POLÍTICA DE SEGURIDAD APLICADA AL TRATAMIENTO DE DATOS PERSONALES

FUNDACIÓN IMPULSARSE PARA EL DESARROLLO DEL EMPLEO Y LA INTEGRACIÓN SOCIAL

1. OBJETO Y ÁMBITO DE APLICACIÓN

Esta Política recoge las normas, obligaciones y buenas prácticas que deben ser conocidas y respetadas por toda persona que acceda a los sistemas, datos, instalaciones o información de la organización, con independencia de su relación contractual (empleados, becarios, contratistas, proveedores de servicios o colaboradores externos). Deberá estar a disposición de todo el personal, quien podrá acceder a la misma en cualquier momento, debiendo velar por su cumplimiento en el desempeño de sus funciones.

El incumplimiento de las directrices aquí establecidas podrá derivar en responsabilidades disciplinarias, civiles y/o penales conforme a la normativa vigente.

2. RESPONSABILIDADES

2.1. Dirección

La Dirección es responsable de aprobar esta política, dotarla de recursos y velar por su cumplimiento. Designa al Responsable de Seguridad como punto de contacto interno.

2.2. Responsable de Seguridad

Gestiona los incidentes de seguridad, mantiene actualizado el presente manual, imparte formación y resuelve las dudas del personal.

2.3. Todo el personal

Toda persona que tenga acceso a la información y a los sistemas de la organización será responsable del cumplimiento íntegro de las disposiciones recogidas en el presente manual, así como de actuar conforme a las políticas y procedimientos internos establecidos en materia de seguridad y protección de datos.

Asimismo, todos los equipos, dispositivos, aplicaciones y sistemas corporativos deberán utilizarse con la máxima diligencia, responsabilidad y confidencialidad, quedando prohibido su uso para fines distintos de los estrictamente relacionados con la actividad laboral o profesional autorizada por la organización.

3. RECURSOS PROTEGIDOS

Con el objeto de garantizar la seguridad, integridad, disponibilidad y confidencialidad de los datos personales tratados por la organización, se consideran recursos protegidos todos aquellos activos, elementos, sistemas y entornos que intervengan, directa o indirectamente, en el tratamiento de dichos datos.

A continuación, se relacionan los principales recursos protegidos:

- Los centros de tratamiento de datos, oficinas, dependencias, instalaciones y locales donde se encuentren ubicados los ficheros, expedientes, equipos o soportes que contengan datos personales, incluyendo tanto documentación en formato físico como electrónico.
- Los soportes de almacenamiento, físicos o digitales, que contengan datos personales, tales como discos duros, servidores, dispositivos USB, copias de seguridad, sistemas de

almacenamiento en red, equipos portátiles, dispositivos móviles y cualquier otro medio susceptible de almacenar información personal.

- Los puestos de trabajo ya sean locales, móviles o remotos, desde los cuales se pueda acceder a datos personales o realizar cualquier operación de tratamiento sobre los mismos, incluyendo ordenadores, terminales, teléfonos corporativos y dispositivos utilizados en modalidad de teletrabajo.
- Los servidores, infraestructuras tecnológicas y entornos de sistemas operativos y comunicaciones en los que se encuentren alojados los ficheros, bases de datos o aplicaciones que contengan o gestionen datos personales.
- Los sistemas informáticos, aplicaciones, programas, plataformas y herramientas tecnológicas utilizadas para la recogida, registro, organización, conservación, consulta, modificación, transmisión, bloqueo, supresión o cualquier otra operación de tratamiento de datos personales.
- Las redes de comunicación internas y externas, servicios en la nube, conexiones remotas, sistemas de intercambio de información y demás infraestructuras de telecomunicaciones empleadas para el tratamiento o transmisión de datos personales.
- Los sistemas de autenticación, control de accesos, monitorización, registro de actividad y demás mecanismos de seguridad implantados para proteger el acceso y uso de los datos personales.
- Cualquier otro recurso, activo, elemento físico o lógico, infraestructura o servicio que, aun no estando expresamente identificado en el presente documento, intervenga o pueda intervenir en el tratamiento de datos personales y cuya protección resulte necesaria para garantizar el cumplimiento de la normativa vigente en materia de protección de datos.

4. MARCO NORMATIVO

- Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

5. PRINCIPIOS RELATIVOS AL TRATAMIENTO

Los principios que rigen el tratamiento de datos personales se encuentran regulados en el **art. 5 del RGPD** y en los **arts. 4 y ss. de la LOPDGDD**. Constituyen el pilar fundamental sobre el que debe asentarse cualquier operación de tratamiento llevada a cabo en la entidad y, por tanto, deben ser conocidos y aplicados por todos los empleados que, en el ejercicio de sus funciones, traten datos personales de empleados, clientes, proveedores o cualquier otra persona física.

A continuación, se ofrece una visión de conjunto de los seis principios del art. 5 RGPD, así como del principio de responsabilidad proactiva (accountability), que se desarrollan en detalle en los apartados siguientes:

BASE LEGAL	PRINCIPIO	DESCRIPCIÓN RESUMIDA
Art. 5.1.a) RGPD	**Licitud, lealtad y transparencia**	El tratamiento debe tener base jurídica válida e informar al interesado.
Art. 5.1.b) RGPD	**Limitación de la finalidad**	Los datos solo se usarán para los fines declarados al recabarlos.
Art. 5.1.c) RGPD	**Minimización**	Solo se recabarán los datos estrictamente necesarios.
Art. 5.1.d) RGPD	**Exactitud**	Los datos se mantendrán actualizados y se corregirán sin demora.
Art. 5.1.e) RGPD	**Limitación del plazo de conservación**	Los datos no se conservarán más tiempo del necesario.
Art. 5.1.f) RGPD	**Integridad y confidencialidad**	Se aplicarán medidas técnicas y organizativas para proteger los datos.
Art. 5.2 RGPD	**Responsabilidad proactiva**	El responsable debe poder demostrar el cumplimiento de los principios.

5.1 Principio de licitud, lealtad y transparencia

Regulado en el **art. 5.1.a) RGPD**, este principio exige que todo tratamiento de datos personales cumpla simultáneamente tres requisitos:

- Licitud: el tratamiento debe ampararse en alguna de las bases jurídicas del art. 6.1 RGPD.
- Lealtad: los datos no deben utilizarse de forma contraria a las expectativas razonables del interesado.
- Transparencia: el interesado debe disponer de información clara, accesible y completa sobre el tratamiento.

5.1.1 Bases jurídicas del tratamiento (art. 6.1 RGPD)

Para que un tratamiento sea lícito, debe fundarse en al menos una de las siguientes bases:

Apartado	Base jurídica	Contenido
Art. 6.1.a)	**Consentimiento**	El interesado ha prestado su consentimiento para uno o varios fines específicos.

Apartado	Base jurídica	Contenido
Art. 6.1.b)	**Ejecución de contrato**	El tratamiento es necesario para la ejecución de un contrato o para medidas precontractuales.
Art. 6.1.c)	**Obligación legal**	El tratamiento es necesario para el cumplimiento de una obligación legal del responsable.
Art. 6.1.d)	**Intereses vitales**	El tratamiento es necesario para proteger intereses vitales del interesado u otra persona.
Art. 6.1.e)	**Interés público**	El tratamiento es necesario para el cumplimiento de una misión de interés público o ejercicio de poderes públicos.
Art. 6.1.f)	**Interés legítimo**	El tratamiento es necesario para satisfacer intereses legítimos del responsable o un tercero, salvo que prevalezcan los derechos fundamentales del interesado.

⚠ **Nota**	*La base jurídica debe determinarse antes de iniciar el tratamiento y quedar documentada en el Registro de Actividades de Tratamiento (art. 30 RGPD). No es admisible una selección retroactiva de base jurídica.*

5.1.2 Deber de información: sistema de doble capa (arts. 13-14 RGPD y art. 11 LOPDGDD)

Cuando sea de aplicación la LOPDGDD, la información podrá facilitarse en **dos capas** para facilitar su comprensión por parte del interesado. En el resto de casos, deberá cumplirse directamente con lo dispuesto en los arts. 13 o 14 del RGPD según si los datos han sido facilitados por el propio interesado o por un tercero.

Primera capa (Art. 11 LOPDGDD)	• Identidad del responsable del tratamiento y de su representante (en su caso). • Finalidad del tratamiento. • Posibilidad de ejercer los derechos reconocidos en los arts. 15 y ss. del RGPD. • Existencia de perfilado, si procede. • [Si los datos no proceden del interesado] Categorías de datos y fuentes de procedencia.

Segunda capa (Arts. 13-14 RGPD)	• Identidad completa y datos de contacto del responsable y su representante. • Datos de contacto del DPO, si procede. • Fines del tratamiento y base jurídica. • Intereses legítimos del responsable o de terceros (si la base es el art. 6.1.f). • Destinatarios o categorías de destinatarios. • Transferencias internacionales de datos, si procede. • Plazos de conservación. • Derechos del interesado (arts. 15 a 22 RGPD) y derecho a retirar el consentimiento. • Derecho a reclamar ante la AEPD. • Existencia de cesiones a terceros y de decisiones automatizadas o perfilado. • [Si los datos provienen de terceros] Categorías de datos y fuente de procedencia.

Plazos de información (art. 14 RGPD): cuando los datos no procedan directamente del interesado, la información deberá facilitarse en el plazo máximo de un mes desde su obtención. Si los datos se utilizan para contactar al interesado, la información deberá proporcionarse en ese mismo momento. Si los datos van a comunicarse a un tercero, la información deberá facilitarse antes de dicha comunicación.

📋 **Forma**	*La información debe presentarse de forma concisa, transparente, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo. Podrá facilitarse por medios electrónicos cuando la complejidad tecnológica del tratamiento así lo aconseje (considerando 58 RGPD).*

5.2 Principio de limitación de la finalidad

Regulado en el **art. 5.1.b) RGPD**, este principio impide que los datos personales sean tratados con finalidades distintas o incompatibles con aquellas para las que fueron recabados originalmente.

En la práctica, este principio impone las siguientes obligaciones:

- Determinar y documentar la finalidad del tratamiento de forma explícita antes de iniciar la recogida de datos.
- No utilizar los datos para finalidades ulteriores incompatibles con la finalidad original sin una base jurídica habilitante adicional.

- Informar al interesado y, cuando sea necesario, recabar su consentimiento si se decide ampliar o cambiar las finalidades del tratamiento.

Compatibilidad	*Para valorar si una nueva finalidad es compatible con la original, el art. 6.4 RGPD establece que deberán tenerse en cuenta, entre otros factores: la vinculación entre finalidades, el contexto en que se recabaron los datos, su naturaleza y las posibles consecuencias para el interesado.*

5.3 Principio de minimización de datos

El **art. 5.1.c) RGPD** exige que los datos tratados sean adecuados, pertinentes y limitados a lo estrictamente necesario en relación con los fines del tratamiento.

Este principio obliga a:

- Identificar previamente qué datos son imprescindibles para cumplir la finalidad declarada.
- Excluir todo dato que pueda considerarse excesivo, irrelevante o no necesario para dicha finalidad.
- Revisar periódicamente los formularios, sistemas y procesos de recogida de datos para detectar y eliminar campos innecesarios.

Aplicación práctica	*Antes de diseñar cualquier formulario o proceso de recogida de datos, debe realizarse un ejercicio de necesidad: ¿es imprescindible este dato para cumplir la finalidad? Si la respuesta no es un 'sí' claro, el dato no debe recabarse.*

5.4 Principio de exactitud

Regulado en el **art. 5.1.d) RGPD**, este principio obliga al responsable del tratamiento —y en su caso al encargado— a adoptar todas las medidas razonables para garantizar que los datos personales sean exactos y estén actualizados.

Las principales obligaciones derivadas de este principio son:

- Rectificar o suprimir sin dilación indebida los datos que resulten inexactos o incompletos en relación con los fines del tratamiento.
- Implementar mecanismos que permitan a los interesados comunicar y corregir errores en sus datos.
- Establecer procedimientos internos de revisión periódica de la exactitud de los datos.

Este principio se instrumentaliza a través de dos derechos reconocidos por el RGPD:

Derecho de rectificación *Art. 16 RGPD*	Derecho a solicitar la corrección o completitud de los datos personales cuando sean erróneos o incompletos para los fines del tratamiento.
Derecho de supresión *Art. 17 RGPD*	Derecho a obtener la supresión de los datos sin dilación indebida cuando concurra alguna de las siguientes causas: • Retirada del consentimiento otorgado para el tratamiento. • Ejercicio del derecho de oposición sin que concurran motivos legítimos prevalentes. • Tratamiento ilícito de los datos. • Obligación legal de supresión. • Datos obtenidos en el contexto de servicios de la sociedad de la información.

5.5 Principio de limitación del plazo de conservación

El **art. 5.1.e) RGPD** establece que los datos personales no deben conservarse durante más tiempo del necesario para cumplir las finalidades para las que fueron recabados.

Este principio impone las siguientes obligaciones:

- Determinar plazos de conservación concretos para cada categoría de datos y cada finalidad de tratamiento, debidamente documentados.
- Aplicar procedimientos de supresión o anonimización una vez vencido el plazo de conservación.
- Respetar los plazos legales de conservación derivados de normativa sectorial (laboral, fiscal, mercantil, etc.), que pueden coexistir con el plazo general.

📌 **Excepción**	*El mismo art. 5.1.e) RGPD prevé que los datos recabados con finalidades de archivo en interés público, investigación científica o histórica, o fines estadísticos podrán conservarse durante plazos más largos, siempre que se apliquen las garantías técnicas y organizativas adecuadas (art. 89 RGPD).*

📋 **Buena práctica**	*La entidad debe mantener un cuadro de retención documental que recoja, para cada actividad de tratamiento, el plazo de conservación aplicable, la normativa que lo sustenta y el procedimiento de destrucción segura a aplicar al vencimiento del plazo.*

5.6 Principio de integridad y confidencialidad

Regulado en el **art. 5.1.f) RGPD**, este principio exige que los datos personales se traten de manera que se garantice su seguridad mediante la aplicación de medidas técnicas y organizativas apropiadas.

El art. 32.1 RGPD concreta las obligaciones de seguridad del tratamiento:

- Seudonimización y cifrado de los datos personales.
- Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Capacidad de restaurar el acceso y la disponibilidad de los datos de forma rápida en caso de incidente físico o técnico.
- Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas implantadas.

A diferencia de la normativa anterior, el RGPD adopta un **enfoque basado en el riesgo y en la privacidad desde el diseño y por defecto** (arts. 25 y 32 RGPD): no establece un catálogo cerrado de medidas, sino que obliga al responsable a evaluar los riesgos del tratamiento y a implementar las medidas proporcionadas al nivel de riesgo identificado, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento.

⚠️ **Obligación proactiva**	*Las medidas de seguridad deben adoptarse antes de iniciar el tratamiento, no a posteriori. Su eficacia debe revisarse y actualizarse periódicamente. El incumplimiento de las obligaciones de seguridad puede dar lugar a la notificación de una brecha de seguridad a la AEPD (art. 33 RGPD) y a los propios interesados (art. 34 RGPD).*

5.7 Principio de responsabilidad proactiva (accountability)

El **art. 5.2 RGPD** añade un séptimo principio transversal: el responsable del tratamiento no solo debe cumplir los principios anteriores, sino que debe estar en condiciones de **demostrarlo** en todo momento.

Las principales herramientas de accountability son:

- Registro de Actividades de Tratamiento (art. 30 RGPD).
- Evaluación de Impacto relativa a la Protección de Datos —EIPD— (art. 35 RGPD), cuando proceda.
- Designación de Delegado de Protección de Datos —DPO— (arts. 37-39 RGPD y 34-37 LOPDGDD), cuando sea obligatorio o voluntario.
- Políticas internas de protección de datos, formación continua y auditorías periódicas.
- Adhesión a códigos de conducta o certificaciones (arts. 40-43 RGPD).

📌 **Clave**	*El principio de accountability convierte el cumplimiento en un proceso continuo y documentado. No basta con cumplir puntualmente; la entidad debe poder acreditar en todo momento —ante la AEPD o ante cualquier interesado— que sus tratamientos se ajustan a la normativa.*

6. INFORMACIÓN AFECTADA

La organización trata diferentes tipologías y categorías de datos personales en función de la actividad desarrollada.

A los efectos de la presente Política, se entenderá por dato personal toda información relativa a una persona física identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante un identificador, dato o conjunto de datos, tales como nombre y apellidos, documento identificativo, dirección postal o electrónica, número de teléfono, dirección IP, datos de localización, identificadores en línea, imágenes, grabaciones de voz, firma, características físicas, económicas, culturales o sociales, así como cualquier otra información que permita su identificación.

Los datos personales tratados por la organización podrán incluir, entre otros, las siguientes categorías:

- Datos identificativos y de contacto.
- Datos académicos, profesionales y laborales.
- Datos económicos, financieros y de facturación.
- Datos de navegación y uso de sistemas informáticos.
- Datos relativos a clientes, proveedores, empleados, colaboradores y terceros vinculados con la actividad de la organización.
- Datos especialmente protegidos o categorías especiales de datos, cuando su tratamiento resulte necesario y se encuentre debidamente legitimado conforme a la normativa vigente.

El tratamiento de cada categoría y tipología de datos personales implicará la aplicación de medidas técnicas y organizativas específicas, atendiendo a la naturaleza de la información, al nivel de riesgo asociado y a las obligaciones legales aplicables en cada caso.

En consecuencia, todas las personas usuarias, empleados, colaboradores o terceros autorizados que intervengan en cualquiera de las actividades de tratamiento deberán cumplir las obligaciones y medidas de seguridad establecidas en la presente política y en la normativa vigente en materia de protección de datos, durante todo el ciclo de vida de los datos personales, desde su obtención o acceso hasta su conservación, bloqueo y supresión definitiva.

Asimismo, los datos personales únicamente podrán ser tratados para las finalidades expresamente autorizadas, garantizando en todo momento los principios de licitud, lealtad, transparencia, minimización de datos, exactitud, limitación de la finalidad, integridad, confidencialidad y responsabilidad proactiva.

7. TRANFERENCIAS INTERNACIONALES DE DATOS PERSONALES

En caso de que fuera necesario realizar transferencias internacionales de datos, se verificará el grado de protección del país de destino y se adoptarán las garantías exigidas por la normativa. En primer lugar, se comprobará si existe una decisión de adecuación aprobada por la Comisión. A falta de la misma, se optará por cualquiera de los mecanismos recogidos en el artículo 46 RGPD, siendo preferible la firma de unas cláusulas contractuales tipo. Tan solo en supuestos excepcionales será alegada una de las excepciones contenidas en el artículo 49 RGPD. En todo caso nada de esto será aplicable cuando la transferencia sea necesaria en un proceso de cooperación internacional con organismos de terceros países y fuera de aplicación cualquier tratado o convenio

internacional, así como la Directiva (UE) 2016/680 y los artículos 43 a 47 de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

8. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

De conformidad con lo establecido por el artículo 30 RGPD, deberá llevarse un registro de las actividades efectuadas bajo la responsabilidad de la organización, debiéndose mantener actualizado frente a los cambios que se sucedan. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país u organismo internacional, incluida la identificación del país u organismo y la garantía aplicada;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Asimismo, cuando se actúe como Encargado del tratamiento igualmente se llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organismo internacional, incluida la identificación del país u organismo y la garantía aplicada;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Dichos registros constarán por escrito, inclusive en formato electrónico.

9. EJERCICIO DE DERECHOS DE LOS INTERESADOS

La normativa de protección de datos permite a los interesados ejercer ante el responsable del tratamiento los derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.
A estos efectos, la entidad ha habilitado los canales que, a continuación, se exponen, para que los interesados remitan las correspondientes solicitudes de ejercicio de derechos dirigiéndose a la organización a través del correo electrónico, dirección postal o cualquier otro canal interno habilitado y comunicado al personal.

Asimismo, con el objetivo de regular y establecer de forma detallada el protocolo de actuación ante el ejercicio de los derechos, la entidad ha desarrollado dicho protocolo de respuesta.

Dicho protocolo de actuación informa acerca del procedimiento establecido para atender los derechos de los interesados y resulta de aplicación tanto a los empleados autorizados a gestionar las solicitudes de derechos interpuestas por los interesados y el personal a su cargo, así como a otros terceros con acceso a datos y a aquellos encargados del tratamiento de la organización, incluido el personal a su cargo, quedando todos ellos sujetos a lo establecido en el citado protocolo, debiendo actuar en todo momento siguiendo las instrucciones establecidas.

10. DIRECTRICES DE SEGURIDAD

10.1 POLÍTICA DE CONTRASEÑAS

El control de acceso mediante contraseñas constituye una de las principales medidas de seguridad para proteger los sistemas y la información de la organización. El uso de contraseñas robustas y seguras resulta esencial, ya que una contraseña débil o comprometida puede poner en riesgo la confidencialidad, integridad y disponibilidad de los datos tratados.

El acceso a los datos personales y a la información confidencial de la organización estará limitado en función de las responsabilidades y funciones asignadas a cada persona trabajadora. Para ello, se establecerán permisos y perfiles de acceso asociados a cada puesto o rol, garantizando que cada usuario únicamente pueda acceder a la información estrictamente necesaria para el desempeño de sus funciones.

Cada usuario dispondrá de unas credenciales de acceso únicas, personales e intransferibles. Queda expresamente prohibido compartir contraseñas o permitir el uso de las credenciales propias por terceros.

Las contraseñas deberán cumplir los criterios de seguridad establecidos por la organización y mantenerse bajo estricta confidencialidad.

10.1.1 Requisitos de las contraseñas

Toda contraseña debe cumplir TODOS los criterios siguientes:

- Mínimo 10 caracteres.
- Combinar letras mayúsculas, minúsculas, números y símbolos (!@#$%)
- Vigencia máxima de 3 meses.
- Única por servicio: nunca reutilizar en distintas plataformas.
- No reutilizar las últimas 5 contraseñas anteriores.

10.1.2. Reglas de uso

✓ HACER	✗ NO HACER
Usar una contraseña diferente para cada sistema o aplicación	Apuntar contraseñas en notas adhesivas, papeles o archivos sin cifrar
Cambiar la contraseña cada 3 meses o inmediatamente si se sospecha de compromiso	Compartir contraseñas con compañeros, ni siquiera con el equipo de IT
Usar un gestor de contraseñas cifrado con doble factor de autenticación (2FA)	Usar datos personales: nombre, fecha de nacimiento, DNI, nombre de mascota
Activar 2FA en todos los servicios que lo permitan	Usar patrones de teclado: qwerty, 123456, asdf, etc.

Notificar inmediatamente al Responsable de Seguridad si sospechas que tu contraseña ha sido comprometida	Activar 'Recordar contraseña' en navegadores de equipos compartidos

11. USO DE DISPOSITIVOS Y PUESTO DE TRABAJO

11.1. Política de escritorio limpio

El puesto de trabajo físico debe mantenerse ordenado para evitar accesos no autorizados a documentos o dispositivos.

✓ HACER	✗ NO HACER
Retirar documentos impresos de la impresora inmediatamente	Dejar documentos confidenciales visibles sobre la mesa al ausentarse
Guardar bajo llave los documentos físicos sensibles al finalizar la jornada	Colocar bebidas sin tapa hermética junto a equipos o documentos
Almacenar en lugar seguro los dispositivos móviles corporativos (portátiles, móviles, tablets)	Dejar memorias USB o discos externos conectados y desatendidos
Destruir documentos obsoletos con destructora de papel	Tirar documentos con datos a la papelera ordinaria sin destruirlos

11.2. Política de pantalla limpia

La pantalla del equipo puede exponer información sensible a personas no autorizadas. Es obligatorio aplicar las siguientes medidas:

- Configurar el bloqueo automático de pantalla a los 10 minutos de inactividad.
- En ausencias cortas (hasta 30 min): bloquear pantalla con Windows + L o equivalente.
- En ausencias largas o al finalizar la jornada: cerrar sesión y apagar el equipo.
- Orientar la pantalla de forma que sólo el usuario pueda ver su contenido.
- No dejar información sensible visible al abandonar el puesto.

12. DISPOSITIVOS ELECTRÓNICOS Y RECURSOS CORPORATIVOS

Todos los dispositivos electrónicos, equipos informáticos y demás recursos corporativos puestos a disposición del empleado deberán utilizarse de conformidad con las medidas de seguridad mínimas establecidas por la organización, entre las que se incluyen, sin carácter limitativo, las siguientes:

✓ HACER	✗ NO HACER
En caso de que el empleado quiera hacer uso del dispositivo para fines personales, deberá contar con la autorización previa y por escrito por parte de la organización	Emplear dichos dispositivos con fines ajenos a la actividad laboral.
Los dispositivos deberán contar con las últimas instalaciones de parches y actualizaciones del sistema operativo, de acuerdo con las actualizaciones periódicas previstas por el desarrollador del sistema.	No utilizar otros dispositivos diferentes a los ofrecidos por la organización para funciones laborales.

Las configuraciones de seguridad deberán venir predeterminadas por el responsable informático de la empresa. En caso de extravío, robo, hurto o acceso no autorizado al dispositivo, el personal deberá comunicar el acontecimiento de forma inmediata a la persona Responsable de Seguridad.	Todo dispositivo que contenga información crítica, confidencial o categorías especiales de datos conforme al RGPD deberá contar con medidas de protección adecuadas que garanticen la seguridad de la información y eviten accesos no autorizados. No conectar a internet los dispositivos corporativos utilizando redes WIFI públicas sin utilizar el acceso VPN corporativo.
Comunicar cualquier incidente de seguridad ocurrido. Trabajar exclusivamente con las herramientas, aplicaciones y sistemas corporativos autorizados y facilitados por la organización para el desempeño de la actividad laboral.	No almacenar ningún dato ni información confidencial de la organización en soportes extraíbles. No instalar, utilizar ni almacenar en local software, aplicaciones o herramientas no autorizadas por la organización, ni recurrir a alternativas no permitidas para el tratamiento de información corporativa o de carácter personal.

13. CORREO ELECTRÓNICO

El correo corporativo es una herramienta de trabajo. Su uso inadecuado es una de las principales vías de entrada de amenazas (phishing, malware) y de fuga de información.

✓ HACER	✗ NO HACER
Verificar siempre el remitente antes de abrir adjuntos o enlaces	Usar el correo corporativo para fines personales o privados
Cifrar los correos que contengan datos personales o información confidencial	Enviar bases de datos, datos personales o información confidencial sin cifrado
Usar CCO (con copia oculta) al enviar correos a múltiples destinatarios	Abrir adjuntos o hacer clic en enlaces de remitentes desconocidos
Reportar correos sospechosos al Responsable de Seguridad	Reenviar correos en cadena o de contenido comercial no autorizado
Cerrar sesión en el correo al usar equipos compartidos o públicos	Configurar el correo corporativo en dispositivos sin autorización

ALERTA: Phishing

Si recibes un correo que solicita credenciales, datos bancarios o acciones urgentes, NO hagas clic ni respondas. Notifícalo de inmediato al Responsable de Seguridad.

14. USO DE INTERNET Y LA RED CORPORATIVA

✓ HACER	✗ NO HACER

Navegar únicamente por sitios necesarios para el desempeño laboral	Conectarse a redes Wi-Fi públicas sin usar la VPN corporativa
Usar la VPN corporativa al conectarse desde redes externas o públicas	Descargar software, música, películas u otro contenido sin autorización
Reportar cualquier comportamiento anómalo de la red o del equipo	Escanear puertos, probar vulnerabilidades o realizar ataques internos/externos
Desconectar dispositivos USB no autorizados inmediatamente	Acceder a la red de invitados con equipos corporativos
	Instalar extensiones de navegador no autorizadas
	Realizar cualquier actividad que comprometa la disponibilidad o integridad de la red

15. SOFTWARE E INSTALACIONES

La instalación de software no autorizado puede introducir malware, vulnerabilidades o problemas de licencias con consecuencias legales y técnicas graves.

✓ HACER	✗ NO HACER
Solicitar por escrito autorización previa al instalar cualquier software.	Instalar software, aplicaciones o extensiones sin autorización escrita
Verificar que el software tiene licencia válida antes de instalarlo.	Usar versiones piratas o sin licencia de ningún programa
Mantener siempre actualizado el sistema operativo y las aplicaciones.	Deshabilitar el antivirus o las actualizaciones automáticas del sistema
Comprobar la compatibilidad del software con el sistema corporativo.	Realizar pruebas o desarrollos con datos personales reales sin autorización

16. USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL

El uso de sistemas de IA generativa (chatbots, asistentes, generadores de contenido, etc.) requiere especial cautela para proteger la confidencialidad de la información corporativa y personal.

✓ HACER	✗ NO HACER
Solicitar autorización previa a la Dirección o departamento responsable para usar herramientas de IA	Introducir datos personales de clientes, empleados o terceros en sistemas de IA
Usar IA exclusivamente para tareas laborales autorizadas	Compartir información confidencial, secretos empresariales o propiedad intelectual con herramientas de IA externas
Tratar los resultados generados por IA con sentido crítico y verificarlos	Publicar o distribuir contenido generado por IA sin revisión y autorización previa
	Usar herramientas de IA no autorizadas para tomar decisiones que afecten a personas

Recuerda:
Lo que introduces en una herramienta de IA externa puede ser procesado y almacenado por terceros. Nunca introduzcas información que no publicarías en un canal público.

17. CONTROL DE ACCESOS FÍSICO Y LÓGICO

17.1. Acceso físico a las instalaciones

- Las llaves, tarjetas de acceso y códigos son de uso personal e intransferible.
- Está prohibido hacer copias de llaves o ceder el acceso sin autorización expresa.
- Cerrar con llave despachos, armarios y salas con información sensible al ausentarse.
- El cuarto del servidor sólo es accesible para el personal autorizado por el Responsable de Seguridad.
- Comunicar de inmediato la pérdida de cualquier elemento de acceso.

17.2. Acceso lógico a sistemas

- Cada usuario accede únicamente a los sistemas y datos necesarios para su función (principio de mínimo privilegio).
- Está prohibido acceder a información que no corresponda a tus responsabilidades laborales.
- Las cuentas de usuario se revocan inmediatamente al finalizar la relación contractual.
- Los permisos se revisan periódicamente para eliminar accesos innecesarios.

18. GESTIÓN DE SOPORTES Y BORRADO SEGURO

18.1. Uso de soportes extraíbles

Los dispositivos extraíbles (USB, discos externos, tarjetas SD) son una vía habitual de fuga de información y de introducción de malware.

✓ HACER	✗ NO HACER
Solicitar autorización para sacar cualquier soporte con datos fuera de las instalaciones	Sacar soportes con datos personales o confidenciales sin autorización
Cifrar siempre el contenido de soportes extraíbles que contengan datos sensibles	Conectar dispositivos USB de origen desconocido a equipos corporativos
Registrar la asignación y devolución de soportes extraíbles	Tirar o desechar discos duros, memorias USB u otros soportes sin destrucción segura
Entregar al Responsable de Seguridad los soportes que deban desecharse	

18.2. Borrado seguro

El simple uso de la tecla 'Supr' o arrastrar a la papelera NO elimina la información de forma segura. Sólo elimina la referencia al archivo, pero el contenido permanece en el disco.

- Vaciar la papelera de reciclaje al final de cada jornada laboral.

- Para archivos con datos sensibles, usar herramientas de borrado seguro autorizadas por el departamento de IT.
- Los equipos dados de baja deben ser entregados al Responsable de Seguridad para su destrucción certificada.
- Los documentos en papel con datos personales deben destruirse con destructora, nunca tirarse enteros.

19. GESTIÓN DE INCIDENTES DE SEGURIDAD

Un incidente de seguridad es cualquier evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información.

Ejemplos de incidentes que DEBEN notificarse al Responsable de Seguridad:

- Pérdida o robo de dispositivos o documentos con información
- Acceso no autorizado a sistemas o datos
- Correo de phishing recibido o enlace malicioso accedido
- Virus o malware detectado en el equipo
- Envío accidental de datos personales a un destinatario incorrecto.

Contraseña expuesta o comprometida

19.1. Protocolo de actuación

1. No actuar de forma precipitada: no apagar el equipo ni borrar evidencias.
2. Notificar de inmediato al Responsable de Seguridad detallando qué ocurrió, cuándo y qué datos o sistemas pueden estar afectados.
3. Colaborar con la investigación facilitando toda la información disponible.
4. El Responsable de Seguridad evaluará junto con el /la Abogado/a de Protección de Datos, el alcance y, si procede, notificará a la Agencia Española de Protección de Datos (AEPD) y/o a los interesados afectados
5. Se documentará el incidente y se implementarán medidas correctivas para evitar su repetición.

20. COPIAS DE SEGURIDAD

Las copias de seguridad son la garantía de que la organización puede recuperar su información ante un incidente. Son responsabilidad de todos facilitar su correcto funcionamiento.

- El departamento de IT establece la política y frecuencia de las copias de seguridad.
- Todo el personal debe guardar la información en las ubicaciones y sistemas corporativos designados, no en el escritorio local del equipo.
- No está permitido almacenar información corporativa exclusivamente en dispositivos personales o servicios de nube no autorizados.
- Ante cualquier duda sobre si un dato está siendo respaldado, consultar con el departamento de IT.

Versión	Fecha	Descripción
V.1.0	2026	Versión inicial