AYUNTAMIENTO DE SAN SEBASTIÁN

Anuncio

La Junta de Gobierno Local del Ayuntamiento de Donostia/San Sebastián el día 17 de mayo de 2016 aprobó la Política de Seguridad de la Información.

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

El desarrollo de la Administración Electrónica implica el tratamiento de gran cantidad de información por parte de los sistemas de tecnologías de la información y de las comunicaciones. La información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiaran la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Al objeto de dar cumplimiento al ENS, el Ayuntamiento de San Sebastián, conocedora de los riesgos que pueden afectar a los sistemas de información, que soportan los trámites electrónicos puestos a disposición a la ciudadanía, y teniendo en cuenta que ésta pone a su disposición su activo más valioso "su propia Información" es consciente de que éstos deben ser administrados con la suficiente diligencia, y que se deben de tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

De este modo, todos los departamentos y/o áreas del Ayuntamiento de San Sebastián, que se encuentran dentro del ámbito del ENS, tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, para el Ayuntamiento de San Sebastián, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 7 del ENS.

Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, el Ayuntamiento de San Sebastián implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, el Ayuntamiento de San Sebastián:

- Autoriza los sistemas antes de entrar en operación.

- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección

El Ayuntamiento de San Sebastián establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS (reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 8 del ENS. Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

Respuesta

El Ayuntamiento de San Sebastián establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Recuperación

Para garantizar la disponibilidad de los servicios, el Ayuntamiento de San Sebastián dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos. Se trata de los procedimientos y las normas contenidos en el Documento de Seguridad del Ayuntamiento de San Sebastián de 18 de mayo de 2012.

Seguridad de datos

El Ayuntamiento de San Sebastián deberá adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado según lo establecido en el artículo 9 de la Ley Orgánica 15/1999 de protección de datos de carácter personal, y los artículos 89 y siguientes del Real Decreto 1720/2007 por el que se aprueba el reglamento que desarrolla dicha ley. En este sentido, se estará también a lo establecido por el Documento de Seguridad del Ayuntamiento de San Sebastián que establece normas y procedimientos concretos sobre el modo en que deben gestionarse los datos de carácter personal, ficheros que los contengan, soportes y documentos en que se encuentran, auditorías, medidas de control, copias de respaldo, administración de usuarios, notificación y gestión de incidencias, recuperación de datos, ejercicio del derecho de acceso a datos de carácter personal, procedimiento para los derechos de rectificación y cancelación, control de acceso físico, etc.

MISIÓN DEL AYUNTAMIENTO DE SAN SEBASTIÁN

El Ayuntamiento de San Sebastián, para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población. Para ello pone a disposición de la misma la realización de trámites online con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, crear la confianza necesaria entre ciudadano y Ayuntamiento en esta relación.

ALCANCE

Se determinará el alcance desde un doble punto de vista, el organizativo por un lado y el relativo a sistemas de información o alcance funcional.

En cuanto a este último, esta Política se aplicará a los sistemas de información del Ayuntamiento de San Sebastián, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo. Existen recursos que se utilizan para las las relaciones entre administraciones y ciudadanos que han sido creadas y siguen siendo mantenidas por empresas privadas. Son aplicaciones y páginas web cuyo desarrollo ha sido encargado a éstas por diferentes departamentos e incluso organismos municipales. En lo que a éstos se refiere, se deberán incluir dentro del ámbito de la ENS, y se deberá notificar a estas empresas los criterios de seguridad por los que se rige el Ayuntamiento, sus organismos autónomos y sus sociedades públicas a fin de que adecuen los recursos a estos requisitos de seguridad.

En lo que al punto de vista organizativo se refiere, y en lo relativo al ENS, las obligaciones del mismo vinculan directamente al Ayuntamiento de San Sebastián y sus organismos autónomos: CIM, Musika Eskola y Donostia Kirola. Pero el cumplimiento de la misión del Ayuntamiento de San Sebastián requiere tener en cuenta todas las funciones desempeñadas por el Ayuntamiento tanto de forma directa como indirecta, e incluir por ello también a las Sociedades Públicas Polloe S.A., y San Sebastián Turismo S.A., que han decidido integrarse plenamente mediante la asunción de esta Política de Seguridad de la Información, y participando en el Comité de Seguridad de la Información. Esta Política de Seguridad de la Información y el Comité de Seguridad de la Información quedan abiertos a la integración al nivel que se acuerde del resto de sociedades públicas.

El esfuerzo de integración e inclusión de organismos autónomos y sociedades públicas se debe a que (1) estas sociedades están ofreciendo servicios y trámites que parten de competencias propias municipales por lo que resulta obligatorio asegurarse de la seguridad de los sistemas y de la protección de datos; (2) en caso de que haya incidencias de seguridad, la responsabilidad última recae sobre el propio Ayuntamiento, cuyos concejales y alcalde son los consejeros de estas sociedades; (3) fijar unas normas, unos criterios y unas responsabilidades compartidas en materia de seguridad de la información contribuye a una mayor cohesión y a un mejor servicio; y (4) el ciudadano percibe la presencia del Ayuntamiento en estas sociedades, y atribuye la responsabilidad última de su actuación a éste.

Todos los miembros del Ayuntamiento de San Sebastián, afectados por el alcance del ENS tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del Ayuntamiento de San Sebastián, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía, está integrado por las siguientes normas:

a) Real Decreto 3/2010 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
b) Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común en tanto esté en vigor
c) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas cuando entre en vigor.
d) Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público cuando entre en vigor
e) Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal.
f) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
g) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos en tanto esté en vigor
h) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
i) Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
j) Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.
k) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
l) Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.
m) Ley 59/2003, de 19 de diciembre, de firma electrónica.
n) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
o) Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
p) Boletín Oficial de Guipuzkoa nº 119, de 23 de junio de 2008 por el que se aprueba definitivamente el Reglamento de Administración Electrónica del Ayuntamiento de Donostia-San Sebastián.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de San Sebastián derivadas de las anteriores y publicadas en las sedes electrónica comprendidas dentro del ámbito de aplicación de de la presente Política así como el Documento de Seguridad de 18 de mayo de 2012 aprobado por el Pleno del Ayuntamiento de Donostia-San Sebastián.

ORGANIZACIÓN DE LA SEGURIDAD

Estructura organizativa

Roles de Seguridad de la Información

Los roles fundamentales en la Seguridad de la Información son los siguientes:

- Responsable de información, que se desempeñará por el Técnico Jurídico de la Dirección de Presidencia
- Responsable del servicio, que será desempeñado por el/la Director/a de Presidencia
- Responsable de seguridad del ENS, que será desempeñado por el/la Director/a de Innovación o Desarrollos Tecnológicos
- Responsable de información, que se desempeñará por el/la Técnico Jurídico del Área de Presidencia
- Responsable de Sistema del ENS: El/la Jefe/a de Producción

En el caso de los Sistemas de los Organismos Autónomos que queden fuera del ámbito de de los servicios gestionados por el Centro Informático Municipal de San Sebastián, el representante de dichos organismos en el Comité de Seguridad de la Información asumirá el rol de Responsable de Seguridad y Sistemas de dichos servicios.

Las políticas y roles de seguridad de protección de datos residen en la Comisión de Seguridad

Comité de Seguridad

El Comité de Seguridad estará constituido por los siguientes cargos y personas:

- Presidente/a: El/la concejal/a Delegado de Presidencia y Transparencia, Recursos Humanos e Innovación
- Secretaria/o: El/la Jefe/a de Servicio de Organización y Calidad
- Responsable de Seguridad del ENS: El/la director/a de Innovación o Desarrollos Tecnológicos
- Responsable de Sistemas del ENS: El/la Jefe/a de Producción
- Responsable del Servicio: El/la Director/a de Presidencia
- Responsable de Información: El/la Técnico Jurídico de la Dirección de Presidencia
- Responsables de seguridad ENS de organismos autónomos o personas en quienes deleguen
- Responsables de Seguridad ENS de las Sociedades Públicas Turismo y Polloe

Se convocará al resto de personas con responsabilidades en los roles del ENS según las necesidades del Comité de Seguridad de la Información. De igual manera, se convocará a las personas responsables de Seguridad de ENS de cada área municipal en función de las necesidades del Comité de Seguridad de la Información.

Las reuniones ordinarias del Comité de Seguridad de la Información tendrán una periodicidad semestral. Podrán convocarse reuniones extraordinarias cada vez que las necesidades o las circunstancias así lo exijan.

Funciones de las Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación se detallan y se establecen las funciones y responsabilidades de cada una de las figuras:

- La persona Responsable del Servicio, determina los requisitos de seguridad de los servicios prestados dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS.
- El Responsable de la Información, determina los requisitos de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad ENS.
- El Responsable de Seguridad ENS, su función es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho.
- EL Responsable del Sistema, es el encargado de las operaciones del sistema.

Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

- **Atender las inquietudes, en materia de Seguridad de la Información**, del Ayuntamiento y de los diferentes departamentos informando regularmente del estado de la Seguridad de la Información a la Alcaldía.
- **Asesorar en materia de Seguridad de la Información**, siempre y cuando le sea requerido.
- **Representar frente a terceros** (entidades privadas y otras Administraciones Públicas) l**a figura de responsable de seguridad LOPD en acciones transversale**s. La representación será avalada previo informe favorable del estado de la seguridad emitidos de manera solidaria por parte de los Responsables de Seguridad LOPD y Responsables delegados por ficheros.
- **Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables** y/o entre diferentes Áreas/Departamentos del Ayuntamiento, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

- **Recoger las funciones y obligaciones de los Responsables de la Información y los Servicios ENS, en aquellas acciones transversales**, en las que le sea solicitado y/o se considere necesario.
- **Promover la mejora continua del sistema de gestión de la Seguridad de la Información.** Para ello se encargará de:
    - **Coordinar los esfuerzos** de las diferentes áreas/servicios en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - **Proponer planes de mejora** de la Seguridad de la Información del Ayuntamiento, con su dotación presupuestaria correspondiente., priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación (**Privacy by Design**). En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - **Realizar un seguimiento de los principales riesgos** residuales asumidos por el Ayuntamiento y recomendar posibles actuaciones respecto de ellos.
    - **Realizar un seguimiento de la gestión de los incidentes de seguridad** y recomendar posibles actuaciones respecto de ellos.
- **Elaborar (y revisar regularmente) la Política de Seguridad de la Información** para su aprobación por el Órgano Superior del Ayuntamiento.
- **Elaborar la normativa de Seguridad de la Información** para su aprobación en coordinación con el Ayuntamiento de San Sebastián .
- **Verificar la idoneidad de los procedimientos de seguridad de la información** y demás documentación.
- **Elaborar programas de formación destinados a formar y sensibilizar al personal** en materia de Seguridad de la Información y en particular de protección de datos de carácter personal.
- **Elaborar y aprobar los requisitos de formación y calificación de administradores,** operadores y usuarios desde el punto de vista de Seguridad de la Información.
- **Promover la realización de las auditorías periódicas ENS y LOPD** que permitan verificar el cumplimiento de las obligaciones del Ayuntamiento en materia de seguridad.

Procedimientos de designación

El Ayuntamiento de San Sebastián procederá a realizar la constitución del comité y de las distintas responsabilidades. Todos los nombramientos se revisarán cada 4 años o cuando los puestos quedes vacantes.

DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de San Sebastián solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos. Estas medidas estarán recogidas en el Documento de Seguridad aprobado por el Pleno del Ayuntamiento de Donostia-San Sebastián.

OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento de San Sebastián, que se encuentran dentro del ámbito del ENS serán objeto de sesiones presenciales o de concienciación en materia de seguridad en función de la periodicidad que el Comité de Seguridad de la Información establezca como necesario y razonable en base a las necesidades detectadas, y siendo en todo caso un programa de concienciación continua que aspira a atender a todos los miembros del Ayuntamiento de San Sebastián, organismos autónomos y sociedades públicas incluidas en su perímetro, y en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

1. Categorización de los sistemas.
2. Análisis de riesgos.
3. El Comité de Seguridad procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (políticas, protocolos, procedimientos, instrucciones técnicas, etc.)

Del mismo modo, esta Política de Seguridad de la Información complementa las políticas de seguridad del Ayuntamiento de San Sebastián en materia de protección de datos de carácter personal.

La Normativa de Seguridad estará a disposición de todos los miembros de la Institución que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en www.donostia.eus/documentodeseguridad

TERCERAS PARTES

Cuando el Ayuntamiento de San Sebastián preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de San Sebastián utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.