Esquema Nacional de Seguridad (ENS)

NOR-001 P

NORMATIVA DE USO DE LOS SISTEMAS DE INFORMACIÓN

Julio 2023

Código	Versión	Fecha	Modificación
NOR-001 P	2.7	02-2023	Revisión
NOR-001 P	3.0	07-2023	Inclusión de calificación de la información
NOR-001 P	4.0	05-2026	Inclusión de Navegación web

Elaborado por:	Revisado por	Aprobado por	Responsable Documento
RSIS	Comité de Seguridad; Comité DPD; RRHH	Junta de Gobierno Local	Responsable de Seguridad

Clasificación: OFICIAL GENERAL

ÍNDICE

1. OBJETO

Conforme a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS, en adelante), este documento contiene la **Normativa de Uso de los Sistemas de Información del Ayuntamiento de Pamplona**, gestionados bajo su responsabilidad, señalando asimismo los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.

Los **Sistemas de Información**[1] constituyen elementos básicos para el desarrollo de la actividad del Ayuntamiento de Pamplona, por lo que los usuarios deben utilizar estos recursos de manera responsable mediante el seguimiento de normas, políticas y buenas prácticas que salvaguarden los sistemas de información y los recursos tecnológicos proporcionados por la Entidad, de manera que se garantice su correcta y óptima utilización.

El objeto del presente documento es establecer 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 la información municipal (incluidos datos de carácter personal), en soporte electrónico y en papel razón por la cual el Ayuntamiento de Pamplona determina las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.

Las aplicaciones informáticas, el correo electrónico, la utilización de Internet, redes de datos y de otros dispositivos, se han convertido en herramientas importantes y necesarias, tanto para la gestión interna de la Entidad, como para la ciudadanía que interactúa con ella a través de Sedes electrónicas y otros medios puestos a su disposición. Es preciso garantizar que tanto su uso, con un alto grado de confianza, y un nivel de servicio adecuado y razonable.

Es fundamental que todo el personal de la Entidad que utiliza sistemas de información municipales en el desarrollo de sus funciones sea conocedor de esta norma.
Este documento se considera de uso interno y, por consiguiente, no podrá ser divulgado salvo autorización.

2. ALCANCE

Esta Normativa General es de aplicación a todo el ámbito de actuación del Ayuntamiento de Pamplona y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de

[1] Se entiende por **Sistema de Información** todo conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. (RD 311/2022, ENS – Anexo IV – Glosario.

Seguridad de la Información, así como de los principios morales y éticos en la utilización de los recursos puestos a disposición de las personas usuarias para el desempeño de sus actividades.

Mediante la presente Normativa, se establece la regulación del uso de los sistemas de información y recursos tecnológicos de la Entidad, a través del establecimiento de medidas de cumplimiento obligatorio para todas las personas que, de manera permanente o eventual, presten sus servicios en el Ayuntamiento de Pamplona, en las Entidades Dependientes o vinculadas al mismo, o accedan a los sistemas, incluyendo en su caso, el personal de proveedores externos, cuando proceda y sea usuario de los Sistemas de Información del Ayuntamiento de Pamplona

En el ámbito de la presente normativa, se considera persona usuaria a cualquier persona que se conecte a la red del Ayuntamiento de Pamplona o a alguno de los Sistemas de Información del Ayuntamiento de Pamplona.

3. LEGISLACIÓN Y NORMATIVA APLICABLE

Las referencias tenidas en cuenta para la redacción de esta normativa han sido las indicadas en el punto Marco Normativo de la Política de Seguridad aprobada, el cual está integrado por la legislación definida en un registro al efecto.

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".

4. ROLES Y RESPONSABILIDADES

La gestión de esta Normativa corresponde a la Gerencia la cual es competente para:

- Interpretar las dudas que puedan surgir de su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Con periodicidad anual el Comité de Seguridad revisará la presente Normativa, que se someterá, en caso de que existan modificaciones, a la aprobación por el Comité TICS y por la Junta de Gobierno Local. Los puntos mínimos a considerar en las revisiones serán los siguientes:

- Identificación de acciones de mejora en la gestión de la seguridad de la información.
- Adaptación a los posibles cambios normativos, de infraestructuras tecnológicas, organizativas, etc.
- La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el

marco legal, infraestructura tecnológica, organización general, etc.

Será el Comité de Seguridad, el órgano encargado de la custodia y divulgación de la versión aprobada de este documento.

5. NORMATIVA INTERNA DE USO DE LOS SISTEMAS DE INFORMACIÓN

5.1. CONSIDERACIONES PREVIAS

Las normas que se indican en este apartado se aplicarán a todas las personas usuarias que utilicen cualquiera de los dispositivos facilitados por el Ayuntamiento de Pamplona, así como las personas u organizaciones que usando otro tipo de dispositivos acceden a los sistemas de información de la entidad.

Se entiende por **dispositivo** cualquier medio electrónico, tecnológico, equipo informático y de comunicaciones con capacidad de acceso a los Sistemas de Información de la Entidad.

Se entiende por **sistema de Información** todo conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Los dispositivos y el sistema de información que el Ayuntamiento de Pamplona pone a disposición de los usuarios, únicamente deberá ser utilizado para el desempeño de las funciones y tareas que tengan encomendadas, y deberá hacerse un uso diligente de los mismos.

Los dispositivos propiedad del Ayuntamiento de Pamplona que pone a disposición de las personas usuarias carecen de la consideración de sistema particular privado y no están destinados a un uso personal.

En lo relativo a los activos de información, también se deberá considerar que toda la información albergada, transmitida, desarrollada o procesada por cualquiera de los sistemas carecerá de carácter privado, siendo la Entidad su único titular.

El acceso a los Sistemas de Información de la Entidad por medios electrónicos, supone un riesgo que exige adoptar una serie de precauciones y medidas para su adecuada utilización. Por ello todos los dispositivos deben incorporar medidas técnicas y de protección, para reducir las vulnerabilidades que puedan llegar a tener.

5.2. NORMAS GENERALES DE USO DE DISPOSITIVOS

- Toda persona que disponga o haga uso de algún recurso informático es responsable directo de su correcta utilización. Será responsable del buen uso, mantenimiento y protección de los dispositivos que le han sido entregados.
- Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido. Todos los activos entregados por la

organización, incluyendo dispositivos, soportes y datos, deberán ser devueltos al final de la relación laboral, salvo acuerdo entre las partes. Salvo autorización expresa, las personas usuarias no tendrán privilegios de administrador sobre los equipos.

ⓘ Solo se podrá utilizar software homologado por ANIMSA. Su instalación deberá solicitarse siempre a ANIMSA. La instalación se realizará velando por que provenga de una fuente fiable, que se posean las licencias de uso oportunas, y que funcione de forma adecuada en el equipo destino.

Las siguientes actividades están expresamente prohibidas:

✗ Conectar dispositivos que no estén autorizados a la red de la Entidad o conectar a los dispositivos autorizados, otros dispositivos que no estén autorizados expresamente.

✗ Alterar la configuración física, configuración de seguridad ni el software de los dispositivos.

✗ Destruir, alterar, inutilizar o dañar de cualquier otra forma los datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos de la Entidad o de terceros.

✗ Obstaculizar intencionadamente el acceso de otras personas a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la Entidad, así como realizar acciones que dañen, interrumpan o generen errores en sus sistemas.

✗ Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la Entidad o de terceras organizaciones sin autorización.

✗ Intentar aumentar el nivel de privilegios de una persona usuaria en el sistema.

✗ Introducir voluntariamente programas, código no autorizado o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la Entidad o de terceros.

✗ Instalar copias ilegales de cualquier programa.

✗ Extraer sin permiso de las instalaciones de la Organización cualquiera de los componentes lógicos o físicos de los sistemas, con la excepción de aquellos elementos (portátiles, teléfonos móviles, dispositivos USB) de cuya naturaleza se desprenda su carácter portátil, y de los que se tenga permisos de uso.

5.2.1. Normas específicas para portátiles y dispositivos móviles

Se considerarán **dispositivos móviles** los equipos portátiles, tabletas y terminales móviles, así como cualquier dispositivo portátil que permita el trabajo fuera de las instalaciones de la organización.

En relación con el uso de dispositivos móviles, se adoptarán las siguientes medidas de seguridad:

- Los equipos se entregan con unas medidas de seguridad implementadas, quedando prohibida modificar, desactivar o eliminar las medidas de seguridad configuradas por defecto.
- La información contenida en los dispositivos deberá estar cifrada o, en su defecto, protegida mediante contraseña, eliminando la información una vez deje de ser necesaria.
- Cada usuario es responsable de:
  - la información almacenada en los dispositivos móviles y del uso realizado con ella.
  - copiar en ubicaciones de red la información sensible contenida en dispositivos móviles con el fin de garantizar las copias de seguridad de la misma.
  - custodiar el equipo móvil, siendo la persona usuaria responsable de adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas. Está terminantemente prohibido dejar los dispositivos sin vigilancia o custodia.
- La sustracción, pérdida o extravío del dispositivo deberá ser notificado a Atención a Usuarios de ANIMSA tan pronto como sea posible, para la adopción de las medidas que correspondan.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el proyecto, etc.) que originaron la entrega de un dispositivo informático, se deberá devolver al Departamento de Sistemas de ANIMSA para que pueda ser asignado a un nuevo usuario. En el momento de devolver el dispositivo se debe garantizar la correcta eliminación del contenido.
- Con carácter general no está permitido el uso de dispositivos móviles propios, "BYOD (Bring Your Own Device)", para el acceso o almacenamiento de información municipal salvo autorización expresa. En todo caso, se seguirá el procedimiento indicado en la Política de BYOD correspondiente.

5.3. ACCESO A LOS SISTEMAS DE INFORMACIÓN

Se entiende por **Sistema de Información** a todo conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

La mayor parte de los procedimientos administrativos se gestionan en la actualidad accediendo desde diferentes dispositivos a aplicaciones que residen en servidores conectados a la red corporativa municipal. Estos accesos se regirán por las siguientes medidas.

5.3.1. Permisos de acceso

- Para acceder a los sistemas de información es necesario haber sido dado previamente de alta en los servicios corporativos.
- El alta de las personas en el sistema se realizará según el sistema establecido para gestionar las Altas, Bajas y Modificaciones de Personal. El alta de los usuarios seguirá el procedimiento indicado en la Política de Gestión de usuarios correspondiente.
- La autorización del acceso tendrá en cuenta los principios de mínimo privilegio y la necesidad de conocer, por el que se establece el perfil necesario de cada persona según sus funciones encomendadas, de manera que se autorice solo el acceso a la información y recursos que precise para el desarrollo de las mismas.
- Se comunicará siempre la baja de las personas usuarias para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo cuando estas personas finalicen la actividad laboral por la que se les concedió el acceso o ante variaciones de sus funciones o departamentos.

5.3.2. Credenciales de acceso

- Cuando se da de alta una persona en los servicios corporativos se le asigna unas **credenciales** de acceso compuestas por una **cuenta de usuario** y una **contraseña**.
- La cuenta de usuario es única para cada persona en el Ayuntamiento, e independiente del dispositivo desde el que se realiza el acceso.
- Todo acceso al sistema, dispositivos y aplicaciones corporativas, requiere la identificación mediante usuario y contraseña y son de uso único e intransferible. Nunca debe utilizarse la cuenta asignada a otra persona.
- En aquellos sistemas que dispongan de doble factor de autenticación (2FA) se habilitará el mismo siempre y cuando la persona usuaria disponga de los medios necesarios para validarse utilizando 2FA.
- Las personas usuarias no revelarán o entregarán, bajo ningún concepto, sus credenciales de acceso a otra persona, ni las mantendrán por escrito a la vista o al alcance de terceros. Nunca se deben compartir. La responsabilidad de las consecuencias de un acceso inadecuado, será de la persona titular de la cuenta de usuario que haya quedado registrada en el sistema
- No está permitido emplear identificadores y contraseñas de otras personas para acceder al sistema y a la red de la Entidad.
- Si una persona tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, deberá proceder inmediatamente a comunicar la correspondiente incidencia de seguridad.

- ⓘ Es responsabilidad de cada persona hacer buen uso de su cuenta y accesos. En caso de mala utilización esta cuenta podrá ser desactivada.
- ⓘ Cuando una persona deje de atender su equipo durante un cierto tiempo, se bloqueará la sesión o se activarán los salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo.
- ✗ No está permitido intentar modificar el registro de accesos.

5.3.3. Uso de contraseñas.

Para el establecimiento de contraseñas hay que tener en cuenta los siguientes aspectos:

- ⓘ Establecer contraseñas seguras y seguir las recomendaciones de buenas prácticas publicadas.
- ⓘ Que tengan una longitud mínima de 8 caracteres y que incluyan letras mayúsculas y minúsculas, caracteres especiales (del tipo @, #, +, etc.) y dígitos.
- ⓘ Que no estén compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables a la persona usuaria (nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de la persona usuaria, de grupo o del sistema, DNI, etc.)
- ⓘ Las contraseñas no deben anotarse: deben recordarse. En caso de necesitarlo, utilizar gestores de contraseñas.
- ⓘ Las contraseñas deben cambiarse periódicamente y siempre que se considere conveniente. Esto garantiza el uso privado de las mismas.
- ⓘ Las políticas de contraseñas seguras podrán forzarse desde sistemas utilizando mecanismos habilitados al efecto en los servicios de gestión de identidades municipales.

5.4. CALIFICACIÓN DE LA INFORMACIÓN

Teniendo en cuenta lo establecido legalmente sobre la naturaleza de esta, en base a la legislación definida en la Política de Seguridad de la Información, el Ayuntamiento de Pamplona ha establecido una serie de **niveles y subniveles de calificación de la información:**

- ⓘ **Pública:** Se considerará toda aquella información de uso general y público dentro y fuera del Ayuntamiento. La divulgación, pérdida o destrucción de esta información no generará ningún impacto.
- ⓘ **Uso oficial:** Se considerará toda aquella información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad, qué sólo debe ser conocida por los integrantes del Ayuntamiento (todos o parte). Se divide en:

- **Interna:** Información que no se debe distribuir al público en general, sino que es información que puede ser conocida por todos los miembros dentro del Ayuntamiento (todos o parte), y no por personas externas a la misma, salvo autorización expresa. En este caso, la divulgación no autorizada, pérdida o destrucción de esta información podrá generar impactos limitados para la organización.
- **Sensible:** Información que no debe distribuirse, ya que es información que puede ser conocida únicamente por destinatario/s específico/s dentro del Ayuntamiento y cuya divulgación no autorizada, pérdida o destrucción pueda generar impactos importantes para la entidad local siendo la siguiente:
  - Categorías especiales de datos establecidos en el artículo 9 del Reglamento Europeo de Protección de Datos (RGPD): origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, salud, vida sexual, orientación sexual o artículo 10 del RGPD (condenas e infracciones penales).
  - Información que contiene datos personales, que sin considerarse de categorías especiales contienen datos de carácter personal que no son difusión pública.
  - Documentos en fase de desarrollo, contengan datos personales o no, que sirvan de soporte para la elaboración de la documentación de trabajo.

La **NOR_004P Normativa de calificación de la Información** desarrollará este apartado, incluyendo las medidas de seguridad asociadas a cada nivel de calificación.

5.5. CUIDADO Y PROTECCIÓN DE LA INFORMACIÓN

La información manejada en el quehacer diario se encuentra sometida a importantes riesgos como la pérdida, el robo o la fuga de información, entre otras amenazas. Esto cobra especial importancia si se trata de datos sensibles, confidenciales, o protegidos, que deberán ser custodiados de forma que sólo tengan acceso a los mismos las personas debidamente autorizadas.

Las personas usuarias de la información deben ser conscientes de sus responsabilidades respecto al uso seguro de los misma.

En líneas generales:

- Es responsabilidad de la persona usuaria conocer, aceptar y cumplir la normativa vigente en materia de seguridad relacionada con el desempeño de sus funciones.

- ⓘ El personal deberá restringir a terceros el acceso a los archivos o tratamientos de datos titularidad del Ayuntamiento de Pamplona.
- ⓘ Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando la persona usuaria del mismo así lo solicite o cuando se trate de datos especialmente protegidos que requieran de las medidas de seguridad establecidas por la legislación vigente.
- ✗ 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.
- ✗ La persona usuaria se abstendrá de copiar cualquier tipo de información del Ayuntamiento de Pamplona en ordenadores propios, pendrives o a cualquier otro soporte informático, salvo que solicite autorización al responsable de la Información 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.

5.5.1. Almacenamiento de la información.

- ⓘ Toda la información tratada por el personal del Ayuntamiento de Pamplona debe ser tratada y almacenada en los sistemas de información corporativos diseñados para tal fin ya que disponen de las medidas de seguridad, salvaguarda y soporte correspondientes.
- ✗ No se permite la incorporación de información dentro de los sistemas de información (documentos escaneados, fotografías, …) que no se correspondan con la actividad laboral y sin la autorización correspondiente. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartido ni local.
- ⓘ En el caso de ser necesaria la incorporación de información especialmente sensible, deberá solicitarse autorización al responsable funcional del tratamiento, siendo ésta quien autorizará o no dicho tratamiento y almacenamiento.
- ⓘ Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todos los usuarios, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria

5.5.2. Copias de seguridad

- ⓘ De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades de red corporativas

compartidas y gestionadas por ANIMSA donde se almacene la información.

- La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de dirigirse a Atención a Usuarios de ANIMSA.
- Con carácter general, la información almacenada de forma local en los equipos de los usuarios (disco duro local) **no será objeto** de salvaguarda mediante ningún procedimiento corporativo. Por tanto, cuando tal almacenamiento esté autorizado, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.

5.5.3. Gestión de soportes de información.

Se entiende por **soporte de información** tanto los discos los servidores y equipos de usuario final como los discos removibles, cintas, CD, DVD, USB, tarjetas de memoria, componentes de impresoras, material impreso y cualquier otro medio de almacenamiento de información con capacidad de que la información pueda ser recuperada de formar automática o manual.
Para los soportes de información se tendrá en cuenta que:

- Las personas usuarias solamente podrán utilizar medios de almacenamiento autorizados o proporcionados por ANIMSA, los cuales cumplirán las normas de seguridad de la organización.
- Con carácter general, no está permitido el uso de soportes o medios de almacenamiento extraíbles **personales** (memorias USB, discos duros, almacenamiento en dispositivos móviles, etc.) sin autorización expresa. Para evitar su uso se podrán habilitar medidas técnicas para forzar el cumplimiento de esta política.
- Cuando se autorice su uso, los soportes extraíbles estarán destinados a un uso exclusivamente profesional, como herramienta de transporte puntual de ficheros, no como herramienta de almacenamiento habitual.
- La eliminación de cualquier soporte con información, (especialmente cuando se trate de datos de carácter personal) se debe realizar de forma controlada y segura, garantizando que la información contenida por los mismos no sea accesible o recuperable por personal no autorizado. En este sentido, el usuario deberá tener en cuenta las siguientes indicaciones:
  - Asegurarse que el contenido del soporte puede ser eliminado según las políticas de conservación de la información vigentes en cada momento.
  - Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente por la persona designada como responsable de la Información previa petición.

- En caso de duda consultar con Atención a Usuarios de ANIMSA

5.5.4. Metadatos y datos ocultos de los documentos electrónicos

Se define "metadatos y datos ocultos" como aquella información existente en los documentos electrónicos, que no son visibles con la configuración estándar o configuración por defecto de las aplicaciones informáticas utilizadas para su creación y tratamiento, siendo necesario aplicar alguna opción específica dentro de la configuración de estos para su visualización.

Cuando se generan documentos con aplicaciones de Microsoft Office (Word, Excel, PowerPoint, etc.), un documento PDF o se realiza una fotografía o vídeo, estos archivos llevan integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc.

ⓘ Todo archivo que vaya a ser publicado internamente en el Ayuntamiento, remitido electrónicamente a un tercero o publicado en Internet (página web, sede electrónica, etc…), deberá ser revisado para determinar los metadatos asociados al mismo, procediendo a su modificación o supresión, si procede, siguiendo el procedimiento establecido para ello en el Ayuntamiento.

5.6. SOPORTE PAPEL

El soporte papel no permite disponer de trazabilidad, por lo que, la información contenida en este soporte, que se encuentra en mesas, cajones o estanterías, se encuentra especialmente expuesta. En consecuencia, se deberá evitar en la medida de lo posible trabajar con documentación en papel.

Cuando los documentos en soporte papel 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.

Para evitar posibles incidencias, se cumplirán las siguientes medidas:

ⓘ Los puestos de trabajo permanecerán despejados, limpios y ordenados, con los materiales y recursos imprescindibles para realizar las tareas oportunas que se lleven a cabo en cada momento, así como cuidar que no queden a la vista de personas no autorizadas, anotaciones o post-it sobre la mesa o la pantalla que puedan contener información de interés.

ⓘ Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en las mesas de trabajo, mostradores u otro mobiliario.

- ⓘ En el momento que un recurso, material o información ha dejado de utilizarse para la tarea que se está realizando, se retirará a otro lugar, de forma que quede cerrado con llave u otro mecanismo similar que evite accesos no autorizados, pérdida, robo o fuga de la información. En especial, se guardarán en un lugar seguro todos los soportes o documentos que contengan información de carácter personal cuando éstos no sean usados, particularmente, fuera de la jornada de trabajo.
- ⓘ La información en papel que ya no sea de utilidad, se depositará en los contenedores especialmente dispuestos al efecto (respetando la normativa de Archivo municipal). No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores estándar, de modo que la información pueda ser legible o fácilmente recuperable.
- ⓘ Cuando se impriman documentos, estos deberán permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.
- ⓘ Se definirá la impresión a doble cara por defecto y se deberá imprimir sólo en los casos que sea necesario, siendo preferible trabajar en formato electrónico.
- ⓘ La impresión de información de carácter personal deberá realizarse, siempre que sea posible, en impresoras asignadas a la persona o personas dedicadas a generar dichos documentos y ubicadas en áreas protegidas frente a accesos indebidos.
- ✗ Nunca se dejará información y soportes que contengan información sensible a la vista sin ningún tipo de seguridad.

5.6.1. Sobre almacenamiento y custodia de papel

- ⓘ Al finalizar la jornada de trabajo, toda la documentación e información, permanecerán en los armarios, cajones y salas disponibles para garantizar la seguridad de éstos mientras se esté fuera del horario laboral.
- ⓘ En caso de disponer de un despacho, cerrar la puerta, al término de la jornada de trabajo o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
- ⓘ Se mantendrán 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 información especialmente si se trata de datos de carácter personal.
- ⓘ Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo del Ayuntamiento de Pamplona. Dichos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información.

5.6.2. Traslado de documentación en papel

- En los procesos de traslado de 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 hubiere datos de carácter personal.
- En caso de cambiar de dependencia, el proceso de traslado de los documentos en soporte papel se deberá realizar con el debido orden. Asimismo, se procurará mantener fuera del alcance de la vista de cualquier persona de la Entidad aquellos documentos o soportes en papel donde consten datos de carácter personal.
- Si se envían a terceros ajenos a la Entidad categorías especiales de datos o datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial, étnico, etc.) contenidos en soporte 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. Su envío debe estar autorizado por la persona Responsable de la Información (o, en su caso, de la persona Responsable funcional del Tratamiento).

5.6.3. Incidencias relacionadas con documentación en papel

- Se comunicarán con la mayor diligencia posible las incidencias de seguridad de las que se tenga conocimiento a través de Atención a Usuarios de ANIMSA.
- Las incidencias que puedan afectar a la seguridad de los datos de carácter personal deberán ser comunicadas al Comité Delegado de Protección de datos a través de la dirección protecciondedatos@pamplona.es
- Entre otros, tienen la consideración de incidencia de seguridad, que afecta a los ficheros en papel, los sucesos siguientes:
  - Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal.
  - Uso indebido de las llaves de acceso.
  - Acceso no autorizado del personal a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal.
  - Pérdida de soportes o documentos en papel, con datos de carácter personal.
  - Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal.

5.6.4. Digitalización de documentos

- Con carácter general, cuando se digitalicen documentos la persona usuaria deberá ser especialmente cuidadosa con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.
- Una vez finalizado el proceso de digitalización, no olvidar tomar los originales del escáner.
- Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, quien lo encuentre intentará localizar a la persona que lo escaneó para que ésta la recoja inmediatamente. En caso de no localizar la persona propietaria, destruir la documentación en los contenedores establecidos al efecto.

5.7. BLOQUEO DE PUESTOS DE TRABAJO

Todas las personas usuarias que, por cualquier motivo se deban ausentar momentáneamente o deban descuidar el puesto de trabajo, deben concienciarse de la necesidad de mantener la seguridad de sus sistemas o dispositivos de trabajo y seguirán las siguientes directrices:

- Siempre que se abandone el sistema o dispositivo es obligatorio bloquearlo (en el sistema Windows se hará pulsando a la vez las teclas ***Windows + L*** o ***Ctrl + Alt + Supr***).
- Cuando se deje de utilizar una aplicación se cerrará la sesión, evitando de este modo el consumo de recursos y protegiendo el acceso a los datos de la misma.
- Al finalizar la jornada laboral deben finalizarse todas las sesiones activas y apagar el equipo. Esta medida será de aplicación sólo a dispositivos de los que no se requiera su funcionamiento continuo como componentes de algún sistema / servicio que exija continuidad o no se requiera de su acceso remoto.
- Al menos una vez al día se deberá reiniciar el equipo para que se efectúen las instalaciones necesarias del sistema.

Para evitar la utilización de sesiones abiertas por personas no autorizadas, se establecen las siguientes medidas corporativas:

- El bloqueo automático del sistema o dispositivo tras un periodo de inactividad quedará establecido en 15 minutos con carácter general, y sin perjuicio del establecimiento de tiempos menores, si la aplicación o la tipología de los datos tratados así lo aconsejan. Se deberá tener especial consideración con los sistemas críticos de la Entidad como son, por ejemplo, los servidores. Toda sesión activa en un sistema o dispositivo será cancelada tras 45 minutos de inactividad con carácter general, y sin perjuicio del establecimiento de tiempos de menor o mayor duración, si la

aplicación o el nivel de seguridad de los datos tratados así lo aconsejan.

- Los periodos de inactividad especificados en los puntos anteriores deberán ser implantados a través de políticas impidiendo de este modo cualquier modificación por parte de la persona usuaria.
- Para acceder a un equipo o dispositivo que ha sido bloqueado por inactividad se requerirá la autenticación de la persona usuaria.

5.8. USO DE LA RED CORPORATIVA

La **red corporativa** sirve para el acceso del personal de la Entidad a la información de las aplicaciones informáticas, para el acceso a los repositorios de archivos corporativos, para la comunicación de datos entre los distintos equipos y dispositivos y para el acceso a Internet.

Es, por tanto, un recurso compartido y limitado, en el que la forma de utilización por parte de cada persona usuaria, afecta al resto.

Por otro lado, es un recurso sensible que debe ser protegido, ya que una incidencia en la red puede dejar sin poder trabajar a todo el personal de la Entidad, a la ciudadanía que realiza gestiones online a través de la Sede Electrónica, o a otras organizaciones que tengan autorizado el acceso a información a través de sistemas de interoperabilidad. Además, puede ser un medio por el que se puedan atacar el resto de recursos, dando lugar a ciberincidentes de amplio impacto.

Por todo ello, se establecen las siguientes medidas para el uso de la red corporativa:

- Se monitorizará el tráfico de red y se podrán implementar medidas de control del tráfico y/o filtrado de contenidos en cualquier momento y sin previo aviso, previa aprobación de la persona designada como Responsable de Seguridad.
- En caso de que una persona usuaria considere necesario acceder a alguna dirección incluida en una de las categorías filtradas, se pondrá en contacto con su responsable directo para que gestione las solicitudes de acceso correspondiente.
- Como parte de la monitorización de la red corporativa, se monitorizará el tráfico y acceso desde/hacia internet por parte de los equipos y dispositivos conectados a la red corporativa.

5.8.1. Utilización de internet

Con carácter general, el personal de la Entidad dispone 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 gestionada por 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.

Por lo tanto, se establecen las siguientes normas de uso:

- La utilización de Internet por parte de las Personas usuarias autorizadas debe limitarse a la obtención de información relacionada con el trabajo que se desempeña y en un ámbito absolutamente profesional. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.
- Cada persona es responsable del uso que realice al conectar a Internet y del acceso a los diferentes contenidos que obtenga a través de los recursos y servicios de la Entidad.
- El sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.
- El sistema que proporciona el servicio de navegación a Internet podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino.
- Dado que la organización podrá monitorizar y registrar los accesos realizados desde los dispositivos conectados a la red corporativa, en caso de que una persona usuaria considere necesario acceder a alguna dirección incluida en una de las categorías filtradas, se pondrá en contacto con su responsable para que éste gestione el acceso correspondiente.
- Las personas usuarias son las únicas 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.

ⓘ Cualquier incidente de seguridad relacionado con la navegación por Internet, deberá ser comunicado sin demora a Atención a Usuarios de ANIMSA.

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 de la persona Responsable de la Seguridad.

✗ Sólo se podrá acceder a Internet mediante alguno de los navegadores suministrados y configurados por ANIMSA en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización de dicho Servicio

✗ 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. Las personas usuarias 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 Organización 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.

✗ El uso de chats o programas de conversación en tiempo real no autorizados, no está permitido.

✗ Se prohíbe el uso de programas de compartición de contenidos, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.

✗ La descarga de software ejecutable desde Internet, no está permitida.

5.8.2. Higiene en la navegación web

A efectos de preservar la privacidad y reforzar la seguridad durante la navegación web, se deberá tener en cuenta que:

- Durante la navegación por Internet a través de navegadores, se recogen datos que son almacenados en los equipos y dispositivos, y que pueden suponer un riesgo para la privacidad.
  - Las cookies son ficheros que permiten funcionalidades técnicas, de seguridad y, en su caso, de operatividad, permitiendo que los sitios web reconozcan particularidades y preferencias de la persona usuaria, así como su comportamiento.
  - La memoria caché almacena datos de los sitios visitados para permitir una navegación más eficiente y rápida. Parte de esta información puede ocupar un volumen significativo de almacenamiento.
- En ambos casos, la información procesada incluye elementos personales y privados que pueden resultar de utilidad para ataques de terceros, permitiendo que conozcan datos como credenciales, localizaciones o hábitos, por lo que las personas usuarias deberán proceder al borrado periódico de la siguiente información de los navegadores que utilicen:
  - Historial de navegación y de descargas.
  - Memoria caché del navegador.
  - Cookies y otros datos del sitio.
- Asimismo, para evitar que terceros no autorizados puedan acceder a información sensible, se deberá proceder al borrado de:
  - Autorrelleno de formularios.
  - Permisos del sitio.
  - Contraseñas.
  - Configuraciones y permisos de sitios web.
- El Ayuntamiento de Pamplona podrá implantar herramientas de limpieza e higiene de la navegación cuando resulte viable y oportuna su automatización, garantizando en todos los casos la privacidad y confidencialidad en el proceso de borrado.

5.9. CORREO ELECTRÓNICO

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición del personal 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.

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.

La Entidad, consciente de los problemas de seguridad y responsabilidad legal que ocasiona el uso del correo electrónico, dispone las siguientes normas:

- ⓘ El correo electrónico corporativo se considera una herramienta de trabajo básica, por lo que se debe emplear en base al "sentido común" y teniendo en cuenta la responsabilidad del servicio, tratando en cualquier caso de no poner en compromiso ni los sistemas ni la imagen de la Organización. No se utilizará la herramienta de correo electrónico con fines ajenos al propio desarrollo de las actividades que cada persona usuaria tiene encomendadas en la Entidad.
- ⓘ El acceso al correo se realizará mediante usuario y contraseña. Dicha identificación deberá seguir las mismas directrices que las planteadas para el acceso al sistema y las aplicaciones.
- ⓘ Las cuentas de correo corporativas 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.
- ⓘ Las personas usuarias serán responsables de todas las actividades realizadas con las cuentas de correo y sus respectivos buzones provistos por la Entidad.
- ⓘ La utilización del correo electrónico por personal externo requiere la previa autorización por escrito.
- ⓘ La Entidad se reserva el derecho de revisar y controlar el uso correcto del correo electrónico corporativo.
- ⓘ Cuando sea necesario acceder a la carpeta personal y/o cuenta de correo corporativa de la persona usuaria, esta se deberá realizar contando con la autorización expresa de la persona titular de las mismas y solo podrá ser realizado por el Responsable del/de la usuario/a o por la persona en que éste delegue.
- ⓘ La Entidad se reserva 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.
- ✗ Está **terminantemente prohibido** falsificar, ocultar, suprimir o sustituir la identidad del emisor en cualquier correo electrónico y leer correos ajenos, sin autorización previa.
- ⓘ El Ayuntamiento de Pamplona y ANIMSA quedarán facultados para filtrar el contenido del correo electrónico de la cuenta de correo proporcionada por ANIMSA a los empleados para el desarrollo de sus funciones laborales, al objeto de prevenir virus o en el supuesto de que existan razones fundamentadas en una firme sospecha sobre la existencia de actividades delictivas o dolosas del trabajador.

- El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa.
- Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

5.9.1. Envío y recepción de correos.

- Las personas usuarias deberán ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por el Ayuntamiento de Pamplona. Es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios y siempre y cuando el fin último sea el cumplimiento de las funciones laborales.
- Todos los correos salientes deberán incluir el modelo de firma establecida en la imagen corporativa del Ayuntamiento de Pamplona.
- La forma y contenidos de los correos enviados por los usuarios estarán alineados con las normas éticas y de cortesía marcadas por la Entidad, y en ningún caso se enviarán correos ofensivos, amenazantes o de mal gusto.
- Antes del envío de un mensaje se debe revisar la barra de direcciones. El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información.
- Los envíos masivos de información, así como lo correos que se destinen a gran número de personas, serán los estrictamente necesarios, para impedir un colapso del sistema de correo.
- En el caso de se requiera enviar un mensaje de correo electrónico a varias personas (especialmente en el envío de correos masivos), se utilizará el **campo CCO (copia oculta)** para introducir las diferentes direcciones de correo, con excepción de aquellos mensajes en los que necesariamente se requiera la identificación de las personas destinatarias para confirmar que han sido informadas.
- ✗ No enviar mensajes en cadena. Las alarmas de virus y las cadenas de mensajes son, en muchas ocasiones, correos simulados, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus, se debe proceder a su borrado inmediatamente.
- ✗ No responder a mensajes de Spam.
- Asegurar la identidad del remitente antes de abrir un mensaje. Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) de la persona atacada.

ⓘ 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.), por ello, los archivos adjuntos recibidos serán analizados por las herramientas antivirus antes de ser abiertos o ejecutados. Los correos sospechosos o de dudosa procedencia podrán no ser entregados a sus destinos.

✗ No abrir correos basura ni correos sospechosos. Es conveniente borrar los correos sospechosos o, al menos, situarlos (sin abrir) en una zona de cuarentena.

ⓘ 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.

5.9.2. Almacenamiento de correos

ⓘ Los usuarios deben 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.

✗ No utilizar el correo electrónico como espacio de almacenamiento. La capacidad del servicio de correo de la Organización es limitada. Cuando una cuenta se satura puede ser que se restrinjan por parte del servidor los privilegios de envío y/o recepción de mensajes o que se realice un borrado, más o menos selectivo, de los mensajes almacenados. Por todo ello, se recomienda conservar únicamente los mensajes imprescindibles y revisar periódicamente aquellos que hubieren quedado obsoletos.

5.9.3. Utilización del correo

ⓘ Se podrá acceder al correo corporativo municipal con el **acceso remoto (vía web)**. En dichos accesos se recomienda adoptar las siguientes cautelas:

- 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.

ⓘ El acceso a cuentas de correo personales/gratuitas (gmail, yahoo, hotmail, etc.) desde los equipos (fijos o móviles) puestos a disposición de los usuarios, supone una amenaza a la seguridad, por lo que no se deberá acceder a ellas desde los sistemas de información municipales.

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 o por el sistema automático de distribución de software oficial.

✗ 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 los usuarios de la Entidad, fuera de los límites laborales establecidos por la misma.

✗ No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia. Se recomienda su eliminación inmediata.

✗ 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 funcional del tratamiento.

5.10. TELETRABAJO

Se considerará teletrabajo el acceso desde el exterior a recursos internos de la organización con el objeto de realización de tareas propias del puesto de trabajo. En estos casos, se deberán seguir las siguientes normas:

- **Conexión:** Para el acceso a los servicios de la organización, se deberán utilizar exclusivamente los medios ofrecidos por ANIMSA.
- **Seguridad durante la conexión:** Cada trabajador deberá evaluar la seguridad de la ubicación desde la que accede a los servicios de teletrabajo para evitar factores de riesgo como robos, accesos no autorizados e interceptación de la comunicación y/o de la información.
- **Desconexión:** Una vez finalizada la sesión, realizar la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada

5.11. CONFIDENCIALIDAD, PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO

La información contenida en los Sistemas de Información del Ayuntamiento de Pamplona es propiedad de dicho organismo, por lo que las personas usuarias deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa de la propia Institución. Además, se deberá tener en cuenta las siguientes premisas:

- Todo el personal de la organización o ajeno a la misma que, por razón de su actividad profesional, hubiera tenido acceso a información gestionada por la organización (documentos, metodologías, claves, análisis, programas, etc.) deberá mantener sobre ella, por tiempo indefinido, una absoluta reserva.
- Toda persona usuaria que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligada a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Entidad.
- Toda la información contenida en los Sistemas de Información de la Entidad o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas. La información que comprenda datos de carácter personal está protegida por la normativa vigente en materia de Protección de Datos.
- Las personas usuarias sólo podrán acceder a aquella información para la que posean las debidas y explícitas autorizaciones, en función de las labores que desempeñen, no pudiendo en ningún caso acceder a

información perteneciente a otras personas usuarias o grupos para los que no se posea tal autorización.

- Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base a los principios de "mínimo privilegio posible y necesidad de conocer".
- La salida de soportes fuera de los locales de la Entidad que contengan datos de carácter especial, debe ser expresamente autorizada por la persona Responsable funcional del Tratamiento). Toda salida de soportes deberá además quedar registrada. La entrada de soportes que contengan datos personales deberá quedar registrada. Asimismo, el soporte deberá ser dado de alta en el inventario de soportes de acuerdo con el procedimiento establecido en la Entidad.
- 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. Asimismo, el soporte deberá ser dato de baja del correspondiente inventario.
- La persona usuaria mantendrá la confidencialidad de la información a la que tenga acceso por motivos del desempeño de su puesto de trabajo, incluso una vez finalizada la relación laboral. Toda la información sensible a la que se tenga acceso será utilizada previa autorización y dentro de las actividades de trabajo previstas. La utilización de dicha información, fuera de este ámbito es una operación ilegal que puede dar lugar a responsabilidades no sólo disciplinarias sino también judiciales. Las personas que intervengan en tratamientos de datos e información sensible están obligadas al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones laborales con la organización.
- La persona usuaria será responsable de toda aquella información que almacene en su equipo personal o de forma externa a la infraestructura de la organización, ya que estos no están sujetos a la política de copias.

Queda prohibido, asimismo:

- ✗ El uso de unidades externas de almacenamiento de la información para uso privado, tales como: pendrives, discos duros externos, CD-R, DVD-R, etc.

- ✗ Transmitir o alojar información con datos de carácter personal en servidores externos a la Entidad salvo autorización expresa. Para ello se deberá proceder a su análisis por parte del Comité Delegado de Protección de Datos, al objeto de comprobar la inexistencia de trabas legales para ello y se verificará la suscripción de un contrato expreso entre la Organización y la empresa responsable de la prestación del servicio, incluyendo los Acuerdos de Nivel de Servicio que procedan, el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.
- ✗ Transmitir o alojar información con datos de carácter personal propiedad de EELL cliente, en servidores externos a la misma, salvo autorización expresa.

5.12. PROPIEDAD INTELECTUAL

Respecto a derechos de **Propiedad intelectual** se prohíben expresamente las siguientes actuaciones:

- ✗ Está estrictamente prohibida la ejecución de programas informáticos sin la correspondiente licencia de uso.
- ✗ Los programas informáticos están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, salvo que los términos de su licencia de uso lo permitan expresamente, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación,
- ✗ Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, a la que se tenga acceso utilizando medios electrónicos proporcionados por el Ayuntamiento de Pamplona, sin la debida autorización.

5.13. COMUNICACIÓN DE INCIDENCIAS

Cuando un usuario detecte cualquier anomalía (mal funcionamiento, aplicaciones que no arrancan o que se cierran de manera inesperada, pérdida de documentos, de memorias USB, etc.) o incidente de seguridad (virus, suplantación de identidad, pérdidas de clave, etc.) que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información del Ayuntamiento de Pamplona, deberá comunicarse con la mayor diligencia posible a través del **Departamento de Atención a Usuarios de ANIMSA.**

6. ACCESO Y PERMANENCIA EN DEPENDENCIAS DE ACCESO RESTRINGIDO

6.1. Zonas de acceso restringido

Se consideran zonas de acceso restringido las siguientes:

- **CPDs:** salas donde se ubican los servidores TIC y los locales

de las centrales telefónicas.

- **Cuartos Técnicos de Telecomunicaciones:** salas donde se ubican los racks de telecomunicaciones del edificio y/o la central telefónica.

Se consideran diferentes tipos de perfiles de acceso:

- **Acceso permanente:** personal que realiza tareas habituales en las salas de operación y en los CPDs, y que dispone de mecanismo de acceso asignado a su nombre, personal e intransferible. Aunque el acceso sea permanente podrían existir limitaciones horarias en función del grupo al que pertenezcan.
- **Acceso ocasional (temporal):** personal interno o externo de ANIMSA que debe realizar tareas ocasionales durante un periodo de tiempo definido, y a los que se debe proveer de autorización temporal.

El Responsable de Seguridad o las personas en quien delegue aprobarán los accesos a las zonas o dependencias de acceso restringido.

En cada área restringida habrá al menos, una persona encargada del control y registro de los accesos por parte de las personas con perfil de acceso ocasional. Estas personas se encargarán de la identificación y registro del acceso por parte del personal externo autorizado a ello.

Los cuartos técnicos estarán siempre cerrados bajo llave o con cerradura electrónica. Sólo podrán acceder a los cuartos técnicos los administradores de sistemas de información y proveedores de servicio debidamente autorizados.

6.2. Acceso físico

El acceso físico a las zonas de acceso restringido seguirá lo establecido en las políticas de acceso de ANIMSA

- El personal ajeno que temporalmente deba acceder a los edificios, instalaciones o dependencias de la Organización, deberá hacerlo siempre bajo la supervisión de algún miembro de la misma.
- Se identificará a las personas externas que accedan a las dependencias de ANIMSA, se registrará su acceso y se les entregará una tarjeta de identificación que deberán llevar en lugar visible hasta su salida.
- Una vez en el interior, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común (aula, aseos, salas de reuniones, etc.).

6.3. Acceso lógico de terceros a los sistemas de información

- Para los accesos lógicos de terceros (incluido el acceso remoto)

al sistema de información del Ayuntamiento de Pamplona, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo.

ⓘ Si de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas utilizadas. Estas peticiones deberán dirigirse al Departamento de Sistemas, a través de la herramienta HelpDesk (HDK) por parte del responsable del departamento para el que realicen los trabajos correspondientes.

7. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

El Ayuntamiento de Pamplona se asegurará de que, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente se:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

Esta supervisión se realizará en todo caso **con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, laboral, y demás disposiciones que resulten de aplicación,** se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Los datos serán conservados durante el tiempo que sea necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. La legitimación para el tratamiento es un cumplimiento de las obligaciones establecidas en la normativa que regula la relación entre los usuarios y la entidad. Los datos serán tratados de manera confidencial y solo serán cedidos a otras entidades cuando se cumplan las exigencias establecidas en la legislación vigente de Protección de Datos.

Cualquier interesado podrá ejercitar sus derechos, mediante comunicación dirigida a protecciondedatos@pamplona.es según lo recogido en la Política de Privacidad.

De igual modo cuando lo considere pertinente, podrá acudir a la Agencia Española de Protección de Datos (AEPD).

Se llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegitimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.

En caso de que existieran indicios de que se está llevando a cabo una utilización indebida, La Entidad se reserva el derecho de revisar y auditar la información existente en dichos recursos informáticos y el uso de las aplicaciones, de Internet, del correo electrónico corporativo y del teléfono corporativo que esté haciendo cada persona. Dicho control patronal se realizará respetando los principios rectores de necesidad, idoneidad y proporcionalidad, siendo las medidas de fiscalización las necesarias, adecuadas y las menos invasivas de todas las que sean plausibles.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

El Comité de seguridad velará por el cumplimiento de la presente Normativa e informará sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

8. ACCESO A LA NORMATIVA, COMPROMISO DE CUMPLIMIENTO Y PROCESO DISCIPLINARIO

TODAS las personas usuarias de los sistemas de información y de los recursos informáticos de la Entidad están **obligadas** a cumplir lo prescrito en la presente normativa.

Para ello se les dará acceso a la presente Normativa de uso Sistemas de Información, durante el tiempo de desempeño de sus funciones y se realizarán las acciones oportunas para informar a cada empleado y empleada de las normas y condiciones de uso de los medios electrónicos y sistemas de información puestos a su disposición. De esta forma, la persona usuaria quedará informada previamente de la existencia de esta normativa que limita el uso de los sistemas de información para tareas profesionales y 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.

Esta normativa se proporcionará no solo al personal directamente empleado por la Entidad sino también a cualquier otro personal subcontratado por un tercero o cualquier usuario que deba acceder a

los sistemas de información de la Entidad para la prestación de los servicios contratados.

Cualquier incumplimiento de lo indicado en la presente normativa, ya sea de forma intencionada o por un comportamiento negligente, puede dar lugar a la suspensión temporal o definitiva del uso de los recursos y servicios asignados a la persona, sin perjuicio de la revisión de los hechos concretos en el ámbito de la normativa disciplinaria en el caso del personal público y, de manera general, de las responsabilidades a que, en su caso, hubiere lugar en materia administrativa, civil o penal.