Índice de Contenidos

Fecha	Edición.Revisión	Cambios Realizados
30-06-2021	0.1	Borrador inicial del documento
26-11-2021	1.0	Versión aprobada en el CSI
17-08-2022	1.1	Adecuación con el nuevo ENS (RD 311/2022)
04-01-2023	1.2	Actualización referencia ENS (RD 311/2022)
18-07-2023	1.3	Cambio de alcance de Ayuntamientos a Entidades

1 Decálogo de normativa interna de uso de medios electrónicos

1. • El objeto del presente documento es la **definición de la normativa aplicable al uso de los medios electrónicos**, dentro del alcance señalado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)

2. • El presente documento es de **aplicación a todo empleado/a que**, de manera permanente o eventual, administre, opere **o interactúe con los servicios prestados por el Organismo**.

3. • **No está permitido conectar dispositivos que no estén autorizados** a la red del Organismo ni esta permitidos conectar dispositivos no autorizados a otros dispositivos autorizados.

4. • **No está permitido alterar la configuración física, configuración de seguridad ni el software** de los dispositivos provistos y propiedad de la Entidad.

5. • Está **prohibido utilizar, copiar o transmitir información contenida en los sistemas informáticos para uso privado** o cualquier otro distinto del servicio al que está destinada.

6. • **Las contraseñas, token de autenticación, o tarjeta de acceso al sistema y/o a la red, son personales e intransferibles**, siendo el usuario/a el único responsable de las consecuencias que pudieran derivarse de su mal uso.

7. • **La utilización de internet** por parte de los usuarios/as autorizados **debe limitarse** a la obtención de información y el acceso a los servicios relacionados **con el trabajo que se desempeña.**

8. • **Comunicar con la mayor diligencia posible al Responsable de Seguridad y al Delegado de Protección de Datos, las incidencias de seguridad** de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales.

2 Objeto

El objeto del presente documento es establecer la normativa de uso seguro de los medios electrónicos en la Entidad y dentro del alcance del Esquema Nacional de Seguridad.

El presente documento establece las normas de uso de los dispositivos asignados al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como al acceso y tratamiento de datos de carácter personal, en soporte electrónico y en papel.

Es fundamental que todos los empleados/as de la Entidad que utilizan equipamiento informático y accedan o traten información de carácter personal para la realización de sus funciones y tareas sean conocedores de esta norma.

A través de la presente normativa, se han implantado las siguientes medidas atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la Entidad, que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS):

- Marco Organizativo- Normativa de Seguridad [org.2];
- Medidas de Protección- Gestión del personal- Deberes y Obligaciones [mp.per.2];
- Medidas de Protección- Protección de los Servicios- Protección del correo electrónico [mp.s.1]

Los requisitos que se recogen en la guía CCN-STIC 808 Verificación y cumplimiento del ENS son:

Org.2:

Categoría	Requisito	Evidencia
Básica	Se debe disponer de uno o varios documentos que constituyan la normativa de seguridad escrita.	La normativa de seguridad debe estar impresa y/o guardada en formato electrónico.
	Dicha normativa debe precisar el uso correcto de equipos, servicios e instalaciones.	Deben existir normativas respecto a la protección de equipos desatendidos, uso del correo electrónico con fines personales, medidas contra el acceso físico no autorizado a las instalaciones, etc. Estas normativas deben indicar cómo localizar los procedimientos relacionados.
	Dicha normativa debe precisar lo que se considera un uso indebido.	Existirán normativas que indican lo que se considera un uso indebido de los equipos, los servicios, las instalaciones, la información, etc.
	Dicha normativa debe precisar la responsabilidad del personal con respecto al cumplimiento o violación de estas normas (derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente).	Debe existir normativas que indican los derechos, deberes y medidas disciplinarias (referencia a la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público o adaptaciones particulares).

Mp.per.2:

Categoría	Requisito	Evidencia
Básica	Se informará a cada persona que trabaja en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.	Se debe disponer de un procedimiento documentado que especifica la forma de informar a cada persona que trabaja en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, así como la forma de recabar su aceptación explícita y firmada. Se dispondrá de un documento para cada perfil con sus deberes y responsabilidades.
	Respecto a dicha información de deberes y responsabilidades, se especificarán las medidas disciplinarias a que haya lugar.	Dicho documento informará de las medidas disciplinarias a que haya lugar.
	Se debe especificar que cubre tanto el periodo durante el cual se desempeña el puesto como las obligaciones en caso de término de la asignación o traslado a otro puesto de trabajo.	Dicho documento debe informar que las obligaciones se mantienen tanto en el periodo durante el cual se desempeña el puesto como posteriormente, en caso de término de la asignación o traslado a otro puesto de trabajo.
	Se debe especificar que el deber de confidencialidad respecto de los datos a los que tenga acceso cubre el periodo durante el cual se desempeña el puesto como en caso de término de la asignación o traslado a otro puesto de trabajo.	Dicho documento informará que las obligaciones de confidencialidad se mantienen tanto en el periodo durante el cual se desempeña el puesto como posteriormente, en caso de término de la asignación o traslado a otro puesto de trabajo.
	Se deben establecer, en el caso de personal contratado a través de un tercero, los deberes y obligaciones del personal.	Se dispondrá de una normativa documentada que especifica los deberes y obligaciones del personal contratado a través de un tercero. Existirá evidencia documental de la exigencia de esta normativa.
	Respecto del personal contratado a través de un tercero, se deben establecer los deberes y obligaciones de cada parte.	Se dispondrá de una normativa documentada que enumera los deberes y obligaciones de cada parte. Existirá evidencia documental de la exigencia de esta normativa.
	Respecto del personal contratado a través de un tercero, se debe establecer el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.	Se dispondrá de un procedimiento documentado que define la resolución de incidentes relacionados con el incumplimiento de las obligaciones por parte del personal del tercero.

Mp.s.1:

Categoría	Requisito	Evidencia
Básica	La información que se distribuye por medio de correo electrónico se protege, tanto en el cuerpo de los mensajes como en los anexos.	Se debe disponer de un procedimiento documentado para la protección, acorde a su nivel de clasificación, de la información que se distribuye por medio de correo electrónico y se protege tanto en el cuerpo de los mensajes como en los anexos.
	Se protege la información de encaminamiento de mensajes y establecimiento de conexiones.	Se debe disponer de una política o normativa documentada que especifica la protección del encaminamiento de mensajes y establecimiento de conexiones.
	Se debe proteger a la organización frente a problemas que se materializan por medio del correo electrónico, como del correo no solicitado (spam).	Se debe disponer de una política o normativa documentada que especifica que la organización debe ser protegida frente al spam. Se debe disponer de un sistema anti-spam debidamente configurado y mantenido.
	Respecto a la protección frente a problemas por el e-mail, se debe proteger frente a programas dañinos (virus, gusanos, troyanos, espías u otros de naturaleza análoga) relacionado con op.exp.6 Protección frente a código dañino.	Se debe disponer de una política o normativa documentada que especifica que la organización debe ser protegida frente a programas dañinos en el e-mail. Se debe disponer de un sistema anti-virus debidamente configurado y mantenido.
	Respecto a la protección frente a problemas por el e-mail, se debe proteger frente a código móvil de tipo “applet”.	Se debe disponer de una política o normativa documentada que especifica que la organización debe ser protegida frente a código móvil en el e-mail. Se debe disponer de un sistema anti-virus que contempla código móvil debidamente configurado y mantenido.
	Se deben establecer normas de uso del correo electrónico.	Se debe disponer de una normativa documentada que especifica el uso correcto y autorizado del correo electrónico.
	Respecto a dicha norma de uso del e-mail, se debe contemplar limitaciones al uso como soporte de comunicaciones privadas.	Dicha normativa debe especificar las limitaciones al uso como soporte de comunicaciones privadas.
	Se deben llevar a cabo actividades de concienciación y formación relativas al uso del correo electrónico.	Se debe disponer de plan de formación y concienciación que cubre el uso del correo electrónico (relacionado con [mp.per.3] concienciación y [mp.per.4] formación).

3 Alcance

Esta normativa es aplicable a todo el ámbito de actuación de la Entidad, especialmente a las TIC.

Además, aplicará y será de obligado cumplimiento para los organismos autónomos dependientes, entidades públicas empresariales dependientes y consorcios de la Entidad en relación con todos los sistemas de información que éste les preste.

Esta normativa es de obligado cumplimiento para todo el personal que acceda a los sistemas de información TIC, así como a la propia información gestionada por los diferentes organismos en cualquiera de sus formas y formatos. Aplica con independencia de cuál sea la relación o adscripción con el mismo.

4 Legislación y normativa aplicable

Las referencias tenidas en cuenta para la redacción de esta normativa han sido las indicadas en el documento marco: NOR-000: Legislación y Normativa Aplicable.

Además, se ha tenido en cuenta en especial la Guía "CCN-STIC-821 Normas de seguridad en el ENS" y el Anexo I de la Guía "CCN-STIC-822" – Procedimientos de seguridad en el ENS".

A su vez, la '**POL-ENS-000 Política de Seguridad**' se encuentra alojada en https://www.tenerife.es/documentos/TenerifeES/POL-ENS-000.pdf a disposición de todos los usuarios para su conocimiento.

5 Roles y responsabilidades

Rol	Responsabilidades
* Responsable de Seguridad	• Elaborar la normativa interna de uso de medios electrónicos.
* Comité de Seguridad de la Información	• Aprobar la normativa interna de uso de medios electrónicos.
* Cualquier persona con acceso a los sistemas	• Cumplir con la normativa interna de uso de medios electrónicos.

**Los roles concretos correspondientes serán los aplicables según lo establecido en la Entidad*

6 Normativa interna de uso de medios electrónicos

6.1 Obligaciones de la Entidad

La Entidad facilita a los usuarios/as el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo mientras éstos mantengan una relación laboral con el mismo. Este equipamiento pasará por un proceso de bastionado previo a su entrega.

Dentro de este tipo de equipamiento se encuentran tanto aquellos dispositivos propiedad de la Entidad como, excepcionalmente, aquellos otros que ésta haya autorizado para ser utilizados en su infraestructura informática y de comunicaciones.

En el primer caso, los dispositivos son propiedad de la Entidad y por tanto no están destinados a un uso personal. Como consecuencia de esto, la Entidad se reserva el derecho de revisar, sin previo aviso, los equipos y el uso de Internet y del teléfono corporativo que esté haciendo cada usuario/a, en caso de que existieren indicios de que se está llevando a cabo una utilización indebida. De esta forma el usuario/a queda informado de que el resultado de los controles efectuados puede ser utilizado para llevar a cabo, en su caso, las actuaciones disciplinarias previstas por la normativa vigente.

6.2 Uso de los dispositivos informáticos

Los usuarios/as deben cumplir las siguientes medidas de seguridad para el uso del equipamiento informático que se les haya proporcionado para las tareas relacionadas con su puesto de trabajo:

Conexión de otros dispositivos	• No está permitido conectar dispositivos que no estén autorizados a la red de la Entidad. • Tampoco se pueden conectar a los dispositivos autorizados, otros dispositivos que no estén autorizados expresamente.
Ubicación del dispositivo	• No está permitido variar la ubicación física de los dispositivos asignados a una ubicación.
Configuración del dispositivo	• No está permitido alterar la configuración física, configuración de seguridad ni el software de los dispositivos.
Uso de dispositivos y de la red	• Los dispositivos, así como la red de información que la Entidad pone a disposición de los usuarios/as están destinados a permitir el desempeño de las funciones y tareas profesionales que estos tienen encomendadas, estando prohibido el uso para otras finalidades de carácter personal, o bien para la realización de actos desleales o que pudieran ser considerados ilícitos.
Antivirus	• El usuario/a deberá comprobar que su antivirus se actualiza con regularidad. En caso contrario deberá notificarlo como una incidencia de seguridad.
Uso de la información	• Está prohibido utilizar, copiar o transmitir información contenida en los sistemas informáticos para uso privado o cualquier otro distinto del servicio al que está destinada. • El usuario/a se abstendrá de copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de esta Entidad en ordenador propio, pendrives o a cualquier otro soporte informático, salvo que solicite autorización al Responsable de la Seguridad y se adopten las medidas de seguridad correspondiente. Asimismo, los datos contenidos en este tipo de soportes deben ser suprimidos una vez hayan dejado de ser útiles y pertinentes para la satisfacción de los fines que motivaron su creación. Durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte informático externo, se deberá restringir el acceso y uso de la información que obra en los mismos. • El usuario/a deberá restringir a terceros (familiares, amistades o cualesquiera otros) el acceso a los archivos o ficheros titularidad de la Entidad y dispuesto a razón única de las funciones o tareas desempeñadas en la misma. Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando el usuario/a del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.

Identificación y autenticación	• Las contraseñas, token de autenticación, o tarjeta de acceso al equipo, sistema y/o a la red, concedidos por la Entidad son personales e intransferibles, siendo el usuario/a el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. Por cuestiones de seguridad no están permitidas prácticas como: • Emplear identificadores, contraseñas o cualquier token de autenticación de otros usuarios/as para acceder al sistema y a la red de la Entidad. • Intentar modificar o acceder al registro de accesos. • Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros.

6.3 Uso de la red corporativa

La red corporativa es un recurso compartido y limitado. Este recurso sirve no sólo para el acceso de los usuarios/as internos de la Entidad a la Intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas corporativas y la comunicación de datos entre sistemas de tiempo real y explotación.

Los usuarios/as deben cumplir las siguientes medidas para el uso de la red corporativa:

Uso de internet	• La utilización de Internet por parte de los usuarios/as autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña, debiendo por lo tanto evitarse la utilización que no tenga relación con las funciones del puesto de trabajo de usuario/a, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado. • La Entidad podrá controlar el uso de acceso a Internet proporcionado. Para ello seguirá un sistema basado en un control de las páginas visitadas, lo que podrá suponer el almacenamiento y control de las cookies que se generen. • La normativa completa sobre el uso de Internet puede consultarse en el Anexo II. Normas de uso de Internet del presente documento.
Uso del correo electrónico	• Se considera el correo electrónico como un instrumento básico de trabajo. • El acceso al correo se realizará mediante una identificación consistente en un usuario/a y una contraseña. Dicha identificación deberá seguir las mismas directrices que las planteadas para el acceso a las aplicaciones. • Los envíos masivos de información, así como lo correos que se destinen a gran número de usuarios/as serán solo los estrictamente necesarios que puedan provocar un colapso del sistema de correo. • No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia. • La Entidad se reserva el derecho de que el *Responsable de Seguridad* o el *Responsable del Sistema* pueda revisar y controlar el uso correcto del correo electrónico corporativo. • En caso de ausencia, baja temporal o definitiva, el *Responsable del Departamento* correspondiente podrá redireccionar a su dirección de correo los mensajes que lleguen a la cuenta de la persona de baja con la finalidad de continuar con el normal desarrollo de la actividad de la Entidad. • La normativa completa sobre el uso del correo electrónico puede consultarse en el epígrafe correspondiente en el Anexo I. Normas de uso del correo electrónico del presente documento.
Compartición de contenidos	• Se prohíbe el uso de programas de compartición de contenidos, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.

6.4 Acceso a aplicaciones y servicios

Tanto el equipamiento informático como todos los recursos facilitados al usuario/a para la realización de las tareas relacionadas con su puesto de trabajo (tales como teléfonos móviles, aplicaciones, servicios, etc.) son propiedad de la Entidad, o son propiedad del usuario/a, pero han sido autorizados para dichos usos, por lo que deberá hacerse un uso diligente de los mismos. En este sentido, podrá revisarse la utilización que cada usuario/a esté haciendo de los teléfonos móviles facilitados para el desempeño de su puesto de trabajo. En caso de que existieran indicios acerca del uso indebido de los mismos, podrá realizarse un control de la actividad que se considere sospechosa o fraudulenta, así como de la facturación, y de los destinatarios de las llamadas realizadas.

Gran parte de los procedimientos administrativos se gestionan en la actualidad accediendo desde ordenadores personales a aplicaciones que residen en servidores conectados a la red corporativa. Los usuarios/as deben cumplir las siguientes medidas de seguridad establecidas por la Entidad para el uso de aplicaciones y servicios corporativos:

Identificación y autenticación	• Tanto el acceso al ordenador como a las distintas aplicaciones corporativas será identificado (mediante usuario/a y contraseña, tarjeta de acceso, u otro mecanismo) y previamente autorizado por el responsable correspondiente.
Soportes informáticos (pendrives y discos duros externos USB, CDs, DVDs, disquetes, etc.)	• La salida de soportes que contengan datos de especial sensibilidad fuera de los locales de la Entidad debe ser expresamente autorizada por el Responsable del Tratamiento. Toda salida de soportes deberá además quedar registrada de acuerdo con el ***PRO-190 Procedimiento de transporte y entrada y salida de soportes*** en la Entidad. • La entrada de soportes que contengan datos personales deberá quedar registrada de acuerdo con el ***PRO-190 Procedimiento de transporte y entrada y salida de soportes*** en la Entidad. Asimismo, el soporte deberá ser dado de alta en el inventario de soportes de acuerdo con procedimiento establecido en la Entidad. • Debe evitarse el uso de unidades de almacenamiento de la información externas para uso privado como por ejemplo disquetes, pendrives, discos duros externos, CD-R, DVD-R, etc. • En caso de necesitar desechar un soporte que contenga datos personales, se destruirá mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. El Departamento de Informática cuenta con el equipamiento necesario para destruir la información de forma segura e irreversible. Asimismo, el soporte deberá ser dado de baja del correspondiente inventario.
Custodia de las contraseñas/tarjetas/token	• La custodia de la contraseña/tarjeta/token de acceso es responsabilidad del usuario/a. Nunca debe utilizarse la cuenta de usuario/a asignada a otra persona. • Las contraseñas no deben anotarse, deben recordarse.
Renovación de las contraseñas	• Las contraseñas deben cambiarse periódicamente. Los usuarios/as disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente. Esto garantiza el uso privado de las mismas.
Incidencias con las contraseñas	• Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al Responsable de Seguridad, siguiendo el proceso de comunicación de incidencias y peticiones que la Entidad tenga establecido. Esto resulta también de aplicación a la información en papel.

Ficheros en formato no digital. En relación con los ficheros en soporte o documento papel, el usuario/a deberá observar las siguientes diligencias con respecto a la confidencialidad de la información, acceso autorizado a la información en atención a las necesidades de su trabajo, gestión de soportes y documentos, trabajo fuera de las instalaciones de la Entidad.

Puesto de trabajo despejado	• Todos los puestos de trabajo deben permanecer despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
Almacenamiento de documentos	• Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo. • La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios y/o cajones bajo llave. • Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.
Destrucción	• Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados (máquinas destructoras), de forma que no sea recuperable la información que pudieran contener.
Incidencias	• Comunicar con la mayor diligencia posible al Responsable de Seguridad y al Delegado de Protección de Datos o la persona o departamento que se ocupe de la Protección de Datos personales de la Entidad (siguiendo el proceso de comunicación de incidencias y peticiones que la Entidad tenga establecida), las incidencias de seguridad de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales. • Entre otros, tienen la consideración de incidencia de seguridad, que afecta a los ficheros en papel, los sucesos siguientes: o Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal. o Uso indebido de las llaves de acceso. o Acceso no autorizado de usuarios/as a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal. o Pérdida de soportes o documentos en papel, con datos de carácter personal. o Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal.

6.5 Uso del teléfono

Teléfono fijo	• La Entidad pone a disposición de sus profesionales terminales de teléfono fijos a fin de facilitar desarrollo de la actividad profesional de los mismos, debiendo ser su uso estrictamente profesional. • El uso indebido de los teléfonos de la organización por parte de los empleados o empleadas dará lugar a la aplicación de las medidas disciplinaras oportunas.
Teléfono móvil corporativo	• En función de las características de la actividad profesional a desarrollar por algunos profesionales, ésta podrá poner a disposición de sus profesionales el uso de teléfono móvil de empresa o similar. • Dicho teléfono móvil es propiedad de la Entidad, y como herramienta necesaria de trabajo, su uso por parte del profesional deberá ser exclusivamente profesional. • El uso indebido de dichos teléfonos móviles para fines privados podrá dar lugar a la adopción por parte de la compañía de las medidas disciplinarias que considere oportunas.
Teléfono móvil personal	• En caso de necesidad por motivo de la actividad del profesional, éste requiera la conexión de su teléfono móvil privado a la red de datos corporativa deberá canalizar dicha petición a través del Departamento de Informática de la Entidad.

6.6 Tratamiento de datos de carácter personal

El presente documento establece las normas de uso del ordenador asignado al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, a nivel informático y en papel.

En este sentido, se considerará Datos de carácter personal, a cualquier información alfabética, numérica, gráfica, fotográfica, acústica o de cualquier otro tipo, relativa a un aspecto/s físico, psíquico, fisiológica, cultural, social o económico de la persona, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

En el Anexo IV se incluye una recopilación de las normas aplicables al tratamiento de datos de carácter personal que se indican a lo largo de la presente normativa.

En el Anexo V se incluye el Modelo a emplear para el derecho de información acerca del tratamiento de los datos personales.

6.7 Compromiso de confidencialidad

El personal de la Entidad debe guardar secreto profesional sobre toda información que conozca durante la prestación de sus servicios profesionales, comprometiéndose a no divulgarla, publicarla, revelarla ni de otra forma, directa o indirecta, ponerla a disposición de terceros, ni total ni parcialmente, cualquiera que sea el soporte en el que se encuentre la información. Esta obligación de secreto subsistirá aún después de terminadas sus actuaciones en la Entidad.

Además, en los casos en los que dicho personal tuviera acceso a datos de carácter personal, que resultaran estrictamente necesarios para el cumplimiento del presente contrato, se compromete y obliga:

- A tratar los datos, de conformidad con lo establecido Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, y a adoptar e implementar las medidas de seguridad, conforme a lo establecido en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo.
- A tratar los datos, conforme a las instrucciones de la Entidad, esto es, para la estricta prestación de los servicios encargados y a no aplicar o utilizar los datos personales con un fin distinto al convenido, y a no comunicarlos ni cederlos, ni siquiera para su conservación, a otras personas, físicas o jurídicas.
- A destruir, o devolver a la Entidad, según aplique, los datos de carácter personal, así como cualquier tipo de soporte informático o documento en el que constan los datos personales, una vez prestados los servicios contratados, sin conservar copia alguna de los mismos y sin que ninguna persona externa, física o jurídica, entre en conocimiento de los datos, a no ser que se tenga autorización expresa de la citada Entidad, todo ello de conformidad con lo establecido al efecto en Ley Orgánica 3/2018 de 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- En el caso de ser Delegado Sindical o miembro del Comité de Empresa, se le informa que el Estatuto de los Trabajadores (ET) establece un deber de sigilo, aplicable a los miembros del Comité de Empresa y este en su conjunto, así como, en su caso, los expertos que les asistan, respecto a aquella información que, en legítimo y objetivo interés de la entidad y en cumplimiento de la legalidad vigente, se les haya comunicado expresamente con carácter reservado. Tal y como establece el ET, en todo caso, ningún tipo de documento entregado por la empresa al comité podrá ser utilizado fuera del estricto ámbito de aquella ni para fines distintos de los que motivaron su entrega. El deber de sigilo subsistirá incluso tras la expiración de su mandato e independientemente del lugar en que se encuentren.

6.8 Exención de responsabilidad

La Entidad empleará todos los mecanismos de los que disponga para garantizar la seguridad de los recursos y servicios del sistema. En virtud de los principios de responsabilidad y autoprotección, los usuarios/as deberán adoptar todas aquellas medidas que garanticen la seguridad del sistema informático de la Entidad.

La Entidad, aunque procurará la aportación de todos los medios materiales y humanos que permitan la continua disponibilidad y buen funcionamiento de los recursos y servicios provistos por los sistemas de información, no puede garantizar que dicho buen funcionamiento tenga lugar en todo momento. Las interrupciones en su funcionamiento serán previamente advertidas sólo si ello es racionalmente posible.

La Entidad queda eximido de cualquier responsabilidad derivada del mal funcionamiento de los recursos y servicios que tenga su origen en una circunstancia accidental, fuerza mayor, trabajos necesarios de mantenimiento o cualquier otra causa no imputable al mismo.

La utilización de estos recursos y servicios está sometida a la exclusiva responsabilidad del usuario/a de los mismos, que conoce esta circunstancia y la acepta.

6.9 Proceso disciplinario

Todos los usuarios/as de los sistemas de información y de los recursos informáticos de la Entidad están obligados a cumplir lo prescrito en la presente Norma Interna de Uso de Medios Electrónicos.

Cualquier incumplimiento de lo indicado en la presente Norma, ya sea de forma intencionada o por una utilización negligente, puede dar lugar a la suspensión temporal o definitiva del uso de los recursos y servicios asignados al usuario/a, sin perjuicio de la revisión de los hechos concretos en el ámbito de la normativa disciplinaria en el caso de los empleados/as públicos/as y, de manera general, de las responsabilidades a que, en su caso, hubiere lugar en materia penal y/o civil.

La valoración de las consecuencias del incumplimiento para el infractor, y las medidas a adoptar serán tomadas de conformidad con las normas que regulan la relación de servicio, funcionarial o laboral entre la Entidad y el usuario/a, y serán los órganos competentes de la Entidad los que decidirán las acciones a tomar en el caso de incumplimiento de la presente Normativa.

Anexo I. Normas de uso del correo electrónico

El objetivo del presente epígrafe es regular el acceso y utilización del correo electrónico (e-mail) por parte de los usuarios/as de los Sistemas de Información de la Entidad, con el objeto de homogeneizar criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios/as.

Concepto. El correo electrónico es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios/as de la Entidad para el envío y recepción de las comunicaciones mediante el uso de cuentas de correo corporativas. Junto con los mensajes también pueden ser enviados ficheros adjuntos.

Caracteres. Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.

Especificaciones. La Entidad, conscientes de los problemas de seguridad y responsabilidad legal que ocasiona el uso del correo electrónico, dispone las siguientes especificaciones:

Responsabilidad	• Los usuarios/as serán responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la Entidad. • Los usuarios/as deberán ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por la Entidad. • Las cuentas de correo son personales e intransferibles. Salvo en casos puntuales -para los que deberá solicitarse y obtenerse la correspondiente autorización-, no se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información confidencial. • Los mensajes de correo transmiten información en sus cabeceras (en principio ocultas) que indican datos adicionales del emisor, por lo que deben tenerse en cuenta posibles repercusiones (como daños a la imagen institucional) que podría acarrear una mala utilización de este recurso.
Uso aceptable	• Como norma general, no se utilizará la herramienta de correo electrónico con fines ajenos al propio desarrollo de las actividades que cada usuario/a tiene encomendadas en la Entidad. • La utilización del correo electrónico por personal externo requiere la previa autorización por escrito de la Dirección. • La forma y contenidos de los correos enviados por el usuario/a en ningún caso podrán ser ofensivos, amenazantes o de mal gusto. • El usuario/a debe mantener ordenados y clasificados todos sus buzones y carpetas. Los correos inservibles deben ser eliminados, y todos los archivos adjuntos almacenados en el equipo o unidad de disco habilitada.

Usos no permitidos que implican un riesgo para la seguridad	• La instalación y uso de cualquier otra aplicación de correo electrónico, así como de una versión diferente de la aplicación homologada que no haya sido autorizada e instalada por el personal técnico autorizado. • La difusión de contenido ilegal; como por ejemplo amenazas, código malicioso, apología del terrorismo, pornografía infantil, software pirata, o de cualquier otra naturaleza delictiva. • El uso no autorizado de servidores propiedad de la Entidad para el envío de correo personal. • El envío masivo de correos publicitarios o de cualquier otro tipo que no guarde relación alguna con las necesidades de negocio de la Entidad. Este hecho, además, puede llegar a ser interpretado como “spamming”. • La divulgación, independientemente del formato en que se encuentren, de correos que revelen datos del directorio o de usuarios/as pertenecientes a la Entidad, fuera de los límites laborales establecidos por la misma. • En el caso de se requiera enviar un mensaje de correo electrónico a varios destinatarios, se utilizará preferentemente el campo CCO (copia oculta) para introducir las direcciones de correo de los destinatarios, con excepción de aquellos mensajes en los que necesariamente se requiera la identificación de todos los destinatarios para confirmar que han sido informados.
Diligencia	• Los archivos adjuntos recibidos serán analizados por las herramientas antivirus antes de ser abiertos o ejecutados. Los correos sospechosos o de dudosa procedencia no serán abiertos, y menos aún los archivos adjuntos que contengan. Su eliminación debe ser inmediata. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.). • No emplear el correo electrónico como medio de comunicación para enviar o recibir información confidencial o que contenga datos que correspondan a categorías especiales según el RGPD (datos de salud, opiniones políticas, afiliación sindical, religión, convicciones religiosas, origen racial o étnico, vida sexual, datos genéticos o biométricos, orientación sexual). Únicamente, y en aquellos casos en los que sea estrictamente necesario, se utilizará este medio, en cuyo caso, se enviará con las medidas de seguridad apropiadas para cada tipo concreto de información mediante la utilización de un software de cifrado, previa autorización expresa del Responsable del Tratamiento. • En la medida de lo posible, desactivar la vista previa. Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos. Del mismo modo, limitar el uso de HTML. El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute. • Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.

	• Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada. • Desactivar las características de recordar contraseñas para el navegador. • Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.
Incidencias	• Los usuarios/as, con la mayor diligencia posible, deberán comunicar al Responsable de Seguridad (siguiendo el proceso de comunicación de incidencias y peticiones que la Entidad tenga establecido) y a sus responsables directos sobre cualquier anomalía que detecten en su correo, así como de la apertura de un correo sospechoso o cualquier alerta generada por el antivirus.
Monitorización	• La Entidad se reservan el derecho a revisar los ficheros LOG de los servidores, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la Entidad como responsable civil subsidiario.

Anexo II. Normas de uso de Internet

El objetivo de la presente Norma es regular el uso de Internet por parte de los usuarios/as de la Entidad, con el objeto de homogeneizar criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios/as

Con carácter general, los usuarios/as de la Entidad disponen de acceso corporativo a Internet como herramienta de productividad, conocimiento, apoyo al desempeño y mejora de los sistemas de trabajo y búsqueda de información. Esta herramienta es propiedad de la Entidad, la cual se reserva el derecho de conceder o anular dichos accesos conforme a los criterios que crea convenientes.

Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet, por los siguientes motivos:

- Seguridad: debido al riesgo de infección por software dañino (virus, troyanos, etc.).
- Volumen del tráfico externo de datos: garantizando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias de la Entidad.
- Volumen del tráfico interno de datos: como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
- Ética: es ineludible el compromiso que la Entidad debe mantener con la sociedad, a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

Responsabilidad	• Internet es un servicio que la Entidad pone a disposición de su personal para uso estrictamente profesional. • Los usuarios/as son los únicos responsables de las sesiones iniciadas en Internet con sus credenciales de acceso, y se comprometen a acatar las reglas y normas de funcionamiento establecidas en la presente Normativa. • El acceso a Internet el contenido al que el usuario/a puede acceder a través de Internet desde los recursos y servicios propiedad de la Entidad, así como a monitorizar y registrar los accesos realizados desde los mismos. En caso de que un usuario/a considere necesario acceder a alguna dirección incluida en una de las categorías filtradas, se pondrá en contacto con su responsable directo para que éste gestione el acceso correspondiente.
Usos no permitidos que implican un riesgo para la seguridad	• En ningún caso se modificarán las configuraciones de los navegadores (opciones de Internet) de los equipos ni la activación de servidores o puertos sin la autorización expresa. Todos los equipos que así lo estima la Entidad, ya están configurados para su acceso a Internet. • Se prohíbe expresamente el acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las

	buenas costumbres y, en general, de todo tipo de contenidos que incumplan las normas éticas y de cortesía de la Entidad. • No se permite el almacenamiento en los equipos de archivos y contenidos personales descargados vía Internet, especialmente aquellos que violen la legislación vigente relativa a Propiedad Intelectual. Los usuarios/as deberán respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual de cualquier información visualizada u obtenida mediante Internet haciendo uso de los recursos informáticos o de red de la Entidad. • Se prohíbe el uso de Internet mediante los recursos informáticos o de red de la empresa con fines recreativos, así como para obtener o distribuir material violento o pornográfico, o para obtener o distribuir material incompatible con los valores de la Entidad. • No está permitido el uso de chats o programas de conversación en tiempo real que no hayan sido previamente autorizados. • La descarga de software ejecutable desde internet, salvo que se autorice de forma expresa.
Incidencias	• Cualquier incidente de seguridad relacionado con la navegación por Internet, deberá ser comunicado sin demora al responsable directo oportuno y al Responsable de Seguridad (siguiendo el proceso de comunicación de incidencias y peticiones que la Entidad tenga establecido).

Anexo III. Modelo de aceptación y compromiso de cumplimiento

Todos los usuarios/as de los recursos informáticos y/o sistemas de información de la Entidad deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa de Uso de Interno de Medios Electrónicos.

Para su aceptación se ha elaborado el presente modelo de aceptación de la Normativa de uso de medios electrónicos:

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal de la Entidad* _____ *],* como usuario/a de recursos informáticos y sistemas de información de la Entidad, declara haber leído y comprendido la Normativa de Usos de medios electrónicos de la Entidad (*versión x*), y aceptar los términos y condiciones de uso establecidos en el mismo, estando de acuerdo en cumplirlos, atender a las modificaciones del documento que le hayan sido debidamente comunicadas, comprometiéndose, bajo su responsabilidad, a su cumplimiento. La normativa se encuentra publica en la siguiente dirección pública:

https://www.tenerife.es/documentos/TenerifeES/NOR-010.pdf

A su vez, se hace entrega de las credenciales (usuario y contraseña que el usuario deberá modificar tras el primer uso), quedando constancia de su recepción con la firma del presente formulario.

En _____, a ____ de _____ de 20__

Entidad:	<Nombre Entidad>
Trabajador (Nombre y Apellidos):	
DNI número:	
Firmado:	

Por: <<Nombre y Apellidos>>

DNI número: _____

Anexo IV. Normas de tratamiento de datos de carácter personal

FICHEROS INFORMÁTICOS

En particular, respecto a la información de carácter personal contenida en ficheros informáticos, deberá cumplir, en consonancia con lo expuesto en anteriores apartados, las siguientes diligencias:

- **Claves de acceso al sistema informático. -** Las contraseñas de acceso son personales e intransferibles, siendo el Usuario/a el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. Queda prohibido, asimismo, emplear identificadores y contraseñas de otros Usuarios para acceder al sistema informático.
- **Bloqueo o apagado del equipo informático. -** Bloquear la sesión del Usuario/a en el supuesto de ausentarse temporalmente de su puesto de trabajo. Esto, sobre todo, deberá tenerse en cuenta, por parte del personal que esté en atención al público.
- **Almacenamiento de archivos o ficheros en la red informática. -** Guardar todos los ficheros de carácter personal empleados por el Usuaria/o, en el espacio de la red informática habilitado por la Entidad, a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.
- **Manipulación de los archivos o ficheros informáticos. -** Únicamente las personas autorizadas, podrán introducir, modificar o anular los datos personales contenidos en los ficheros. Los permisos de acceso de los Usuarios/as a los diferentes ficheros son concedidos por la Entidad según el procedimiento establecido.
- **Generación de ficheros de carácter temporal. -** Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea/s determinada/s. Estos ficheros deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática.
- **No uso del correo electrónico para envíos de información de carácter personal sensible. -** No utilizar el correo electrónico (corporativo o no) para el envío de información de carácter personal especialmente sensible (esto es, salud, ideología, religión, creencias, origen racial o étnico). Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros. De modo que, se pondrá en conocimiento del Departamento de Informática para que implemente el cifrado, encriptado u otro mecanismo que salvaguarde la integridad y privacidad de la información.
- **Comunicación de incidencias que afecten a la seguridad de datos de carácter personal. -** Comunicar las incidencias de seguridad de las que se tenga conocimiento según el procedimiento establecido.

FICHEROS EN PAPEL

En relación con los ficheros en soporte o documento papel, el Usuario deberá cumplir con las siguientes diligencias:

- **Custodia de llaves de acceso a archivadores o dependencias. -** Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios, archivadores u otros elementos que contenga soportes o documentos en papel con datos de carácter personal.
- **Cierre de despachos o dependencias. -** En caso de disponer de un despacho, cerrar con llave la puerta, al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
- **Almacenamiento de soportes o documentos en papel. -** Guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro, cuando éstos no sean usados, particularmente, fuera de la jornada laboral. Cuando estos soportes o

documentos, no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso.

- **No dejar en fotocopiadoras, faxes o impresoras papeles con datos de carácter personal. -** Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de la fotocopiadora, impresora o faxes.
- **Documentos no visibles en los escritorios, mostradores u otro mobiliario.** - Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario.
- **Desechado y destrucción de soportes o documentos en papel con datos personales. -**No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información. A estos efectos, deberá ser siempre desechada o destruida mediante destructora de papel u otro medio. Se prohíbe terminantemente echar en papeleras, contenedores de cartón o papel, soportes o documentos, donde se contengan datos personales.
- **Archivo de soportes o documentos. -** Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo de la Entidad. Dichos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información. Los soportes o documentos se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de los mismos.
- **Traslado de soportes o documentos en papel con datos de carácter personal.**- En los procesos de traslado de soportes o documentos deberán adoptarse medidas dirigidas para impedir el acceso o manipulación por terceros y, de manera que, no pueda verse el contenido, sobre todo, si hubieren datos de carácter personal. Deberá evitarse la utilización de carpetas transparentes, o especialmente frágiles y sustraer o poner a la vista de terceros el contenido de los documentos, durante el trayecto.
- **Traslado de dependencias.** - En caso de cambiar de dependencia, en el proceso de traslado de los soportes o documentos en papel, se deberá realizar con el debido orden. Asimismo, se procurará mantener fuera del alcance de la vista de cualquier personal de la entidad, aquellos documentos o soportes en papel donde consten datos de carácter personal.
- **Envío de datos personales sensibles en sobre cerrado. -** Si se envían a terceros ajenos a la Entidad, datos especialmente sensibles (esto es, salud, ideología, afiliación sindical, religión, creencias, origen racial o étnico) contenidos en soporte o documento papel, se debe realizar, en sobre cerrado y, en cualquier caso, tener presente que haya de efectuarse por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.
- **Entrega de documentación con detalles de empleo a RR.HH.:** Cuando los empleados entreguen a los responsables de RR.HH. documentación: nóminas firmadas, partes de alta o baja, u otra documentación que contenga información relativa a los detalles de empleo, deberán de ser entregados en mano al responsable, o bien dentro de un sobre cerrado indicando a quién va dirigido.
- **Comunicación de incidencias que afecten a la seguridad de datos de carácter personal. –** Se deberán comunicar las incidencias de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales.

Anexo V. Modelo derecho de información tratamiento datos personales

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL		
Responsable del tratamiento	**Entidad** Dirección Teléfono Cuenta de correo electrónico	
Delegado de Protección de Datos	Cuenta de correo electrónico de DPD	
		Plazo de conservación
Usos y finalidades de los datos	**RECURSOS HUMANOS Y GESTIÓN DE NÓMINAS. -** Gestión, Selección, Promoción y/o Formación; Gestión de nóminas y otros tipos de retribuciones. Gestión de Personal [Altas, Bajas, Viajes y Pernoctas, Nóminas, Anticipos, Permisos y licencias, Vacaciones, Control de horario, así como otros aspectos relativos al ámbito laboral].	Los datos serán conservados aun después de que hubiera cesado la relación laboral con la Entidad, durante el tiempo que puedan ser requeridos por control o fiscalización de la entidad pública competente (Organismo de la Seguridad Social, Agencia Tributaria, Juzgados o Tribunales).
	PREVENCIÓN DE RIESGOS LABORALES. - Gestión de la Prevención de Riesgos Laborales, con tratamiento de información relativa al puesto de trabajo y situaciones de riesgo, así como formación en la materia.	
	SERVICIO MÉDICO Y VIGILANCIA DE LA SALUD. - Gestión y control servicios de vigilancia de la salud. En este caso, los datos personales son tratados, única y exclusivamente, por personal sanitario y/o sometido a un deber de secreto o sigilo profesional pertenecientes a nuestro servicio propio o, en su caso, a entidad/es contratada/s a estos efectos; no teniendo la Entidad, acceso a esta información de carácter personal, conforme establece la legislación en Prevención de Riesgos Laborales. De este modo, los resultados de las pruebas médicas a las que sea sometido el trabajador sólo serán comunicados al mismo, de forma confidencial. La Entidad única y exclusivamente, será informada acerca de la aptitud para el desempeño del puesto de trabajo.	
	FORMACIÓN. - Gestión de las inscripciones en los cursos de formación obligatoria. Control de asistencia. Expedición de títulos. Constancia de formación particular voluntaria.	
	TRATAMIENTO IMAGEN **a) Medida de control y puesta en conocimiento del personal. -**La imagen (fotografía) es necesaria para la identificación del personal dentro del organigrama de la entidad, así como por motivos de seguridad, sirve para el control de acceso a las instalaciones. Se incluirá, en su caso, en espacio corporativo, a nivel electrónico o de forma impresa. **b) Promoción o difusión de la actividad. -**Solicitamos su autorización para la captación de su imagen y su publicación en página web de la entidad y/o redes sociales u oros medios de difusión, con el fin de promocionar las actividades de la entidad:	a) Será conservada durante la vigencia de la relación laboral. b) Será conservada mientras dispongamos de su consentimiento.

	☐AUTORIZO ☐NO AUTORIZO	
	DATOS BIOMÉTRICOS. - Tratamiento de la huella digital o dactilar a los efectos de control horario y la presencia en el puesto de trabajo.	La huella digital o dactilar se conservará por el tiempo que esté vigente el contrato laboral.
	VIDEOVIGILANCIA. – La Entidad está dotado de un sistema de videovigilancia a los efectos de preservar la seguridad de los bienes, personas e instalaciones.	Las imágenes son conservadas por un tiempo no superior a un mes. En caso de que se captaran hechos ilícitos o irregulares las imágenes se mantendrán bloqueadas para la puesta a disposición, en su caso, de las autoridades competentes.
Legitimación	Los datos son tratados en base a la relación laboral contraída con la Entidad y, en su caso, al consentimiento del uso de determinados datos, según los fines antes expresados. En particular, el tratamiento de las imágenes del sistema de videovigilancia está legitimado en el interés público de garantizar la seguridad de personas, bienes e instalaciones.	
Destinatarios de los datos (cesiones o transferencias)	La información de carácter fiscal y laboral recabada será comunicada, en su caso, a los Organismos de la Seguridad Social, Administración Tributaria, INEM, Autoridad Laboral, así como a Órganos de representación, en los supuestos previstos y fijados por la normativa aplicable. Los datos económicos de su nómina serán cedidos a la entidad bancaria o financiera concertada para el pago de nóminas. Así como, a la gestoría o asesoría que fuere contratada para la llevanza de los asuntos de índole laboral de la Entidad. Si durante la vigencia de la relación laboral con la Entidad, Vd. es seleccionado para asistir a cursos de formación, sus datos personales serán cedidos al docente y/o centro donde se impartirán, a efectos de mantener un control de los asistentes y, en su caso, la expedición del título respectivo.	
Política de uso de las TIC	Todos los recursos de la Tecnología de la Información y Comunicación (TIC) de la entidad, incluyendo conexión a Internet, ordenadores y dispositivos móviles o portátiles, son para fines estrictamente laborales y, por tanto, no se utilizarán para fines particulares. La Entidad podrá implantar medidas de vigilancia y control (monitorización) para verificar el funcionamiento de los medios, recursos o dispositivos T.I.C. No se accederá al contenido de las comunicaciones, salvo indicios fundados que mostrarán una conducta ilícita.	
Derechos	Ud. podrá ejercitar los derechos de Acceso, Rectificación, Limitación, Supresión o, en su caso, Oposición. Para ejercitar los derechos deberá presentar un escrito en la dirección arriba señalada, o a nuestro Delegado de Protección de Datos https://.....sedelectronica.es. Deberá especificar cuál de estos derechos solicita sea satisfecho y, a su vez, deberá acompañarse de la fotocopia del NIF o documento identificativo equivalente. En caso de que actuara mediante representante, legal o voluntario, deberá aportar también documento que acredite la representación y documento identificativo del mismo. Asimismo, en caso de considerar vulnerado su derecho a la protección de datos personales, podrá interponer una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es).	
Firma	Como prueba de conformidad con cuanto se ha manifestado acerca del tratamiento de mis datos personales, firmo la presente. Nombre y Apellidos: Fdo.	