NOR003 - MEDIDAS DE SEGURIDAD APLICADAS AL TRATAMIENTO DE DATOS PERSONALES

Clasificación de la Información:

Nivel del Documento	Normativa
Nombre del Fichero	NOR003 - Medidas de seguridad aplicadas al tratamiento de datos personales.docx
Tipo	Difusión limitada
Ámbito de Difusión	Comité de Seguridad del AYUNTAMIENTO DE PAIPORTA
Responsable	Responsable de Seguridad del AYUNTAMIENTO DE PAIPORTA

CONTROL DE FIRMAS

	FECHA	FIRMA
ELABORADO POR MARIA SANCHIS	20/05/2019	
APROBADO POR COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	20/05/2019	

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	11/03/2022	María Sanchis	Versión inicial del documento.
2.0	16/09/2024	María Sanchis	Actualización del apartado 5.

ÍNDICE

1. OBJETO DEL DOCUMENTO

Es objeto del presente documento informar al personal de las medidas de seguridad, tanto técnicas como organizatias, que aplican en la organización y cuyo fn es asegurar la confdencialidad, integridad y disponibilidad de los datos personales, todo ello, de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relatio a la protección de las personas fsicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garanta de los derechos digitales.

2. ÁMBITO DE APLICACIÓN

El presente documento es de aplicación tanto a las actiidades de tratamiento como a los fcheros que contenen datos de carácter personal que se hallan bajo la responsabilidad del Responsable del Tratamiento, tanto cuando actúa como tal o como Encargado/a del Tratamiento; incluyendo los sistemas de información, comunicación, soportes, equipos y resto de recursos empleados, entre los cuales queda incluido el personal, para el tratamiento de datos de carácter personal.

3. RECURSOS PROTEGIDOS

Los recursos que quedan protegidos son:

- Los centros de tratamiento y locales donde se encuentren ubicados los fcheros o se almacenen los soportes que los contengan.
- Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso a datos personales.
- Los seriidores y el entorno del sistema operatio y de comunicaciones en el que se encuentran ubicados los fcheros que contenen datos personales.
- Los sistemas informátcos y/o aplicaciones establecidos para realizar el tratamiento de los datos personales.
- Cualquier otro recurso que, sin estar aquí indiiidualizado, se utlice para tratar datos personales.

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Se informa al personal trabajador que:

- Sólo puede utlizar los datos personales objeto de tratamiento, o los que recojan para su inclusión, exclusiiamente, para las fnalidades que le haya indicado expresamente el Responsable del Tratamiento. En ningún caso podrá utlizar los datos para fnes propios o de terceros ajenos al Ayuntamiento.
- Siempre deberá tratar los datos personales de acuerdo con las instrucciones del Responsable del Tratamiento.
- No comunicará los datos a terceras personas, salio que cuente con la autorización expresa del Responsable del Tratamiento, en los supuestos legalmente admisibles.
- Debe mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en iirtud del desarrollo de sus funciones o tareas laborales, incluso después de que fnalice su objeto.
- Si fuera conocedor/a de alguna incidencia, deberá notfcarla inmediatamente a la persona Responsable del Tratamiento, a la persona Delegada de Protección de Datos o bien a la persona que indique el/la Responsable del Tratamiento.
- Debe garantzar y respetar la confdencialidad de los datos personales a los que tenga acceso, así como mantener el compromiso de cumplir con las medidas de seguridad correspondientes y que constan descritas en el presente documento, de las que ha sido informado/a convenientemente.

5. NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

La persona Responsable del Tratamiento ha establecido las siguientes normas y procedimientos de seguridad, de obligado cumplimiento, por parte de todo el personal:

5.1 Uso adecuado de los recursos de la organización referentes a:

5.1.1 Dispositios tecnológicos que el Responsable del Tratamiento pone a disposición del personal.

Las tablets, ordenadores de sobremesa, portátles, discos duros externos, móiiles, teléfonos inteligentes comocualquier otro dispositio que siria para el tratamiento, transporte y/o almacenaje de información que el Responsable del Tratamiento ponga a disposición del personal para realizar su trabajo, deberán ser custodiados por la persona al cual se haya asignado, debiendo dicha persona cumplir con todas las medidas de seguridad que iengan impuestas por el Ayuntamiento.

Dichos dispositios no podrán emplearse con fnes ajenos a la actiidad laboral. Si el trabajador o la trabajadora necesitan utlizarlo con fnes ajenos a la actiidad laboral, deberán contar con la autorización preiia y por escrito de la organización.

Cuando se utlicen los equipos fuera del centro de trabajo, queda prohibido conectarse a redes WiFi públicas o de acceso gratuito y dejar el equipo desprotegido, debiendo en todo momento estar pendiente del mismo.

5.1.2 Internet y redes WIFI.

Todo el personal debe procurar un uso seguro y legal, tanto de Internet como de las redes WiFi de la organización, por lo cual, bajo ningún pretexto podrán:

- Acceder a páginas web que supongan una actiidad ilegal, o de contenido no relacionado con el trabajo, así como también el acceso a páginas de dudosa procedencia.
- Transmitr, iisualizar, editar, copiar, compartr, descargar y/o manipular de cualquier forma, material ilegal, como por ejemplo: pornografa (de cualquier tpo); material amenazante, fraudulento, discriminatorio, difamatorio, ofensiio, obsceno, insultante o contrario a la moral y las buenas costumbres.
- Transmitr, iisualizar, editar, copiar, compartr, descargar y/o manipular de cualquier forma material de cualquier tpo que esté protegido por el secreto comercial o por patentes iigentes.
- Transmitr, iisualizar, editar, copiar, compartr, descargar y/o manipular de cualquier forma cualquier archiio de tpo musical, de lectura o flmográfco, sin tener los derechos de propiedad intelectual correspondientes.
- Escanear o probar la iulnerabilidad de equipos, sistemas o segmentos de red.
- Eniiar mensajes no solicitados, cualquier tpo de iirus, código malicioso o ataques internos o externos a la red.
- Dañar de cualquier forma equipos, sistemas informátcos o redes y/o perturbar el normal funcionamiento de la red, tanto de la organización como de terceros.
- Interceptar, recopilar o almacenar datos sobre terceros/as que no estén relacionados con la actiidad laboral y sin su conocimiento y consentmiento expreso.
- Obtener acceso no autorizado a equipos, sistemas o programas tanto dentro como fuera de la red.
- Conectarse a la red reseriada para personas iniitadas.
- Conectarse a redes públicas.
- Realizar cualquier otro tpo de acción, tanto de forma directa como indirecta, que ponga en riesgo la disponibilidad, integridad y/o confdencialidad de la información, como la seguridad e integridad de los sistemas que utliza la organización.

5.1.3 Terminales y líneas telefónicas.

Los terminales, tanto fjos como móiiles, tarjetas SIM y líneas telefónicas contratadas, no pueden utlizarse para fnes ajenos a los relacionados con la actiidad laboral que el personal desempeña para el Responsable del Tratamiento.

Solamente podrán utlizarse para fnes personales, los equipos señalados, en caso de emergencia familiar, aunque en ningún caso podrán almacenarse en los mismos datos personales que puedan indiiidualizar a una persona.

Queda también prohibido la manipulación de los terminales para lograr priiilegios superiores a los otorgados por la organización, grabar llamadas, duplicar tarjetas SIM y en general cualquier actiidad contraria.

Respecto de la instalación de aplicaciones, deberá cumplir con lo indicado en el punto 5.5 del presente documento.

5.1.4 Correo electrónico.

Ud. es la principal persona responsable del correcto uso de la cuenta de correo electrónico profesional que se le asigna, por lo cual deberá cumplir con las siguientes obligaciones:

- Está prohibido el eniío de correos electrónicos con en el que se adjunten bases de datos personales o bien se copie el contenido de las mismas dentro del cuerpo del correo electrónico. Si, por razones del trabajo que se desarrolla, debe eniiarse este tpo de información, la misma deberá eniiarse únicamente mediante un archiio adjunto y dicho archiio deberá estar cifrado, la claie, en ningún caso se transmitrá por correo electrónico.
- Está prohibido eniiar o reeniiar mensajes en cadena o con fnes comerciales o publicitarios sin el consentmiento expreso de la persona destnataria.
- Está prohibido permitr el acceso al contenido de su cuenta de correo electrónico profesional a cualquier persona, ya sea personal interno como externo de la organización; sólo podrán tener acceso a su contenido a quien la dirección indique y por razón fundada.
- Respecto de la contraseña, deberá cumplir con lo indicado en el apartado 5.4 del presente documento.
- No podrá utlizar su cuenta de correo personal, bajo ningún pretexto, para la realización de la actiidad laboral.
- El correo electrónico corporatio solo podrá ser utlizado para los fnes correspondientes a la actiidad laboral y en ningún momento con fnes propios o priiados quedando totalmente prohibido el eniío o la recepción de correos ajenos a las funciones laborales con contenido personal.
- Se adiierte que para el eniío de un correo electrónico a iarias personas, se debe utlizar la casilla CCO (con copia oculta) ya que en caso contrario se podría entender que se iulnera el deber de secreto.

En todo caso, se informa al personal empleado de que el Ayuntamiento podrá acceder al correo en caso de considerarlo necesario.

5.2 Polítca de escritorios limpios.

Si no te encuentras en tu puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, que contengan información que puedan contener datos personales, deben ser retrados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para eiitar el acceso no autorizado a los mismos.

Este tpo de documentos y soportes deben ser archiiados de forma segura.

Tu puesto de trabajo debe estar limpio y ordenado; podrás disponer únicamente de los actios que hemos puesto a tu disposición.

No podrás tener recipientes ni eniases sobre tu mesa de trabajo, cuyo cierre no sea hermétco y que contengan líquidos, con el fn de eiitar su iertdo encima de los equipos informátcos y/o cualquier otro tpo de soporte que pueda ierse afectado por el iertdo.

5.3 Polítca de pantallas limpias.

La ubicación de los puestos de trabajo y la colocación de las pantallas está organizada de tal forma que sólo la persona que utliza la misma puede leer lo que se plasma en la pantalla, eiitando miradas indiscretas.

Si la persona autorizada no se encuentra en su puesto de trabajo, debe quitar toda la información sensible de la pantalla y bloquear el acceso a todos los sistemas para los cuales la persona tene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la polítca de pantalla limpia se implementa fnalizando la sesión

en todos los sistemas o bloqueando la pantalla mediante el uso de la siguiente combinación de teclas:

Botón Windows + L

()

Si la persona se ausenta por un período más prolongado (superior a 2 horas o más), la polítca de pantalla limpia se implementa fnalizando la sesión en todos los sistemas y apagando el ordenador.

5.4 Polítca de contraseñas.

El personal tene prohibido diiulgar, compartr y/o entregar, tanto a personal interno como externo de la organización, las contraseñas que tengan para acceder tanto a los sistemas informátcos, programas, como a las Bases de Datos que contengan datos de carácter personal.

Al momento de crear la contraseña, deberá tener en cuenta lo siguiente:

- La contraseña deberá tener, al menos, 6 caracteres.
- Deberán combinarse letras mayúsculas y minúsculas, números y símbolos.
- No podrá utlizar la misma contraseña en diferentes seriicios.
- No podrá utlizar aquellas contraseñas que utlice en su iida priiada, por ejemplo, la de acceso al banco, a su cuenta de red social, etc.
- No podrá reutlizar contraseñas que ya haya utlizado preiiamente.
- No podrá utlizar patrones de teclado, por ejemplo: “qwerty” o “uiop” o “1qaz” “2wsx” o “3edc” ni la combinación de estas.
- Las contraseñas tenen un período de iigencia de 3 meses.
- Una iez creada la contraseña, deberá asegurar su correcta gestón y almacenamiento, por lo cual, deberá seguir las siguientes directias:
- No apuntar la contraseña en notas y pegarlas en el escritorio, pantalla u ordenador.
- No utlizar la opción de “recordar contraseña” que ofrecen los naiegadores.
- No almacenar la contraseña, dentro de su ordenador, en archiios sin cifrar y que estén a la iista de cualquier usuario y que lleien nombres que permita su fácil identfcación, por ejemplo: “listado de contraseñas”, “contraseñas”, “pass”, “password”, etc.

5.5 Sobre la instalación por parte del personal laboral de programas por cuenta propia.

El personal no puede instalar ningún tpo de sofware por cuenta propia sin la autorización preiia y por escrito del Responsable del Tratamiento.

En el caso que la persona trabajadora proceda sin autorización ni conocimiento por parte de la organización de la persona Responsable del Tratamiento, quedará iinculada y será responsable en caso de daños ocasionados al equipo informátco y/o a la información en él contenida como consecuencia de dicha instalación.

Antes de instalar un programa, el personal autorizado deberá comprobar que se cuenta con la licencia y derechos de uso del programa; con la certfcación del programa para su compatbilidad con el sistema operatio y los demás aplicatios; con la garanta del código para eiitar posible presencia de iirus, troyanos y otros programas espías.

En todos los casos, cualquier tpo de sofware que se instale, deberá mantenerse actualizado siguiendo las indicaciones del desarrollador del sofware en cuestón.

5.5.1 Pruebas con datos reales.

Las pruebas anteriores a la implantación y/o modifcación de los sistemas de información que traten fcheros con datos de carácter personal no se realizarán con datos reales.

En el caso de resultar necesario utlizar datos reales con el fn de poder realizar la prueba de forma positia, deberá asegurarse el niiel de seguridad correspondiente al tpo de tratamiento y a los datos de carácter personal afectados para que los mismos no sean objetos de una brecha de seguridad.

5.6 Control de accesos.

El personal sólo puede acceder a los datos y dependencias que sean necesarios para el correcto desarrollo de sus funciones.

5.6.1 Entrada y salida de las instalaciones de la organización.

Existe implantado en la organización un sistema de control de accesos cuyo objetio es la identfcación de personal, con el fn de eiitar el ingreso de personas ajenas a la organización y el registro de jornada horaria con el fn de controlar y monitorizar el fujo del personal del Ayuntamiento.

5.6.2 Despachos.

Aquellos despachos que disponen de una puerta con llaie, son sus ocupantes las personas encargadas de que permanezcan cerrados cuando fnalice la jornada laboral o se ausenten de su puesto de trabajo.

Todos los despachos que dispongan de armarios y cajoneras con llaies, siendo aquellas personas que los utlizan, las encargadas de que permanezcan cerrados cuando fnalice la jornada laboral o se ausente de su puesto de trabajo.

Es responsabilidad de quienes tengan asignadas llaies, la custodia de las mismas al igual que la comunicación de su extraiío a Responsable del Tratamiento, Delegado/a de Protección de Datos o a aquella persona que designe el/la Responsable del Tratamiento.

Queda prohibido realizar copias de las llaies al igual que distribuir las mismas sin autorización expresa de la persona Responsable del Tratamiento. Tampoco se podrá ceder o prestar las mismas a terceras personas sin autorización expresa de la persona Responsable del Tratamiento.

5.6.3 Cuarto del seriidor.

Únicamente la persona Responsable de Seguridad, el/la Delegado/a de Protección de Datos y/o el personal autorizado por la persona Responsable del Tratamiento, están autorizadas para acceder a las dependencias en las que se encuentren los sistemas de información que corresponden al seriidor y a las copias de respaldo.

El acceso se realizará por huella biométrica y en caso de fallo por una llaie maestra.

Es responsabilidad de quienes tengan asignadas llaies, la custodia de las mismas al igual que la comunicación de su extraiío la persona Responsable del Tratamiento, Delegado/a de Protección de Datos o a aquella persona que designe la persona Responsable del Tratamiento.

Queda prohibido realizar copias de las llaies al igual que distribuir las mismas sin autorización expresa de la persona Responsable del Tratamiento. Tampoco se podrá ceder o prestar las mismas a terceras personas sin autorización expresa de la persona Responsable del Tratamiento.

Es responsabilidad de quienes tengan asignadas claies de acceso, la custodia de las mismas al igual que la comunicación de su fltración a la persona Responsable del Tratamiento, Delegado/a de Protección de Datos o a aquella persona que designe el Responsable del Tratamiento.

5.7 Régimen de trabajo fuera de los locales de la organización:

El tratamiento de datos de carácter personal, fuera de los locales de la organización, deberá ser autorizado expresamente por la persona Responsable del Tratamiento, teniéndose en consideración las funciones que realiza el personal en la organización.

En el caso de que se autorice el tratamiento de datos fuera de los locales de la organización, el personal que los

trate, deberá cumplir con todas las medidas de seguridad indicadas en los puntos 5.1 y 5.3 del presente documento y con todas aquellas que establezca la organización para el caso concreto.

5.8 Copias de respaldo y recuperación.

La organización realiza copias de seguridad de forma habitual y sistemátca, por lo cual es su responsabilidad acatar las indicaciones que iengan impartdas por el departamento informátco del Ayuntamiento.

5.9 Gestón de soportes.

5.9.1 Utlización de soportes extraíbles.

Por regla general, el personal no podrá disponer fuera del Ayuntamiento de ningún soporte con datos de carácter personal en los que el Ayuntamiento actúe como Responsable o Encargada del Tratamiento.

El personal laboral que lo desee deberá solicitar una autorización preiia para el tratamiento de datos en relación con las salidas y/o entradas de soportes del centro de trabajo.

Únicamente la persona Responsable del Tratamiento o a quién este designe, podrán autorizar la salida de datos de carácter personal en soportes extraíbles de la organización.

5.9.2 Disposición final de soportes.

Reutlización:

Cuando un equipo deba ser reasignado a otra persona trabajadora de la organización, por ejemplo, porque su usuario/a actual iaría de función dentro del Ayuntamiento o bien deja de prestar seriicios para la misma, la persona Responsable del Tratamiento, se encargará de solicitar la entrega y deiolución cualquier dispositios a traiés del cual puedan tratarse datos personales, incluso aquellos que otorguen el acceso fsico a instalaciones y dependencias de la organización.

A tales fnes, se procederá de la siguiente forma:

- Antes de reasignar el dispositio o equipo en cuestón, se procederá a realizar copia de la información que contengan, en caso de ser necesario.
- Una iez realizada la copia de seguridad, se procederá a realizar un formato completo, de tal forma que no se mantengan usuarios/as ni claies.
- Realizado el formato completo y confgurado el equipo para la nueia persona usuaria, se procederá a su entrega, preiia frma el registro de entrega de dispositio a la persona trabajadora.

Disposición final:

Se informa que la destrucción de la documentación, ya sea en soporte papel o digital, que se genera como consecuencia del desarrollo de las funciones inherentes al puesto de trabajo, sobre todo cuando esta contenga datos personales, tene una labor preiia que si no se realiza correctamente puede deriiar en un incumplimiento de la normatia de protección de datos.

Por lo expuesto, no pueden trarse los documentos ni soportes, de ningún tpo, directamente a la basura, ni aunque se rompan en trozos; la disposición fnal de los mismos se realizará de la siguiente forma:

- Si se ia a desechar el soporte, por ejemplo, un ordenador, portátl o móiil, discos duros, DVD's, CD's, memorias USB, cintas o cualquier otro tpo de dispositio digital; por mal funcionamiento, antggedad, inutlidad, etc., la persona empleada deberá ponerlos a disposición de la persona Responsable del Tratamiento o de la persona designada por este a tal, para que dicha persona proceda a su desechado.
- Si se ia a desechar información contenida en papel, la persona trabajadora deberá destruirlos en las trituradoras habilitados a tal fn.

- Destruir los papeles que contengan información personal empleando las destructoras de papel habilitadas a tal fn, dentro de las instalaciones del responsable.

5.10 Procedimiento de noticación, gestón y respuesta ante las incidencias.

El procedimiento de notfcación y gestón de incidencias consistente en iiolaciones de datos por parte de terceros/as, mediante acceso no consentdo on-line o presencial, debe contener un registro en el que conste:

- El tpo de incidencia.
- El momento en que se ha producido.
- La persona que realiza la notfcación.
- A quién se le comunica.
- Los efectos que se hubieran deriiado de la misma.
- El sistema informátco utlizado en caso de tratarse de gestón automatzada.

6. DATOS VIOLENCIA DE GÉNERO

Se garantzará una información adecuada y que cumpla con los criterios de asistencia y confdencialidad a las mujeres iíctmas de Violencia de Género que trabajen en el Ayuntamiento sobre las medidas de protección que les asisten.