DOSIER DE FORMACIÓN

GDPR - LOPDGDD

Reglamento Europeo de Protección de Datos

Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales

DIRIGIDO AL PERSONAL DE LA ORGANIZACIÓN

DOSIER DE FORMACIÓN GDPR - LOPDGDD

TEMARIO

1. CONCEPTOS BÁSICOS DE PROTECCIÓN DE DATOS

1.1. Normativas de privacidad

1.2. Ámbito de aplicación

1.3. Definiciones

1.4. Principios relativos al tratamiento

1.5. Legitimación del tratamiento

2. ACTIVIDADES DE TRATAMIENTO

2.1. Ficheros

- Responsabilidades
- Categoría de datos
- Situaciones específicas de tratamiento
- Ejemplos de actividades de tratamiento

2.2. Intervinientes en el tratamiento

- Personal responsable
- Personal autorizado
- Empresas externas

3. POLÍTICA DE INFORMACIÓN

3.1. Información que debe facilitarse al interesado

3.2. Comunicación de la información al interesado

4. POLÍTICA DE SEGURIDAD

4.1. Acuerdo de confidencialidad y secreto profesional

4.2. Política de seguridad del personal

4.3. Medidas adicionales de seguridad

4.4. Violaciones de la seguridad

- Gestión de una violación de seguridad
- Casuística de violaciones de seguridad

5. DERECHOS

5.1. Derechos del interesado

5.2. Derechos digitales en el entorno laboral

1. CONCEPTOS BÁSICOS DE PROTECCIÓN DE DATOS

1.1 NORMATIVAS DE PRIVACIDAD

GDPR *(europea)*	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
LOPDGDD *(española)*	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

1.2 ÁMBITO DE APLICACIÓN

Material	**Se aplica a:** • Tratamiento de datos personales contenidos o destinados a ser incluidos en un Fichero **No se aplica a:** • Tratamiento no sujeto al Derecho de la UE • Tratamiento efectuado por una persona física en el ámbito personal o doméstico • Tratamiento de datos de una persona jurídica (no son datos personales)

Territorial	**Se aplica a:**
	• Establecimiento ubicado en la UE, independientemente de que el tratamiento tenga lugar en la UE o no
	• Establecimiento no ubicado en la UE, pero que trate datos de INTERESADOS residentes en la UE, cuando las actividades de tratamiento estén relacionadas con:
	  ○ la oferta de bienes o servicios en la UE
	  ○ el control de su comportamiento, en la medida en que este tenga lugar en la UE

1.3 DEFINICIONES

Datos personales	Información relativa a una persona física por la cual pueda determinarse su identidad
Interesado	Persona física sometida al tratamiento de sus datos personales
Tratamiento	Cualquier operación realizada sobre datos personales: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción
Fichero	Conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado
Responsable del tratamiento (RT)	Persona física o jurídica que determina los fines y los medios del tratamiento
Encargado del tratamiento (ET)	Persona física o jurídica que trata datos personales por cuenta del RT
Destinatario de datos	Persona física o jurídica a la que se comunican datos personales
Personal autorizado	Persona autorizada por el RT o ET para realizar un tratamiento de datos
Delegado de protección de datos (DPO)	Persona o entidad encargada de informar y asesorar al RT, ET y al Personal autorizado de las obligaciones del GDPR y la LOPDGDD
Autoridad de control (AC)	Autoridad pública independiente encargada de supervisar la aplicación de las normativas de privacidad: AEPD (española), APDCAT (catalana), AVPD (vasca)

1.4 PRINCIPIOS RELATIVOS AL TRATAMIENTO

Licitud	Lealtad y transparencia con el INTERESADO
Limitación de los fines	Recogidos con fines determinados, explícitos y legítimos y no tratados posteriormente de manera incompatible con dichos fines
Minimización de los datos	Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados
Exactitud	Actualizados sin demora con respecto a los fines para los que se tratan
Limitación del plazo de conservación	Mantenidos de forma que se permita la identificación de los INTERESADOS durante no más tiempo del necesario para los fines por los que se tratan. Excepto si el tratamiento se realiza exclusivamente para fines de archivo en interés público o para investigación histórica, estadística o científica
Integridad y confidencialidad	Implementando medidas técnicas y organizativas adecuadas para proteger los datos contra tratamientos no autorizados o ilícitos y su pérdida, destrucción o daño accidentales
Responsabilidad proactiva	Siendo responsable y capaz de demostrar el cumplimiento de todos los principios del tratamiento

1.5 LEGITIMACIÓN DEL TRATAMIENTO

Licitud	• Consentimiento explícito (firmado) o inequívoco (confirmado por medios electrónicos).
	• Contrato o precontrato con el INTERESADO.
	• Cuando el tratamiento esté fundamentado en la legislación vigente por:
	  ○ Obligación jurídica a la que esté sujeto el RT
	  ○ Interés legítimo del RT o de terceros, siempre que no prevalezcan los intereses o los derechos y libertades del INTERESADO, especialmente si es un menor
	  ○ Procedencia legítima de archivos de acceso público obtenidos de una fuente pública.
	  ○ Cometido de interés PÚBLICO.
	• Cuando sea necesario para la protección de los intereses vitales del INTERESADO u otra persona física

Cuando se precisa el consentimiento explícito	Cuando el tratamiento no pueda legitimarse de otra forma, por ejemplo: • Envío de comunicaciones comerciales sobre productos o servicios (publicidad), excepto si ya es cliente • Obtención y/o publicación de imágenes • Tratamiento de categorías especiales de datos • Tratamiento de datos de menores • Elaboración automatizada de PERFILES
Condiciones para que un consentimiento sea considerado válido	• Facilitar la información del tratamiento al INTERESADO. • Informar al INTERESADO que tiene derecho a retirar el consentimiento en cualquier momento sin que afecte al tratamiento efectuado hasta entonces • Debe ser tan fácil retirar el consentimiento como haberlo dado • El RT asumirá la prueba del consentimiento. Si se realiza por escrito, deberá distinguirse claramente de otros asuntos • El consentimiento no será lícito si se condiciona a una prestación de servicios sin ser necesario para su realización • El consentimiento basado en un contrato debe guardar una relación entre las finalidades y la relación contractual • El consentimiento para varias finalidades precisará que conste de manera específica e inequívoca que se otorga para cada una de ellas • Los consentimientos que infrinjan parcialmente el GDPR serán nulos
Tratamiento de datos de menores	• La edad de los menores para el tratamiento de datos se establece en 14 años • El consentimiento debe darlo su representante legal • La información del tratamiento dirigida a un menor deberá facilitarse con un lenguaje claro, sencillo y adecuado al menor

2. ACTIVIDADES DE TRATAMIENTO

2.1 FICHEROS

RESPONSABILIDADES

Responsable (RT)	• Entidad que determina los fines y los medios del tratamiento por su cuenta
Encargado (ET)	• Entidad que realiza un tratamiento por cuenta (por encargo) de otra entidad RT
Corresponsable (CoRT)	• Entidad que determina los fines y los medios del tratamiento conjuntamente con otro RT

CATEGORÍAS DE DATOS

Básicos	• Cualquier información relativa a una persona que no sean datos ESPECIALES o PENALES.
Especiales	• Origen étnico o racial. • Opiniones políticas. • Convicciones religiosas o filosóficas. • Afiliación sindical. • Datos genéticos o biométricos que permitan la identificación unívoca de una persona. • Datos relativos a la salud. • Datos relativos a la vida y orientación sexuales
Penales	• Datos relativos a condenas y delitos PENALES o medidas de seguridad afines

SITUACIONES ESPECÍFICAS DE TRATAMIENTO

Transferencias internacionales	• TRANSFERENCIAS internacionales de datos a entidades no establecidas en la UE
Alto riesgo	• Tratamiento susceptible de comportar un alto riesgo para la protección de los derechos y libertades de los INTERESADOS
Perfiles	• Elaboración automatizada de PERFILES con toma de decisiones automatizada individuales
Público	• Titularidad o interés PÚBLICO
Grupo empresarial	• Tratamiento realizado por un grupo de empresas

EJEMPLOS DE ACTIVIDADES DE TRATAMIENTO

ACTIVIDADES VINCULADAS AL PERSONAL (RR HH)

Laboral y RR HH	• Gestión laboral del personal	*RT*	*Básico*	*Contrato*
Control horario	• Registro de presencia obtenido mediante huella digital	*RT*	*Especial*	*Interés legítimo*
Currículums	• Gestión de candidatos a empleados	*RT*	*Básico*	*Interés legítimo*
Videovigilancia laboral	• Grabación audiovisual de empleados por seguridad	*RT*	*Básico*	*Interés legítimo*
Geolocalización laboral	• Gestión de datos de geolocalización de empleados	*RT*	*Básico*	*Interés legítimo*

ACTIVIDADES VINCULADAS A LA ACTIVIDAD ECONÓMICA

Clientes y proveedores	• Gestión comercial y administrativa	*RT*	*Básico*	*Interés legítimo*
Fiscal y contable	• Registro de las obligaciones fiscales y contables	*RT*	*Básico*	*Obligación jurídica*
Contactos	• Comunicación, información y gestión de productos y servicios	*RT*	*Básico*	*Consentimiento explícito*
Videovigilancia	• Grabación audiovisual de personas por seguridad	*RT*	*Básico Público*	*Interés público*
Audiovisuales	• Gestión publicitaria audiovisual	*RT*	*Básico*	*Consentimiento explícito*
Historial clínico	• Gestión y administración de datos de salud	*RT*	*Especial*	*Consentimiento explícito*

ACTIVIDADES REALIZADAS POR ENCARGO DE OTRA ENTIDAD

Servicios de asesoría	• Gestión laboral, fiscal y contable	*ET*	*Básico*	*Contrato*
Servicios de PRL	• Gestión de la prevención de riesgos laborales	*ET*	*Básico*	*Contrato*
Servicios informáticos	• Mantenimiento de equipos y aplicaciones informáticas	*ET*	*Básico*	*Contrato*
Servicios de internet	• Gestión de Hosting, Backup, Mailing, etc.	*ET*	*Básico*	*Contrato*
Servicios de seguridad	• Control de acceso, seguridad y vigilancia a instalaciones	*ET*	*Básico*	*Contrato*
Servicios de privacidad	• Consultoría de privacidad	*ET*	*Básico*	*Contrato*

2.2 INTERVINIENTES EN EL TRATAMIENTO

PERSONAL RESPONSABLE

Protección de datos	• Seguridad:
	  ○ Responsable de seguridad interno
	  ○ DPO interno, si existe
	• Registros:
	  ○ Encargado de atender los Derechos del INTERESADO
	  ○ Encargado de gestionar las Violaciones de seguridad

Sistema informático	• Sistemas:
	  ○ Responsable del Sistema informático
	  ○ Encargado de las copias de seguridad/respaldo

PERSONAL AUTORIZADO

Tipos de personal	• Directivos • Empleados • Estudiantes en prácticas • Autónomos • Trabajador familiar • Trabajador externo • Socios • Voluntarios • Personal sin acceso a datos	*Dirección* *Administración* *Recursos humanos* *Comercial* *Técnico* *Mantenimiento* *Sistemas* *Redes sociales* *Limpieza*

EMPRESAS EXTERNAS

Tipos de empresa	• Encargados de tratamiento (ET) • DESTINATARIOS de datos • Corresponsables del tratamiento (CoRT) • Delegado de protección de datos (DPO) • TRANSFERENCIAS internacionales de datos • Empresas sin permiso de acceso a datos

3. POLÍTICA DE INFORMACIÓN

3.1 INFORMACIÓN QUE DEBE FACILITARSE AL INTERESADO

Transparencia de la información	• Forma de facilitar la información:
	  ○ Concisa, transparente, inteligible y de fácil acceso
	  ○ Lenguaje claro y sencillo, especialmente si va dirigida a menores
	• Medios para facilitar la información:
	  ○ Por escrito
	  ○ Medios electrónicos
	  ○ Oralmente, si lo solicita el INTERESADO
	  ○ En combinación con iconos formalizados (visibles, inteligibles y claramente legibles)

Información básica del tratamiento	• Identidad y datos de contacto del RT y del DPO (si existe)
	• Legitimación (base jurídica en que se basa el tratamiento)
	• Fines del tratamiento
	• Plazo de conservación o criterios que lo determinen
	• DESTINATARIOS de los datos (si se prevé o no comunicar o transmitir datos a terceros)
	• Derechos que asisten al INTERESADO:
	  ○ Revocar el consentimiento (solo en el caso que se base en ello)
	  ○ Acceso, rectificación, supresión y portabilidad de datos
	  ○ Limitación u oposición al tratamiento
	  ○ Presentar una reclamación ante la Autoridad de control

Información específica del tratamiento	• Cuando exista una TRANSFERENCIA internacional de datos:
	  ○ Información sobre la existencia o ausencia de garantías adecuadas
	• Cuando exista un mecanismo AUTOMATIZADO de elaboración de PERFILES:
	  ○ Información sobre la lógica aplicada y las consecuencias previstas
	• Cuando exista un propósito de tratar los datos para otros fines:
	  ○ Información sobre estos fines
	• Cuando exista un requisito legal o contractual para obtener los datos:
	  ○ Las consecuencias para el INTERESADO de no facilitarlos
	• Cuando los datos no se hayan obtenido directamente del INTERESADO:
	  ○ La fuente de procedencia de los datos
	  ○ Las categorías de datos tratados

3.2 COMUNICACIÓN DE LA INFORMACIÓN AL INTERESADO

Cuando los datos se obtienen del interesado	• Obligatorio:
	  ○ En el momento de la obtención de los datos
	• No obligatorio:
	  ○ Cuando el INTERESADO ya disponga de la información

Cuando los datos no se obtienen del interesado	• Obligatorio (lo primero que se produzca):
	  ○ En un plazo máximo de 1 mes
	  ○ En el momento de la primera comunicación con el INTERESADO
	  ○ En el momento que se revelen los datos a un DESTINATARIO
	• No obligatorio:
	  ○ Cuando el INTERESADO ya disponga de la información
	  ○ Cuando la comunicación sea imposible o suponga un esfuerzo desproporcionado
	  ○ Cuando el tratamiento esté fundamentado en la legislación vigente

4. POLÍTICA DE SEGURIDAD

4.1 ACUERDO DE CONFIDENCIALIDAD Y SECRETO PROFESIONAL

Es un contrato que debe firmar el personal, con las instrucciones para tratar datos personales.

INSTRUCCIONES PARA EL TRATAMIENTO DE DATOS

Información confidencial	**Datos personales** • Información relativa a una persona física identificada o identificable por la cual pueda determinarse, directa o indirectamente su identidad, sea mediante identificador, nombre, número, localización o elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
	Secretos comerciales • Conocimientos técnicos e información empresarial no divulgados contra su obtención, utilización y revelación ilícitas. • Informaciones técnicas, programas de formación, test, investigación y desarrollo, ideas, invenciones, conceptos, anotaciones, esquemas, diseños, dibujos, organigramas, memorándums, procesos, procedimientos, "know-how", fórmulas, datos, programas y aplicaciones informáticas, mejoras y descubrimientos, conocimientos de cualquier clase puestos a disposición del personal. • Materiales de referencia, materiales y técnicas de marketing, planes de investigación y desarrollo, marketing, nuevos productos. • Nombres de clientes, canales de comercialización, secretos comerciales y cualquier otra información relacionada con clientes y proveedores, listas de precios, políticas de precios, política de ventas, información financiera, presupuestos, plantillas y métodos de gestión y contabilidad. • Títulos e intereses que pudiera alegar sobre las invenciones, patentables o no, realizadas u obtenidas por el personal durante la vigencia de su contrato.
Compromiso de confidencialidad y secreto profesional	• El personal se compromete a cumplir las instrucciones determinadas por la organización para garantizar la confidencialidad y el secreto profesional de toda la "información confidencial". • El personal se obliga explícitamente a no divulgarla, publicarla, cederla, venderla, ni de otra forma, directa o indirecta, ponerla a disposición de terceros, ni total ni parcialmente, y a cumplir esta obligación incluso con sus propios familiares u otros miembros de la organización que no estén autorizados a acceder a dicha información, cualquiera que sea el soporte que la contenga. • El personal sólo accederá a la "información confidencial" si es necesario para la prestación de los servicios para los que ha sido contratado. • Los medios de trabajo proporcionados (ordenadores, internet, correo electrónico, etc.) serán utilizados única y exclusivamente para el desarrollo eficiente del propio trabajo, pudiéndose realizar tareas de verificación, vigilancia y control sobre los mismos sin informar expresamente al personal.

Propiedad de la "información confidencial"	• El personal reconoce que la propiedad de la "información confidencial" pertenece a la organización y se compromete a devolver todas las copias de dicha información y cualquier soporte físico que estén bajo su control cuando la organización se lo solicite.
Tratamiento de datos	• El personal declara conocer las políticas de información y de seguridad establecidas por la organización para garantizar la protección de datos y se compromete a seguir las instrucciones en ellas reflejadas y, en caso apercibir que sean violadas, a notificarlo sin demora injustificada.
Responsabilidad del personal	• El personal será responsable de cualquier perjuicio que pudiera derivarse del incumplimiento de los compromisos adquiridos, pudiendo suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que se vea obligado a atender como consecuencia de dicho incumplimiento.
Información sobre el tratamiento de los datos del personal	• Fines: gestionar la relación laboral o profesional que les une. • Legitimación: para la ejecución de un contrato entre las partes. • Criterios de conservación: se conservarán indefinidamente para fines de archivo mientras ninguna de las partes se oponga a ello. • Comunicación de datos: no serán comunicados a terceros, salvo por obligación legal. • Derechos: el personal puede ejercer los derechos de acceso, rectificación, portabilidad y supresión de sus datos y los de limitación y oposición a su tratamiento. • Reclamaciones: el personal puede reclamar ante la autoridad de control o el DPO si considera que el tratamiento no se ajusta a la normativa.
Fin de la prestación de servicio	• El cumplimiento de las obligaciones de este acuerdo es de carácter indefinido y se mantendrá en vigor con posterioridad a la finalización de la relación laboral. • El personal se compromete a guardar el mismo secreto profesional respecto de la "información confidencial" a la que haya tenido acceso durante el desempeño de sus funciones.

4.2 POLÍTICA DE SEGURIDAD DEL PERSONAL

La organización ha implementado medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado a los riesgos que pueda tener el tratamiento como consecuencia de:

- la destrucción accidental o ilícita de datos
- la pérdida, alteración o comunicación no autorizada
- el acceso a los datos cuando son transmitidos, conservados u objeto de algún otro tipo de tratamiento

El personal deberá velar por la seguridad de los datos tratados por la organización y comunicará al responsable de la empresa cualquier operación de tratamiento que pueda suponer un riesgo que afecte la protección de datos o los intereses y libertades de los INTERESADOS.

Cualquier diseño de una nueva operación de tratamiento o actualización de una operación existente deberá garantizar antes de su implantación, la protección de datos personales y el ejercicio de los derechos de los INTERESADOS en todas las fases del tratamiento: obtención, acceso, intervención, transmisión, conservación y supresión.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

El personal deberá actuar conforme las instrucciones detalladas en el acuerdo de confidencialidad suscrito con la organización y las establecidas en esta Política de seguridad. Para ello se establecen las siguientes medidas de protección de datos que el personal se obliga a cumplir expresamente:

Organización de la información	• Clasificar los datos de manera que se puedan ejercer los derechos del INTERESADO
Conservación de los datos	• Guardar los datos en las ubicaciones destinadas a tal fin (mobiliario, soportes, carpetas o directorio de red, cloud, etc.)
Acceso a la información	• Cada persona sólo está autorizada a acceder a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones • Aplicar los mecanismos de acceso restringido que se hayan implementado • Salvaguardar las claves de acceso de toda divulgación a terceros • Restringir el acceso a los recursos mediante procedimientos que puedan identificar la persona que accede a los mismos
Procesamiento de datos	• Los soportes no deben estar accesibles a personas no autorizadas • Cuando se utilicen impresoras o fotocopiadoras, asegurarse de no dejar documentos impresos en la bandeja de salida • Si una persona se ausenta de su puesto de trabajo temporalmente, deberá ocultar los documentos y bloquear el ordenador para impida la visualización de la información con la que está trabajando
Transporte de soportes	• Realizar únicamente por personal autorizado o empresas externas contratadas para tal fin
Eliminación de documentos	• Destruir con la destructora de documentos o retirados por una empresa homologada
Copia de seguridad y recuperación de datos	• Almacenar toda la información en el directorio de red correspondiente para permitir que se realicen las copias de seguridad

Protección de datos	• Aplicar las medidas de protección de datos establecidas por la organización (seudonimización, cifrado de datos, advertencias de intrusión como antivirus, antispam, etc.)
Gestión de incidencias	Cualquier violación de la seguridad que ocasione la destrucción accidental o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de datos personales • Notificar, sin demora injustificada, cualquier incidencia que tenga conocimiento para la aplicación de medidas que remedien y mitiguen los efectos que hubiera podido ocasionar. • Documentar la incidencia con una descripción detallada y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella. • El conocimiento y no notificación de una incidencia se considera una falta contra la seguridad de los datos y puede suponer el inicio de acciones legales, así como la reclamación de indemnizaciones, sanciones y daños o perjuicios

4.3 MEDIDAS ADICIONALES DE SEGURIDAD

Son medidas de seguridad específicas que la organización puede imponer al personal para prohibir expresamente actividades concretas que conlleven una amenaza para proteger la información confidencial relativa a los datos personales y el secreto comercial.

LA ORGANIZACIÓN PUEDE PROHIBIR LAS SIGUIENTES ACTIVIDADES

Confidencialidad de la información	• Enviar al exterior o revelar a terceros, información que no haya sido declarada como no confidencial • Usar cámaras fotográficas, de vídeo, de sonido o cualquier instrumento que pueda almacenar información audiovisual • Poseer, para usos fuera de su responsabilidad, material o información no relacionados directamente con el puesto de trabajo
Utilización de los sistemas informáticos (SI)	• Descargar o usar programas informáticos ilegales o sin la correspondiente licencia • Descargar, usar, reproducir, ceder, transformar o publicar cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial • Introducir voluntariamente programas, virus, macros, applets, o cualquier otro dispositivo que sea susceptibles de causar alteraciones en los Sistemas Informáticos • Destruir, borrar, alterar, inutilizar o dañar datos, programas o documentos electrónicos • Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la organización • Cifrar información sin estar expresamente autorizado para ello
Salvaguarda y protección de las contraseñas	• Compartir o facilitar el identificador de usuario y la contraseña a otra persona física o jurídica. • Intentar distorsionar o falsear los registros log del sistema • Intentar aumentar o disminuir los privilegios de un usuario en el sistema
Acceso a redes	• Utilizar los datos, la red corporativa o la intranet para incurrir en actividades que puedan ser consideradas ilícitas o ilegales o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas • Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos • Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos • Almacenar datos personales en el disco duro del ordenador, debiendo ser utilizadas las carpetas de la red corporativa asignadas para tal fin

Recursos telemáticos y acceso a Internet	• Utilizar los recursos telemáticos y/o acceder a redes públicas como Internet, páginas web, news, redes sociales y otras fuentes de información para temas no relacionados directamente con la actividad de la organización o los cometidos del puesto de trabajo del personal. • El acceso a debates en tiempo real (Chat/IRC), ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema
Utilización del correo electrónico y mensajería	• Considerar como privados los mensajes de correo electrónico recibidos • Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios • Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario • Enviar o reenviar mensajes en cadena o de tipo piramidal

4.4 VIOLACIONES DE LA SEGURIDAD

Una violación de seguridad es cualquier incidencia que ocasione 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.

GESTIÓN DE UNA VIOLACIÓN

Notificación al personal responsable	• Notificar inmediatamente cualquier incidencia que tenga conocimiento, al personal responsable
Documentación a entregarle	• Documentar la incidencia con una descripción detallada y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella

CASUÍSTICA DE VIOLACIONES

Acceso a datos no autorizado	• Encargo del tratamiento sin contrato de protección de datos • Acceso indiscriminado a impresoras, fotocopiadoras, etc. • Acceso no autorizado a información confidencial • Acceso no autorizado a los sistemas informáticos
Comunicación de datos no autorizada	• Transmisión ilícita de datos a un DESTINATARIO • Vulneración del secreto profesional • Publicación de imágenes sin autorización del INTERESADO • Envío masivo de email sin ocultar los destinatarios (copia oculta) • TRANSFERENCIA internacional de datos sin garantías de protección de datos
Alteración de datos	• Modificación de datos malintencionado • Falsificación de datos • Recuperación ineficaz de copias de respaldo
Pérdida de información	• Extravío u olvido de soportes • Robo o sustracción de información • Desinstalación de aplicaciones informáticas • Por causas del transporte • Reorganización de la empresa • Destrucción de datos • No usar destructora de papel o de soportes digitales • Incendio, inundación u otras causas ajenas a la empresa
Ausencia de medidas de seguridad	• Antivirus, antispam, antimalware, antiransomware, fireware, etc. • Cifrado, seudonimización, etc. • Identificación y autentificación para acceder a los sistemas informáticos • Mecanismos de seguridad para acceder al mobiliario o departamentos • Disposición de datos a la vista de personas no autorizadas (recepción, monitores, mesas, etc.).

5. DERECHOS

5.1 DERECHOS DEL INTERESADO (GDPR)

Acceso	• Derecho a que se le comuniquen los datos que posee la organización y a ser informado del tratamiento efectuado con ellos
Rectificación	• Derecho a que se le rectifiquen los datos cuando resulten inexactos o incompletos
Supresión	• Derecho a que se supriman sus datos cuando ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados
Portabilidad	• Derecho a que se transmitan sus datos a la organización que éste designe o directamente a él mismo
Limitación del tratamiento	• Derecho a que se marquen sus datos con el fin de limitar el tratamiento
Oposición al tratamiento	• Derecho a oponerse al tratamiento de sus datos por motivos relacionados con su situación particular

5.2 DERECHOS DIGITALES EN EL ENTORNO LABORAL (LOPDGDD)

Intimidad y uso de dispositivos digitales	• Derecho a la protección de su intimidad en el uso de los dispositivos puestos a su disposición • La organización puede acceder al contenido de los dispositivos • En el caso que se autorice el uso de dispositivos para fines privados requerirá que la organización especifique los usos autorizados
Desconexión digital	• Derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal, el respeto de su tiempo de descanso, permisos y vacaciones, y su intimidad personal y familiar
Videovigilancia y grabación de sonidos	• La organización puede grabar imágenes obtenidas para funciones de control del personal • No puede grabar imágenes obtenidas en lugares destinados al descanso o esparcimiento del personal, tales como vestuarios, aseos, comedores y análogos
Geolocalización	• La organización puede tratar datos de geolocalización obtenidos para funciones de control del personal
Negociación colectiva	• Los convenios colectivos pueden establecer garantías adicionales relacionados con los derechos digitales en el ámbito laboral