Excmo. Ayuntamiento
SANTA CRUZ DE TENERIFE

EL ILMO. SR. DON JUAN ALFONSO CABELLO MESA CONCEJAL-SECRETARIO DE LA JUNTA DE GOBIERNO DE LA CIUDAD DE SANTA CRUZ DE TENERIFE.

CERTIFICA: Que la Junta de Gobierno de la Ciudad de Santa Cruz de Tenerife, en sesión Ordinaria celebrada el día 2 de mayo de 2022 adoptó, entre otros, el siguiente acuerdo:

7.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE SANTA CRUZ DE TENERIFE, A EFECTOS DE REVISIÓN Y ACTUALIZACIÓN.

Visto el siguiente informe propuesta del Servicio Administrativo de Tecnología:

"**ANTECEDENTES DE HECHO**

Primero. – La Junta de Gobierno de la Ciudad, en sesión celebrada el día 26 de junio de 2021, adopto el siguiente acuerdo*: "Aprobar la Política de Seguridad del Ayuntamiento de Santa Cruz de Tenerife*", y cuyo texto se da por reproducido al incorporase al expediente.

Como elemento de dicha política se crea el Comité de Seguridad de la Información, como órgano que "*coordina la Seguridad de la Información a nivel de organización*" y entre cuyas funciones está "*elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección"*.

Segundo.- Con fecha 23 de febrero de 2022 se reúne el Comité de Seguridad de la Información y acuerda, entre otros asuntos, "a*probar el documento propuesto de actualización de la Política de Seguridad de la Información* y su remisión al Servicio Administrativo de Tecnología para la tramitación de la propuesta de acuerdo a la Junta de Gobierno Local".

La revisión de dicho documento, que se transcribirá íntegramente en la parte dispositiva de este informe, se concreta en los siguientes aspectos:

- .- Se modifica su alcance (punto 3), siendo ahora de aplicación y de obligado cumplimiento para todos los órganos municipales del Excmo. Ayuntamiento. si bien cada entidad pública vinculada o dependiente incluida en este ámbito de aplicación podrá disponer formalmente de su propio documento de política de seguridad de la información debidamente justificado, que adecue, en su caso, las directrices comunes del Ayuntamiento de Santa Cruz de Tenerife a sus particularidades.
- .- Se actualiza el marco normativo (punto 5).

 . Se determina la participación de la Junta de Gobierno de la Ciudad en la aprobación de la policía de seguridad (punto 6.1).

 .- Se amplía el Comité de Seguridad, incorporando al Excmo. Sr. Alcalde como Presidente, el Concejal del Área que ostente competencias en materia de Tecnología, y al Delegado de Protección de Datos, éste con voz pero sin voto (punto 6.2).

 .- Se actualiza la asignaciones de responsabilidad a los siguientes roles: Responsable de la Información, Responsable del Servicio, Responsable de Seguridad de la Información, Responsable del Sistema, Administradores de la Seguridad del Sistema (punto 6.3).

 .- Se modifica el procedimiento de designación de personas (punto 6.5).

 .- Se establece como formación una sesión anual para todos los usuarios (punto 10).

Tercero. Sometido el expediente a informe de la Asesoría Jurídica, éste informa de conformidad con fecha 20 de abril de 2022, proponiendo la inclusión de una norma jurídica en el marco normativo del texto; dicha observación es aceptada por este Servicio.

FUNDAMENTOS DE DERECHO

I.- El art. 11 del Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, establece que "1. *Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente. (…). 2. A los efectos indicados en el apartado anterior, se considerarán órganos superiores, los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico, de acuerdo con lo establecido en (…) Ley 7/1985, de 2 de abril, reguladora de las bases del Régimen Local (…)".*

Conforme establece el art. 130 de la Ley 7/1985, de 2 de abril, de Bases de Régimen Local y concordante art. 7.2 del Reglamento Orgánico y de la Administración del Excmo. Ayuntamiento de Santa Cruz de Tenerife, "son Órganos superiores el Alcalde y los miembros de la Junta de Gobierno Local".

II.- Por haber sido informado el texto inicial por los Servicios Jurídicos con fundamento en el art. art. 13 del Reglamento de su Reglamento, se ha sometido el expediente a su conocimiento, en los términos establecido en el Antecedente Tercero.

III.- Ostentando el Excmo. Sr. Alcalde la presidencia de la Junta de Gobierno de la Ciudad conforme lo dispuesto en el art. 16.1 de la LRBRL, y a tenor de lo establecido en el Fundamento I de este informe, es ese órgano colegiado quien ostenta la competencia.

PROPUESTA DE ACUERDO

PRIMERO.- Aprobar la revisión y actualización del documento denominado "POLÍTICA DE SEGURIDAD DEL EXCMO AYUNTAMIENTO DE SANTA CRUZ DE TENERIFE, ", quedando su redacción del siguiente tenor literal:

1.- MISIÓN Y SERVICIOS

Es misión del Ayuntamiento de Santa Cruz de Tenerife la gestión de los servicios que son de su competencia que le son propios conforme a la legislación vigente, en un marco integral de seguridad de la información, disponiendo de medidas técnicas, organizativas, legales y de protección.

Los servicios que presta están recogidos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local y, más en concreto, lo establecido en sus artículos 25 y 26, sin perjuicio de las especialidades de los Ayuntamientos denominados de gran población, regulados en su Título X, como es el caso del Ayuntamiento de Santa Cruz de Tenerife y las normas autonómicas que delegan competencias como es la Ley 7/2015, de 1 de abril, de los municipios de Canarias (artículo 11 sobre atribución de competencias a los municipios de Canarias).

2.- PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Los principios básicos y requisitos de la seguridad de la información desarrollados bajo el marco de esta Política de Seguridad son los recogidos en el Esquema Nacional de Seguridad regulado por el Real Decreto 3/2010 de 8 de enero, modificado por Real Decreto 951/2015, de 23 de octubre, en particular, los previstos en sus capítulos II y III, y su normativa de desarrollo:

- Profesionalidad
- Protección de las instalaciones
- Seguridad por defecto
- Protección de la información

- Prevención proactiva de la información y los servicios
- Mejora continua
- Confidencialidad
- Concienciación y formación
- Integridad y calidad de la información
- Disponibilidad de los sistemas de información y continuidad de los servicios ante contingencias
- Gestión del riesgo
- Proporcionalidad en coste

3.- ALCANCE

Esta política será de aplicación y de obligado cumplimiento para todos los órganos municipales del Ayuntamiento de Santa Cruz de Tenerife, entendiendo por órganos a sus áreas y distritos, unidades administrativas, organismos autónomos y demás entidades públicas vinculadas o dependientes.

Sin perjuicio de las directrices establecidas en la presente política, cada entidad pública vinculada o dependiente incluida en este ámbito de aplicación podrá disponer formalmente de su propio documento de política de seguridad de la información debidamente justificado, que adecue, en su caso, las directrices comunes del Ayuntamiento de Santa Cruz de Tenerife a sus particularidades.

4.- JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD

4.1.- Necesidad de la seguridad en los sistemas de información

La consecución de los objetivos de los servicios que se prestan por el Ayuntamiento de Santa Cruz de Tenerife a la ciudadanía, las empresas, los autónomos y otras entidades del sector público depende de los sistemas de información y las comunicaciones.

Los sistemas de información, en consecuencia, deberán ser gestionados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños, deliberados o accidentales, que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada y/o de los servicios prestados.

El objetivo principal 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 y reaccionando con presteza ante los incidentes.

Los sistemas de información, consecuentemente, deberán estar protegidos frente a las amenazas cuyo impacto pueda afectar a la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad de la información y/o a la disponibilidad de los servicios.

Para responder a estas amenazas se requiere una estrategia de seguridad que se adapte ágilmente a los cambios del ecosistema para garantizar la prestación continua de los servicios.

El Esquema Nacional de Seguridad, por otra parte, establece la obligación, en su artículo 11, de que "*Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente*".

4.2.- Requisitos de seguridad de la información

Los órganos, unidades administrativas y demás entidades públicas vinculadas o dependientes del Ayuntamiento de Santa Cruz de Tenerife deberán aplicar las medidas de seguridad de la información de conformidad con el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades y preparar una respuesta efectiva ante los incidentes para garantizar la continuidad de los servicios prestados.

Asimismo, deberán garantizar que la seguridad de la información es una parte integral de cada etapa del ciclo de vida de los sistemas de información, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo, adquisición de componentes, contratación de servicios externos y explotación.

Los requisitos de seguridad y las necesidades de financiación deberán ser, asimismo, identificados e incluidos en la planificación, así como incluidos en los pliegos de licitación.

Los órganos, unidades administrativas y demás entidades públicas vinculadas o dependientes del Ayuntamiento de Santa Cruz de Tenerife deberán estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 7 del Esquema Nacional de Seguridad (prevención, reacción y recuperación).

5.- MARCO NORMATIVO

5.1.- Responsabilidades derivadas de la naturaleza legal

Se toma como referencia, sin carácter exhaustivo, la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las

Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- 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, modificado por Real Decreto 951/2015, de 23 de octubre.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Reglamento por el que se establece la Sede Electrónica del Ayuntamiento
- Texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, y su normativa de desarrollo.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP)
- Modificaciones LCSP por Ley 22/2021, de 28 de diciembre, de Presupuestos Generales del Estado para el año 2022. Disposición final vigésima novena. Modificación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- Normas aplicables a la Administración Electrónica del Ayuntamiento derivadas y de inferior rango que las citadas, comprendidas en el ámbito de aplicación de esta Política de Seguridad de la Información.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

5.2.- Responsabilidades derivadas de la normativa

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 156.2 sobre el Esquema Nacional de Seguridad establece, como uno de sus principios, que se debe disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos.

El Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.

Así mismo, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, tienen por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.

6.- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La estructura organizativa de la seguridad de la información del Ayuntamiento de Santa Cruz de Tenerife se establece mediante la identificación y definición de las competencias y responsabilidades de los órganos y roles que, a continuación, se describen.

6.1.- Junta de Gobierno

La Junta de Gobierno de la Ciudad deberá garantizar el compromiso del Ayuntamiento de Santa Cruz de Tenerife en la aplicación de las obligaciones en materia de seguridad de la información.

Este compromiso se manifiesta mediante la aprobación de la presente Política de Seguridad de la Información, así como de todas aquellas modificaciones o actualizaciones de esta.

6.2.- Comité de Seguridad de la Información

Es el órgano presidido por el Alcalde-Presidente, actuando el Concejal de Gobierno del Área que ostente la delegación de competencias en materia de Tecnología como Vicepresidente, que coordina la seguridad de la información del Ayuntamiento de Santa Cruz de Tenerife.

Estará constituido, como Vocales miembros, por los Responsables de la Información y del Servicio, el Responsable de Seguridad de la Información, el Responsable del Sistema, el Administrador de la Seguridad del Sistema y el Delegado de Protección de Datos que actuará con voz, pero sin voto.

Sus funciones serán las siguientes:

- Establecer la estrategia de ciberseguridad y privacidad de la información del Ayuntamiento de Santa Cruz de Tenerife.
- Coordinar las iniciativas del Ayuntamiento de Santa Cruz de Tenerife en materia de seguridad de la información y protección de datos personales.
- Definir los objetivos anuales en materia de seguridad de la información, que servirán para el alineamiento de las iniciativas y actividades de seguridad del Ayuntamiento de Santa Cruz de Tenerife.
- Elaborar y revisar anualmente la Política de Seguridad de la información.
- Aprobar la normativa de desarrollo de la Política de Seguridad de la Información.
- Aprobar los planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, en particular, coordinando los diferentes planes que puedan proponerse por los órganos, unidades administrativas, y demás entidades públicas vinculadas o dependientes del Ayuntamiento de Santa Cruz de Tenerife.
- Aprobar los niveles de riesgos residuales y recomendar posibles actuaciones respecto de ellos.

- Aprobar el Plan de Concienciación y Formación de Seguridad de la Información, incluyendo los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Coordinar con los órganos, unidades administrativas y demás entidades públicas vinculadas o dependientes del Ayuntamiento de Santa Cruz de Tenerife la gestión de incidentes de seguridad de la información.
- Evaluar la eficacia de los procesos de gestión de incidentes de seguridad y brechas de datos personales y aprobar actuaciones de mejora en la respuesta y prevención proactiva.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad y privacidad de la información.
- Velar por el cumplimiento de la normativa de aplicación legal y porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de información y las comunicaciones.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Coordinar los planes de continuidad de las diferentes áreas para asegurar una actuación sin fisuras en el caso de que deban ser activados.
- Coordinar y aprobar las propuestas recibidas de proyectos en los diferentes ámbitos de seguridad, supervisando su progreso y analizando y tomando decisión ante las posibles desviaciones.
- Recabar al Responsable de Seguridad informes regulares del estado de la seguridad y de los posibles incidentes.
- Establecer la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de funciones.
- Promover la mejora continua del sistema de gestión de la seguridad de la información
- Informar regularmente del estado de la seguridad de la información

El Responsable de Seguridad de la Información actuará como secretario del Comité de Seguridad de la Información y, como tal, desempeñará las funciones siguientes:

- Convocar, en tiempo y forma, las reuniones del Comité.
- Preparar el orden del día de los asuntos a tratar por el Comité en cada una de sus sesiones.

- Recopilar y distribuir entre los miembros del Comité, con la debida antelación, la documentación a revisar y aprobar, en su caso.
- Elaborar el acta de las sesiones y distribuir entre los miembros del Comité, en un plazo no superior a 5 días hábiles, a contar a partir de su celebración.
- Seguir el avance de la ejecución de los acuerdos y decisiones del Comité, informando en cada sesión sobre su situación.

Lo anterior no es excluyente de la constitución de Subcomités de Seguridad de las entidades públicas vinculadas o dependientes del Ayuntamiento de Santa Cruz de Tenerife, debidamente justificados, en aras a la agilidad y autonomía de actuación, siempre en el marco de sus competencias.

6.3.- Roles de seguridad de la información

La Política de Seguridad, de conformidad con la medida 3.1 del Anexo II del Esquema Nacional de Seguridad, debe describir los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, el procedimiento para su designación y renovación, así como ser conocida por todos los miembros del Ayuntamiento de Santa Cruz de Tenerife.

Se establecen, en consecuencia, los siguientes roles relacionados con la seguridad de la información:

- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad de la Información
- Responsable del Sistema
- Administrador de la Seguridad del Sistema
- Delegado de Protección de Datos

Con el objetivo de buscar la eficacia y la eficiencia de las medidas de seguridad que se adopten en torno a la información, los sistemas de información y los procedimientos administrativos asociados, los roles de Responsable de la Información y Responsable del Servicio podrán ser asumidos por el mismo responsable en razón de la materia de su competencia.

6.3.1- Responsable de la Información.

Las funciones del Responsable de la Información del Ayuntamiento de Santa Cruz de Tenerife serán asumidas por los responsables designados por cada uno de sus órganos y entidades públicas vinculadas o dependientes.

Sus funciones serán las siguientes:

- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad de integridad.
- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
- Ac

eptar los niveles de riesgo residual que afecten a la información.

6.3.2. Responsable del Servicio

Las funciones del Responsable del Servicio en el Ayuntamiento de Santa Cruz de Tenerife serán asumidas por los responsables designados por cada uno de sus órganos y entidades públicas vinculadas o dependientes.

Sus funciones serán las siguientes:

- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad del servicio.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Recabará una propuesta de los niveles de seguridad en cada dimensión del servicio a los Responsable de la Seguridad y del Sistema.
- Aceptar los niveles de riesgo residual que afecten al servicio.

6.3.3. Responsable de Seguridad de la Información.

Las funciones del Responsable de Seguridad de la Información en el Ayuntamiento de Santa Cruz de Tenerife serán asumidas por la Dirección General de Tecnología.

Sus funciones serán las siguientes:

- Reportará directamente al Presidente del Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información.
- Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Recopilará los requisitos de seguridad del Responsable de Información y del Servicio y determinará la categoría del Sistema.
- Realizará el Análisis de Riesgos y el plan de tratamiento de los mismos.
- Elaborará y firmará la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitará al Responsable de Información y del Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la documentación de seguridad del Sistema.
- Participará en la elaboración de la Política de Seguridad de la Información.
- Dirigirá la elaboración y aprobación de la normativa de seguridad de la información.
- Elaborará y aprobará los procedimientos operativos de seguridad de la información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto al Responsable de Sistema, los Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que someterá a la aprobación del Comité de Seguridad de la Información.

- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que someterá a la aprobación del Comité de Seguridad de la Información, que serán probados periódicamente por el Responsable del Sistema.
- Aprobará las directrices propuestas por el Responsable del Sistema para considerar la seguridad de la información durante todo el ciclo de vida: especificación, arquitectura, desarrollo, operación y cambios.
- Analizará y propondrá salvaguardas que prevengan incidentes en un futuro, en caso de ocurrencia de incidentes de seguridad de la información.

6.3.4. Responsable del Sistema.

Las funciones del Responsable del Sistema de Información del Ayuntamiento de Santa Cruz de Tenerife serán asumidas por la Jefatura de Servicio Técnico de Administración Electrónica y Tecnología, y en el caso de sus entidades públicas vinculadas o dependientes, por aquellos responsables que sean designados en el ámbito de sus competencias.

Sus funciones serán las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- El Responsable del Sistema podrá acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.

 Realizar las pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.

 Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

 Planificará la implantación de las salvaguardas en el sistema y ejecutará el plan de seguridad aprobado, en caso de ocurrencia de incidentes de seguridad de la información.

En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de personas usuarias se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, se podrán designar cuantos Responsables del Sistema Delegados considere necesarios.

 La propuesta de delegación corresponde al Responsable de Seguridad.

 Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema.

 Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, a quién deberán reportar.

6.3.5. Administradores de la Seguridad del Sistema.

Las funciones del Administrador de la Seguridad del Sistema en el Ayuntamiento de Santa Cruz de Tenerife serán asumidas por la Jefatura de la Sección de Infraestructuras del Servicio Técnico de Administración Electrónica y Tecnología y, en el caso de sus entidades públicas vinculadas o dependientes, por aquellos responsables que sean designados en el ámbito de sus competencias.

Sus funciones serán las siguientes:

 La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.

 Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

 Asegurar que las pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada.

 Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.

 Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de

información y los mecanismos y servicios de seguridad requeridos.

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Aprobar los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizar el estado de la seguridad del sistema.

En caso de ocurrencia de incidentes de seguridad de la información:

- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves.
- Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos.
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Determinar el modo, los medios, los motivos y el origen de los incidentes de seguridad.

6.3.6. Delegado de Protección de Datos

El Delegado de Protección de Datos del Ayuntamiento de Santa Cruz de Tenerife desempeñará, dentro de su ámbito de actuación y de sus competencias, las funciones recogidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de Abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales y demás disposiciones reguladoras de la materia.

6.4. Jjerarquía en el proceso de decisiones y mecanismos de coordinación

Los diferentes órganos y roles de seguridad de la información (autoridad principal y delegadas) se limitan a una jerarquía simple, a saber: el Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información, que se encargará de la supervisión de la debida implementación las medidas de seguridad, según lo establecido en la presente Política de Seguridad de la Información.

El Responsable de la Seguridad informa al Comité de Seguridad de la Información de los aspectos siguientes:

- Resumen de incidentes relativos a la seguridad de la información.
- Resumen de actuaciones en materia de seguridad.
- Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

El Responsable de la Seguridad informará, asimismo, al Responsable de la Información y del Servicio de los incidentes relativas a la información y al servicio, así como de las decisiones en materia de seguridad que afecten a la información y al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

El Responsable del Sistema informará al Responsable de la Seguridad de los siguientes aspectos:

- Incidentes relativos a la seguridad del sistema y brechas de datos personales.
- Actuaciones en materia de seguridad.
- Eficacia de las medidas de seguridad.

El Administrador de Seguridad informará al Responsable del Sistema de los siguientes aspectos:

- Incidentes relativos a la seguridad del sistema y brechas de datos personales.
- Acciones de configuración, actualización o corrección.

6.5.- Procedimientos de designación de personas

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta política se realizará por la Alcaldía del Ayuntamiento de Santa Cruz de Tenerife.

7. PROTECCIÓN DE DATOS PERSONALES

El Ayuntamiento de Santa Cruz de Tenerife solo tratará 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 técnicas y organizativas necesarias para el cumplimiento de la normativa vigente en materia de protección de datos.

A la vista de la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, se deberán adoptar las medidas necesarias, tales como: el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y la designación del Delegado de Protección de Datos.

GESTIÓN DE RIESGOS

8.1. Justificación

Para todo sistema de información sujetos a esta Política se deberá contar con un análisis de riesgos debidamente actualizado, que identifique las amenazas y evalúe los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad a implantar según lo previsto en el Artículo 6 del ENS.

8.2.- Evaluación de riesgos

Para la aceptación de los niveles de riesgo, el Comité de Seguridad de la Información establecerá una escala de valores de referencia, a saber: valor objetivo, aceptable e inadmisible.

Los criterios para la evaluación de riesgos se especificarán en la metodología de evaluación de riesgos, que utilizará estándares y buenas prácticas reconocidas.

Deberán tratarse, al menos, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión del Ayuntamiento de Santa Cruz de Tenerife, así como, puedan provocar el incumplimiento de una regulación, cuyo impacto se haya apreciado como grave o muy grave.

8.3.- Recursos para el tratamiento de riesgos

El Comité de Seguridad de la Información evaluará y gestionará la asignación de recursos personales y materiales para atender a las necesidades del análisis de riesgos del sistema de información, promoviendo el uso de herramientas y el talento especializado que garantice el rigor y la homogeneidad de los informes de riesgos realizados.

8.4. Aceptación del riesgo residual

Los niveles de riesgo residual serán evaluados por el Responsable de Seguridad de la Información.

Los niveles de riesgo residual esperados tras la implantación de las medidas de seguridad previstas en el Anexo II del ENS deberán ser aceptados previamente por su Responsable de la Información y del Servicio.

Los niveles de riesgo residual serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información para su revisión y aprobación, en su caso.

8.5 Actualización de las evaluaciones de riesgos

El análisis de los riesgos y su tratamiento deberán ser actualizados, según lo establecido en el Artículo 9 del ENS, cuando se presente alguno de los casos que siguen:

- Regularmente, al menos, una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los activos, amenazas del sistema o subsistemas de información que tratan a información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente o brecha de datos personales cuyo impacto sea alto, muy

alto o crítico.

- Cuando se reporten vulnerabilidades graves.

9. GESTIÓN DE INCIDENTES DE SEGURIDAD Y BRECHAS DE DATOS PERSONALES

9.1 .Prevención de incidentes de seguridad y brechas de datos personales

Para evitar o prevenir que la información o los servicios se vean perjudicados por incidentes de seguridad se deberán implantar las medidas de seguridad determinadas por el ENS, así como cualquier medida de seguridad adicional identificada como resultado de la evaluación de amenazas y riesgos.

Los roles y responsabilidades de seguridad de todo el personal estarán, en todo momento, claramente definidas, documentados y comunicadas. Para garantizar el cumplimiento de la presente Política, se seguirán las pautas que siguen:

- Autorizar los sistemas de información antes de su entrada en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Revisar periódicamente por terceros con el fin de obtener una evaluación independiente.

9.2. Monitorización y detección de incidentes brechas de datos personales

Habida cuenta que los servicios pueden degradarse rápidamente debido a incidentes o brechas de datos personales, que van desde una disminución hasta el cese del nivel de prestación, se deberá monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según establece el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa, de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que puedan informar a los responsables tanto regularmente como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

9.3. Respuesta ante incidentes de seguridad o brechas de datos personales

Las pautas a seguir para la respuesta ante los incidentes de seguridad o brechas de datos personales son las siguientes:

- Establecer los debidos mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar las personas que actuaran como puntos de contacto en las comunicaciones de los órganos, unidades administrativas y demás entidades públicas vinculadas o dependientes del Ayuntamiento de Santa Cruz de Tenerife respecto a los incidentes.
- Notificar e intercambiar la información necesaria con el CCN-CERT relacionada con los incidentes críticos, de muy alto o alto impacto.
- Notificar a la Agencia Española de Protección de Datos, como autoridad responsable de la materia, en caso de incidente o brecha de seguridad de datos personales, cuando el riesgo pueda afectar gravemente a los derechos y libertades fundamentales de los afectados.

9.4. Recuperación y planes de continuidad

Para garantizar la disponibilidad de los servicios críticos se deberán desarrollar, probar y mejorar los planes de continuidad de los sistemas de información y las comunicaciones, como parte del plan integral de continuidad de los servicios.

10.- OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento de Santa Cruz de Tenerife y de sus entidades públicas vinculadas o dependientes tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, así como la normativa que la desarrolle, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todo usuario asistirá, al menos, a una sesión anual de formación y concienciación en materia de seguridad de la información y protección de datos personales. Se establecerá, en consecuencia, un plan de concienciación continua para todos los usuarios, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información y comunicaciones recibirán formación específica 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.

El cumplimiento de la presente Política de Seguridad de la Información es obligatorio para el personal interno o externo que intervenga en los procesos de la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

11. TERCERAS PARTES

Cuando por parte de otras organizaciones se presten servicios al Ayuntamiento de Santa Cruz de Tenerife, se les hará partícipes de esta Política de Seguridad de la Información y de la normativa que la desarrolla, así como, se establecerán canales para la coordinación con sus respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se ceda información a terceros, asimismo, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que la desarrolla, que afecte a dichos servicios o información, quedando dicha tercera parte sujeta a las obligaciones establecidas en la normativa, sin perjuicio del desarrollo de sus propios procedimientos operativos para satisfacerla.

En particular, se deberán establecer los procedimientos específicos para la notificación, respuesta y resolución de incidentes de seguridad de la información.

Se garantizará, por otra parte, que el personal de terceros que preste servicios al Ayuntamiento de Santa Cruz de Tenerife esté adecuadamente formado y concienciado en materia de seguridad de información, al menos, con el mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según lo expuesto con anterioridad, se requerirá un informe del Responsable de Seguridad 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.

12.- REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por la Junta de Gobierno de la Ciudad, de acuerdo con el artículo 11 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

13. POLÍTICAS RELACIONADAS

Esta Política de Seguridad de la Información del Ayuntamiento de Santa Cruz de Tenerife servirá de marco para el desarrollo, siempre que se justifique su necesidad, de otras políticas por parte de los órganos, unidades administrativas y demás entidades públicas vinculadas o dependientes del Ayuntamiento de Santa Cruz de Tenerife, detallando las medidas específicas a adoptar sobre los sistemas de Información de su competencia.

Esta Política se desarrollará por medio de normativa de seguridad que describa las medidas de seguridad específicas. La normativa de seguridad estará a disposición de todos los miembros de la organización que precisen conocerla, en particular, para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

14. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Junta de Gobierno de la Ciudad de Santa Cruz de Tenerife en sesión ordinaria el día 25 de abril de 2022.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión.

La presente versión de la Política de Seguridad de la Información ha sido aprobada por el Comité de Seguridad de la Información.

ANEXO.

GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Análisis de riesgos: utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Gestión de incidentes: plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas. ENS.

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. ENS.

Incidente de seguridad: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información. ENS.

Información: caso concreto de un cierto tipo de información.

Política de seguridad: conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos. ENS.

Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios. ENS.

Responsable de la información: persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad: el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio: persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema: persona que se encarga de la explotación del sistema de información.

Administrador de la Seguridad del Sistema las siguientes: persona responsable de la implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

Servicio: función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información: 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 Junta de Gobierno de la Ciudad de Santa Cruz de Tenerife, por unanimidad, adoptó acuerdo de conformidad con el transcrito informe propuesta.

Y para que así conste y surta sus efectos, expido la presente de orden y con el visto bueno del Excmo. Sr. Alcalde, haciendo la salvedad, conforme prescribe el artículo 206 del Real Decreto 2568/1986, de 28 de noviembre, del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, que el borrador del acta donde se contiene el presente acuerdo aún no ha sido aprobado, quedando, en consecuencia, a reserva de los términos que resulten de la misma, en Santa Cruz de Tenerife a la fecha de mi firma.

Visto Bueno
EL ALCALDE,

JOSE MANUEL BERMUDEZ ESPARZA - Alcalde - 04/05/2022 11:42:10

JUAN ALFONSO CABELLO MESA - Concejal - 02/05/2022 15:54:37