Funciones y obligaciones de las Unidades de la Organización

A continuación se definen las funciones a desarrollar por cada una de las unidades de la organización de seguridad en el Ayuntamiento de Vitoria-Gasteiz. El personal asignado a las Unidades de Seguridad desempeñará las funciones enumeradas de forma complementaria y compartida con las tareas que comporte el ejercicio habitual de su trabajo en el Ayuntamiento.

El último punto de este apartado lo constituyen las funciones y obligaciones de todo el personal con acceso a los datos de carácter personal.

1. Responsable de Tratamiento

Dado que la responsabilidad de esta unidad recae en una persona jurídica (el Ayuntamiento de Vitoria-Gasteiz), las funciones operativas de la misma son asumidas y realizadas por su Delegado de Protección de Datos, Delegados de Protección de Datos Departamentales Departamentales y Responsables de Autorización de Accesos.

Esta figura se personifica en la máxima autoridad de la organización: el Alcalde o Alcaldesa.

2. Comisión de Seguridad

- Definición de Estrategias y Políticas de Seguridad de la información.
- Articulación de Normativas de Seguridad.
- Aprobación de los Documentos de Seguridad que se elaboren.
- Revisión de los informes de auditoria que en materia de seguridad se emitan periódicamente.
- Revisión de los informes de verificación del correcto cumplimiento de lo dispuesto en el Documento de Seguridad que periódicamente emita la persona Delegada de Protección de Datos.
- Análisis de los informes explicativos emitidos por la persona Delegada de Protección de Datos, referente a las incidencias que afecten de manera grave a los Sistemas de Información.
- Seguimiento de los diferentes Planes de Seguridad que se definan.
- Coordinación de acciones en materia de seguridad, con la persona Delegada de Protección de Datos, a quien se atribuye el control y supervisión de dichas actividades.
- Tratar cualquier otro tema que se considere de interés en materia de seguridad.

3. Delegado de Protección de Datos

- Definir y establecer las normas y procedimientos que en materia de seguridad afecten a los tratamientos de los datos.
- Coordinar, controlar y supervisar las actividades relacionadas con los tratamientos de datos en materia de seguridad.
- Analizar los informes de Auditoria que periódicamente se realicen y adoptar las medidas que sean necesarias para solventar las deficiencias detectadas.
- Supervisar y analizar de forma periódica las incidencias habidas, relacionadas con la seguridad de los tratamientos de datos.
- Elaborar un informe explicativo de aquellas incidencias que afecten de manera grave a los sistemas de seguridad del Ayuntamiento.
- Establecer medidas cuya aplicación aminore y/o elimine las incidencias producidas.
- Revisar periódicamente la información de control sobre los Registros de accesos y elaborar un informe de las revisiones realizadas y los problemas detectados.
- Autorizar la salida de soportes informáticos que contengan datos de carácter personal.
- Habilitar los mecanismos y procedimientos necesarios, ya sea hardware o software, para cifrar los DCP especialmente protegidos, cuando sea necesario.
- Verificar la definición y aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos.
- Adoptar las medidas oportunas para que el personal usuario del Ayuntamiento conozca las normas de seguridad que afectan al desarrollo de sus funciones y las consecuencias en que puede incurrir en caso de incumplimiento.
- Asegurar la realización de las copias de respaldo y recuperación de los soportes con DCP y, en los casos que sea obligatorio, garantizar su almacenamiento en un lugar diferente a aquel en que se encuentren los equipos informáticos según el procedimiento establecido.
- Cuantas otras se deriven de las diferentes normativas y procedimientos.

4. Delegados de Protección de Datos Departamentales

- Aplicar, divulgar, verificar y realizar el seguimiento de las directrices generales de seguridad en el ámbito del Departamento.
- Elaborar informes periódicos de situación.

- Controlar el cumplimento de la legislación vigente en materia de datos de carácter personal dentro del Departamento.

- En colaboración con la persona Delegada de Protección de Datos, adoptar las medidas oportunas para que el personal usuario del Ayuntamiento conozca las normas y procedimientos de seguridad que afectan al desarrollo de sus funciones y las consecuencias en que pueden incurrir en caso de incumplimiento.

- Todas las que realicen por delegación del Delegado de Protección de Datos.

5. Responsables de Autorización de Accesos

- Conceder o denegar al personal usuario la autorización de acceso a los Sistemas de Información.

- Autorizar al personal que lo requiera el acceso a las dependencias en las cuales están ubicados los ficheros objeto de su responsabilidad.

- Solicitar la actualización del Documento de Seguridad cuando la modificación de un Sistema de Información u otras circunstancias lo requieran.

- Autorizar la salida de soportes informáticos que contengan DCP, por delegación de la persona Delegada de Protección de Datos.

- Aprobar por escrito la recuperación de datos desde copias de respaldo que requiera la utilización de procesos específicos no planificados.

6. Administradores de SSII

- Mantener actualizado el registro o registros de usuarios y usuarias con acceso autorizado a los Sistemas de Información que contengan datos de carácter personal.

- Establecer mecanismos que eviten que un/a usuario/a pueda acceder a información o recursos con derechos distintos a los autorizados.

- Asegurar que el almacenamiento de los archivos de contraseñas garantice la confidencialidad e integridad.

- Implementar y ejecutar cuantas medidas de seguridad técnicas hayan sido definidas por la persona Delegada de Protección de Datos.

7. Obligaciones que afectan a todo el personal

7.1. Puestos de trabajo

- Los puestos de trabajo estarán bajo la responsabilidad de algún/a usuario/a autorizado/a que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

- Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

- Cuando la persona responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos, por ejemplo, a través de un protector de pantalla. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

- En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con usuarios/as no autorizados/as para acceder a los datos de carácter personal, las personas responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

- Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos, etc. que sólo podrá ser cambiada bajo la autorización de su RPD o por administradores autorizados.

- Todo el personal que accede a los SSII del Ayuntamiento debe utilizar únicamente las versiones de software facilitadas por la organización. Todo este personal tiene prohibido instalar copias ilegales de cualquier programa o borrar cualquier programa instalado legalmente, sin autorización.

7.2. Uso apropiado de recursos

Los recursos informáticos y de comunicaciones del Ayuntamiento están disponibles para el cumplimiento de sus funciones. A tal fin quedan prohibidos:

- El uso de los recursos para actividades no relacionadas con las funciones propias de cada persona usuaria.

- Las actividades, equipos o aplicaciones no autorizadas por el Ayuntamiento.

- Introducir en los sistemas de información o la red corporativa contenidos comprometedores para la organización. Estos son contenidos obscenos, amenazadores, inmorales u ofensivos, pero caben también otras posibilidades.

- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX, sniffers, crackeadores o cualquier otro dispositivo lógico que cause o pueda causar cualquier alteración

o daño a los SSII. El personal del Ayuntamiento tiene la obligación de utilizar programas antivirus y sus actualizaciones para prevenir la entrada en los SSII de cualquier elemento destinado a destruir o corromper la información.

- Intentar destruir, alterar o inutilizar de cualquier otra forma los recursos telemáticos del Ayuntamiento.

7.3. Recursos de Red

Ninguna persona con acceso a los SSII debe:

- Conectar a ninguno de los recursos ningún tipo de dispositivo que posibilite la conexión a la red corporativa. Esta tarea corresponde únicamente a las personas administradoras de los Sistemas de Información.

- Conectarse a la red corporativa a través de otros medios que no sean los definidos por el Ayuntamiento.

- Intentar adquirir derechos de accesos distintos a los asignados en función de sus funciones.

- Intentar acceder a áreas restringidas de los SSII.

- Intentar distorsionar o falsear los registros log de los SSII.

- Intentar descifrar las claves, sistemas o algoritmos de cifrado o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otras personas usuarias, ni dañar o alterar los recursos de la organización.

7.4. Identificación y autenticación

- El personal usuario es responsable de toda actividad relacionada con el uso de su acceso autorizado.

- Cada persona con acceso a los SSII será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá comunicarlo a su Delegados de Seguridad Departamental.

- Cada persona con acceso a los SSII deberá utilizar única y exclusivamente su acceso autorizado para entrar al sistema. No deben utilizar ningún acceso autorizado de otro/a usuario/a, aunque dispongan de la autorización de su propietario/a.

7.5. Gestión de incidencias

- Cualquier persona usuaria que tenga conocimiento de una incidencia es responsable de la comunicación de la misma a su Delegado de Protección de Datos Departamental, a través de los mecanismos habilitados al efecto en el procedimiento correspondiente.

- El conocimiento y la no notificación de una incidencia por parte de una persona usuaria será considerado como una falta contra la seguridad del Tratamiento por parte de esa persona.

7.6. Gestión de soportes

- Aquellos medios que sean reutilizables, y que hayan contenido copias de datos de carácter personal, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

- Los soportes que contengan datos de carácter personal deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso de esos datos.

- Cuando la salida de datos de carácter personal se realice por medio de correo electrónico los envíos se realizarán, dejando constancia de estos envíos en el directorio histórico de esa dirección de correo o en algún otro sistema de registro de salidas que permita conocer en cualquier momento los envíos realizados, a quien iban dirigidos y la información enviada.

- Cualquier salida de información con datos de carácter personal, sólo podrá ser realizada por personal autorizado.

- Cuando se produzca una salida de datos de carácter personal de nivel alto, estos deberán ser cifrados o bien se deberá utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

- Se deberán registrar los envíos realizados mediante correo electrónico o transferencia de datos por red, de forma que se pueda siempre identificar su origen, tipo de datos, formato, fecha y hora del envío y persona destinataria de los mismos.

7.7. Deber de Secreto

- El personal usuario de los SSII deberá guardar, por tiempo indefinido, absoluta reserva y no deberá divulgar ni utilizar directa o indirectamente, los datos de carácter personal y demás información a la que tengan acceso durante su vinculación con el Ayuntamiento. Esta obligación continuará vigente incluso después de la extinción de las relaciones con el Ayuntamiento.

- En el caso en que por motivos relacionados con el puesto de trabajo, el personal empleado entre en posesión de información confidencial contenida en cualquier tipo de soporte y a través de cualquier medio, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello otorgue derecho alguno de posesión, titularidad o copia sobre dicha información.

- El incumplimiento de estas obligaciones podría llegar a constituir un delito de revelación de secretos previsto en el art. 197 del Código Penal, que puede dar derecho a exigir compensaciones.