
- Software necesario.
- Tipo de soportes
- Periodicidad de las copias
- Vigencia de las copias
- Ubicación
- Pruebas de restauración

- **Responsables** La entidad identificará a los **responsables** de realizar las copias de seguridad.

- Deberá existir un control de acceso restringido a las mismas por personal autorizado.

- **Contenido de las copias de seguridad**. Se establecerá el contenido de la copia de seguridad, identificándose todos los datos e información que sea necesaria para reanudar la actividad en caso de desastre o de incidente grave. Se debe permitir descartar información sin relación directa con la actividad o ficheros históricos de los que ya existen copias.

- **Frecuencia de las copias de seguridad**. Se establecerá la **frecuencia** con la que se van a realizar los procesos de copia, teniendo en cuenta:

  - La variación de los datos generados;
  - El coste de almacenamiento.

- Se establecerán preferentemente procesos automáticos de copia de seguridad diarias que serán realizados al término de la jornada de trabajo.
- **Cifrado**. Se establecerá un sistema de cifrado de las copias de seguridad, para garantizar la confidencialidad e integridad de la información almacenada.

- **Tipo de Copia de Seguridad**. Se establecerá el **tipo de copia de seguridad** más adecuado en nuestra actividad, pudiendo ser:

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

  - **Incremental**. En las copias incrementales, únicamente **se copian los archivos que se hayan añadido o modificado desde la última copia realizada**, sea total o incremental.

  - **Diferencial**. 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.**

- **Vigencia de las Copias de Seguridad**. Se deberá establecer el periodo de tiempo durante el cual la copia va a tener validez y por tanto se va a conservar**.** Se deberá decidir cuánto tiempo conservar las copias en función de:

  - Si la información almacenada sigue vigente;
  - La vida útil del soporte en el que realizan las copias;
  - La necesidad de conservar varias copias anteriores a la última realizada.

- **Ubicación Copias de Seguridad**. Será necesario buscar una ubicación adecuada para guardar las copias, con los siguientes criterios:

  - Se deberá tener al menos una copia en una ubicación distinta de aquélla en que se encuentre el servidor con los ficheros originales.

- Es recomendable hacer más de una copia de seguridad y utilizar diferentes soportes de almacenamiento de las copias, para protegerlas de distintos riesgos y poder garantizar siempre la disponibilidad de al menos una de ellas.
- Se restringirá el acceso a las ubicaciones donde se encuentran las copias exclusivamente a las personas autorizadas.

- Si se decidiera realizar copia en la nube, se adoptarán las siguientes precauciones para garantizar la seguridad de la información:
  - Se deberá cifrar la información confidencial antes de realizar la copia;
  - Se deberá firmar Acuerdos con el proveedor, que garanticen la disponibilidad, integridad, confidencialidad y control de acceso a las copias.

- **Se establecerán los soportes de almacenamiento de las copias de seguridad** teniendo en cuenta los siguientes aspectos:
  - Complejidad de la organización.
  - Volumen de información que queramos salvaguardar.
  - Sistema o tipo de copia seleccionado.
  - Inversión
  - Durabilidad del soporte.

- Los soportes pueden ser físicos como Memorias o Discos Duros Externos USB, que estén conectados al servidor o equipo central donde se encuentran alojados los ficheros de datos o virtuales como son el almacenamiento de las copias en servidores de terceros Cloud.

- **Control de los soportes de copia.** Se deberá etiquetar e identificar los soportes dónde se realizan las copias de seguridad de manera que se pueda llevar un registro de los soportes sobre los que se ha realizado alguna copia.

- **Destrucción de soportes de copia.** Se adoptarán las medidas adecuadas para desechar de manera segura los soportes utilizados en las copias de seguridad. para asegurar que la información que contienen no podrá ser recuperada posteriormente.

- **Procedimientos de copia y restauración.** Se han de elaborar y aplicar procedimientos que describan cómo hacer las copias y cómo restaurarlas.
  - Se han de revisar periódicamente y con cada cambio importante del inventario de activos de información.
  - **Se comprobará que las copias están bien realizadas y que pueden restaurarse.** Se fijará una periodicidad para realizar pruebas de restauración para garantizar que la información necesaria para la continuidad de la actividad puede ser recuperada en caso de desastre.
  - Se debe documentar el proceso de realización y restauración de copias. Esto permitirá agilizar el proceso de recuperación ante una contingencia o ausencia del personal habitual.

3.8 MEDIDAS RELATIVAS AL USO DE DISPOSITIVOS MÓVILES NO CORPORATIVOS

El uso de dispositivos personales (portátiles, *smartphones*, *etc.)* propiedad del usuario, en el ámbito corporativo es lo que se conoce como *BYOD* (*Bring Your Own Device / Utilización de dispositivos propios.*). Se trata de una práctica muy frecuente, por lo tanto, se debe prestar una especial atención para que su uso no comprometa la seguridad de la información de la entidad.

Se establecen las siguientes medidas de seguridad en lo relativo al **uso de dispositivos móviles no corporativos.**

- **Normas y procedimientos BYOD.** La entidad elaborará normas y procedimientos específicos que regulen el uso de dispositivos BYOD autorizados, en qué condiciones se permite su uso, cómo se accede a la información, configuraciones de seguridad necesarias para poder utilizarlos.

- **Se recomienda prohibir de uso de dispositivos manipulados.**

- **Se informará a los usuarios sobre el uso seguro de los dispositivos en relación a:**
  - Configurar los parámetros de seguridad de los dispositivos;
  - Actualizar tanto el sistema operativo como las aplicaciones periódicamente.
  - No instalar aplicaciones que exijan permisos que pongan en riesgo la información confidencial (acceso a la agenda, geolocalización, etc.);
  - Bloquear los dispositivos con contraseña y activar el bloqueo automático tras un periodo corto de inactividad;
  - No desatender los dispositivos.

- **Limitar el acceso a redes desconocidas.** Se recomienda optar por la conexión de datos de su móvil 3G/4G/. cuando las redes inalámbricas disponibles sean desconocidas. Las redes wifi deben considerarse inseguras.

- **Controlar el almacenamiento de datos corporativos.** Las aplicaciones personales en los dispositivos móviles para el tratamiento de datos en la nube no son tan seguras como las empresariales por lo que hay que prestar especial atención a este intercambio de archivos. Se puede permitir la consulta de información en la nube, pero se recomienda no actualizarla desde estos dispositivos personales.

- **Proceso de borrado de la información.** Se establecerá el proceso a seguir para entregar/eliminar la información en estos dispositivos cuando el usuario abandona la empresa.

- **Control de acceso a la red.** El acceso a la red corporativa a través de dispositivos personales debe estar integrado en el sistema de control de accesos. Para mayor seguridad la empresa puede proporcionar a sus empleados acceso mediante red privada virtual (VPN) que cifra las comunicaciones.

- **Cifrado de información**. Implementaremos en los dispositivos mecanismos de cifrado de la documentación además de los de autenticación de usuarios.

- **Extravío de dispositivos.** Ante la posibilidad de pérdida o extravío de este tipo de dispositivos, estableceremos las siguientes medidas:
  - **Localización** mediante GPS, wifi o la información de la antena de telefonía con la que esté conectado el dispositivo.
  - **Borrado remoto de datos**: esta opción permite que los datos contenidos en el dispositivo se borren de manera remota, impidiendo su utilización por un usuario no legítimo.

- **Desconexión wifi y Bluetooth.** Se desactivará en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no sean necesarios.

3.9 MEDIDAS RELATIVAS AL USO DEL CORREO ELECTRONICO

El correo electrónico es una herramienta de comunicación imprescindible para el funcionamiento de una empresa. Como toda herramienta de comunicación corporativa es necesario definir su uso correcto y seguro.

Para evitar los riesgos que conlleva el uso del correo corporativo debemos concienciar a nuestros empleados o usuarios para que hagan un uso seguro del mismo e informarles de las normas que regulan las condiciones y circunstancias en las que puede utilizarse, así como las posibles sanciones y acciones a tomar en caso de detectarse un mal uso.

Se establecen las siguientes medidas de seguridad en lo relativo al uso del correo electrónico.

- **Normativa de uso de correo electrónico.** La entidad dispondrá de una normativa referente al uso del correo electrónico que el empleado o usuario aceptará al incorporase a su puesto de trabajo.

- Se informará de la prohibición del uso del correo corporativo con fines personales que no tengan que ver con la entidad. El contenido del correo deberá cumplir con la normativa y su uso inadecuado podrá conllevar sanciones. El correo corporativo puede ser supervisado por la dirección de la empresa, incluyendo una cláusula en la normativa que firma el empleado.

- Se informará al usuario que tenga asignada una cuenta de correo electrónico corporativa que este será responsable de las actividades realizadas con esa cuenta y de su respectivo buzón. No permitiendo el uso de esa cuenta a personas distintas del usuario de la misma.

- Si por cualquier causa se produjese este hecho, se presumirá salvo prueba en contrario que el usuario es el único responsable de los actos realizados a través de esa cuenta de correo.

- Se informará al usuario que se **deberá comprobar periódicamente que las direcciones de correos electrónicos de los contactos están actualizadas** en las bases de datos que las contengan.

- Se informará al usuario que **antes del envío de cualquier correo electrónico confirmará que el destinatario nos ha dado su autorización para el envío de correos electrónicos** y en caso de duda el responsable del tratamiento o persona en quien delegue.

- **Utilizar la copia oculta (CCO)**. Cuando se envíen mensajes a múltiples destinatarios, se utiliza la opción de copia oculta, (CCO) en lugar de la copia normal CC. La copia oculta impide que los destinatarios vean a quién más ha sido enviado. El correo electrónico es un dato personal de nuestros clientes y usuarios, que no debemos utilizar para otros fines distintos de aquellos para los que fue solicitado. No se debe divulgar o comunicar a terceros sin su consentimiento.

- Se informará al usuario que **tiene estrictamente prohibido enviar mensajes de correo de forma indiscriminada o participar en cadenas de mensajes.**

- **Antimalware y antispam.** Se deberá instalar aplicaciones antimalware y activar los filtros antispam tanto en el servidor como en el cliente de correo. Estos filtros permitirán que los correos maliciosos sean identificados y no lleguen a la bandeja de entrada evitando así su posible apertura

- **Cifrado.** Se deberá instalar una tecnología de cifrado para proteger la información confidencial.

- **Correos sospechosos.** El usuario que reciba en su bandeja de entrada correos de remitentes no conocidos o que resulten sospechosos, evitaran su apertura procediendo directamente a su eliminación**.** Se puede sospechar cuando:
  -el cuerpo del mensaje presente cambios de aspecto (logotipos, pie de firma, etc.) con respecto a los mensajes recibidos anteriormente por ese mismo remitente;
  -el mensaje contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual;
  -se soliciten credenciales de acceso a una web o aplicación (cuenta bancaria, etc.).

- **Identificación del remitente.** El usuario no abrirá un correo sin identificar el remitente. Si el remitente no es un contacto conocido habrá que prestar especial atención ya que puede tratarse de un correo malicioso.
  Si el remitente es un contacto conocido, pero por otros motivos (cuerpo del mensaje, archivos adjuntos, enlaces...) sospechas que se ha podido suplantar su identidad, debes contactar con éste por otro medio para confirmar su identidad.

- **Análisis de adjuntos**. Al recibir un mensaje con un adjunto, este se debe analizar cuidadosamente antes de abrirlo. Aunque el remitente sea conocido puede haber sido suplantado y no apercibirnos. La descarga de adjuntos maliciosos podría infectar nuestros equipos con algún tipo de malware. Tener el antivirus activo y actualizado puede ayudarnos a identificar los archivos maliciosos.

- **No responder al spam.** No se responderá al mismo, ya que confirmaremos que la cuenta está activa. Se deberá agregar a tu lista de spam y elimínalo. Tampoco lo reenviaremos en caso de cadenas de mensajes.

- **Evitar las redes públicas** Evitar utilizar el correo electrónico desde conexiones públicas (wifi de una cafetería, etc.). Como alternativa, es preferible utilizar redes de telefonía móvil como el 3G o 4G.

3.10 MEDIDAS RELATIVAS AL USO DE INTERNET

Se establecen las siguientes medidas de seguridad en lo relativo al uso del correo electrónico.

- Se informará al usuario **que este será el responsable de las sesiones iniciadas en Internet desde su puesto de trabajo**. No permitiendo el uso de esa sesión a personas distintas del usuario de la misma.

- Si por cualquier causa se produjese este hecho, **se presumirá salvo prueba en contrario que el usuario es el único responsable de los actos realizados a través de esa sesión**.

- Se informará al usuario **que este solo usará las sesiones de internet con fines estrictamente laborales**, prohibiéndose su uso para otros fines, salvo que ese uso esté expresamente autorizado por el responsable de los tratamientos o persona en quien se delegue.

- Se informará al usuario **que este no accederá a sitios web de dudosa confianza**, para evitar riesgos de contagio de programas maliciosos.

- Se informará al usuario **que este tiene expresamente prohibido el acceso, descarga o almacenamiento de páginas con contenidos ilegales, inadecuados o que atenten a la moral y las buenas costumbres**.

- Se informará al usuario que este **tiene expresamente prohibido la instalación en su puesto de trabajo de software descargado de internet**, sin la correspondiente autorización del responsable de los tratamientos o persona en quien se delegue.

- Se informará al usuario **que no se modificará las configuraciones de los navegadores del equipo, ni la activación de servidores o puertos** sin la autorización del responsable de los tratamientos o persona en quien se delegue.

- Se informará al usuario **que no se proporcionará la clave WiFi** de los centros o servicios de la entidad a personas ajenas a la misma.

3.11 MEDIDAS RELATIVAS AL USO DE MENSAJERIA INSTANTANEA

Se establecen las siguientes medidas de seguridad en lo relativo al uso mensajería instantánea.

- Se informará al usuario **que no se hará uso de mensajería instantánea como herramienta de comunicación dentro del entorno laboral,** salvo que ese uso esté expresamente autorizado por el responsable de los tratamientos o persona en quien se delegue.

- En caso de que ese uso este autorizado, estas aplicaciones **deberán ser usadas desde terminales de la entidad y nunca desde terminales personales,** salvo que ese uso esté expresamente autorizado por el responsable de los tratamientos o persona en quien se delegue.

- Se informará al usuario **que no se hará uso de mensajería instantánea para mantener conversaciones con contenido confidencial o envío de archivos o documentos sensibles (datos de salud, etc.).** No son sistemas que reúnan medidas de seguridad adecuadas para estos casos.

- En caso de que ese uso este autorizado, **solo se usará para mantener conversaciones privadas y no a través de grupos.,** salvo que este expresamente autorizado ese uso por el responsable del tratamiento o por la persona en quien delegue.

- **Para la comunicación del mismo mensaje a varios destinatarios simultáneamente, se utilizará la función de Listas de Difusión o Distribución, que** evitan comunicar datos al resto de destinatarios.

- **En caso de que sea autorizada la creación de grupos, previamente se habrá solicitado el consentimiento por escrito de los integrantes para su inclusión en el mismo.**

- **Está terminantemente prohibido crear grupos con menores de edad.**

3.12 MEDIDAS RELATIVAS AL USO DE IMÁGENES DENTRO DE AMBITO DE ACTIVIDAD DE LA ENTIDAD

Las imágenes de personas ya sean en fotografía o video son consideradas datos de carácter personal y su uso o difusión por parte de la entidad en distintos medios debe estar expresamente autorizada por las personas interesadas o en su caso por sus representantes legales,

Se establecen las siguientes medidas de seguridad en lo relativo a la captación y uso de fotografías y videos dentro de ámbito de actividad de la entidad.

- Las imágenes ya sean en fotografía o video captadas dentro del ámbito de actividad de la entidad para poder ser usadas o difundidas en distintos medios de comunicación solo

podrán ser realizadas con dispositivos propiedad de la entidad y por las personas designadas por la misma para ese fin, para poder establecer protocolos de control y seguridad sobre las mismas.

- Se llevará un control para que las personas trabajadoras no difundan o envíen fotografías o videos de personas dentro del ámbito de actividad la entidad a través de páginas web, redes sociales, mensajería instantánea o de cualquier otro medio de difusión en nombre de la entidad sin estar expresamente autorizado por la misma.