Excmo. Ayuntamiento
SANTA CRUZ DE TENERIFE

LA ILMA. SRA. DOÑA GLADIS DE LEON LEON CONCEJAL-SECRETARIA SUPLENTE 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 28 de octubre de 2024 adoptó, entre otros, el siguiente acuerdo:

5.- APROBACIÓN DE LA REVISIÓN Y ACTUALIZACIÓN DEL DOCUMENTO DENOMINADO "POLÍTICA DE SEGURIDAD DEL EXCMO. AYUNTAMIENTO DE SANTA CRUZ DE TENERIFE".

Visto el siguiente informe propuesta del Servicio Administrativo de Tecnología, con propuesta de acuerdo que elevan a la Junta de Gobierno la Dirección General de Tecnología, la Concejalía Delegada con competencias sectoriales en materia de Tecnología y la Concejalía de Gobierno del Área de Presidencia:

"**ANTECEDENTES DE HECHO**

Primero.- La Junta de Gobierno de la Ciudad, en fecha 26 de junio de 2017 adoptó el acuerdo de aprobar la Política de Seguridad del Ayuntamiento de Santa Cruz de Tenerife, cuyo texto se da por reproducido al incorporarse al expediente.

Segundo.- La Junta de Gobierno de la Ciudad, en sesión celebrada el día 2 de mayo de 2022, adopto el siguiente acuerdo: "Aprobar la revisión y actualización del documento denominado Política de Seguridad del Excmo. Ayuntamiento de Santa Cruz de Tenerife", y cuyo texto se da por reproducido al incorporase al expediente.

Tercero.- Con fecha 3 de junio de 2024 se reúne el Comité de Seguridad de la Información y acuerda, entre otros asuntos, "aprobar el documento propuesto de actualización de la Política de Seguridad 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 adapta el capítulo 2 de "Principios de seguridad de la información" al nuevo Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Se elimina el detalle del marco normativo de referencia y se sustituye por el Registro de requisitos legales y el procedimiento de gestión de requisitos legales (aprobados por el Comité de Seguridad en dicha sesión).
- Se corrigen las referencias al anterior Real Decreto del ENS.
- Se añade una referencia a la vigilancia (nuevo concepto del ENS) en el capítulo dedicado a la mejora continua.

- Se incluyen los roles relacionados con la legislación de las infraestructuras críticas y servicios esenciales.
- Se definen las funciones del comité de crisis dentro de la legislación de aplicación.
- Se realiza una revisión de los requisitos del ENS en cada apartado de la Política.

Cuarto.- En fecha 8 de octubre de 2024 se procede a rechazar por los Servicios Jurídicos el encargo de informe en el tramitador de expedientes, con el siguiente texto: "Siguiendo indicaciones de la Directora de la Asesoría Jurídica, no procede informar este documento por cuanto no se trata de una disposición de carácter general, ni se exige dicho informe por norma sectorial."

FUNDAMENTOS DE DERECHO

I.- El art. 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (a partir de ahora RD 311/2022), establece que "2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente".

Conforme establece el art. 2.1 del RD 311/2022, "El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma."

Por su parte, el art. 2.1 e la mencionada Ley 40/2015, señala que el sector público comprende, entre otros, a las Entidades que integran la Administración 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, procede su remisión a ese centro gestor para que emita informe al respecto. En fecha 8 de octubre de 2024 se procede a rechazar por los Servicios Jurídicos el encargo de informe en el tramitador de expedientes, con el siguiente texto: "Siguiendo indicaciones de la Directora de la Asesoría Jurídica, no procede informar este documento por cuanto no se trata de una disposición de carácter general, ni se exige dicho informe por norma sectorial."

III.- De conformidad con lo preceptuado en el artículo 172.1 del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, aprobado por Real Decreto 2568/1986, de 28 de noviembre; artículos 44, letras c) y d), 45.1 y 51.2, letras c) y f), del Reglamento Orgánico del Gobierno y de la Administración de este Ayuntamiento y artículo 40.2.d) de la Ley 7/2015, de 1 de abril, de los municipios de Canarias, la propuesta de acuerdo se debe formular por la Jefatura del Servicio del Servicio Administrativo de Tecnología, y se elevarse a la Junta de Gobierno por la Dirección General de Tecnología, Concejalía Delegada en materia de Recursos Humanos, Tecnología, Transparencia, Protección de datos, Organización, Atención Ciudadana, Estadísticas y Demarcación Territorial, Consumo, Administración Interna, Gabinete de Prensa, Protocolo y Soporte a Distritos y Concejalía de Gobierno del Área de Presidencia.

IV.- Dado que tanto el primer texto de la Política de Seguridad del Excmo. Ayuntamiento de Santa Cruz de Tenerife como su posterior revisión y actualización fueron aprobados por la Junta de Gobierno de la Ciudad, deberá ser este mismo órgano el competente para la revisión y actualización del documento que se pretende realizar.

PROPUESTA DE ACUERDO

ÚNICO.- 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 OBJETIVOS

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

Este documento tiene por objeto crear la Política de Seguridad homogénea e integral del Ayuntamiento de Santa Cruz de Tenerife, considerando tanto la seguridad física como la seguridad de la información y la ciberseguridad, y establecer el marco organizativo y tecnológico de la misma. Esta Política tiene una visión holística de la seguridad y constituye una estrategia de protección común e integral orientada a garantizar, en términos adecuados, la continuidad de los servicios esenciales provistos a la Sociedad.

La Política se aplicará a todos los sistemas de información e infraestructuras críticas que gestionen en el ejercicio de sus competencias, debiendo ser cumplida por su personal y por cualquiera que tenga acceso a sus sistemas de información o bien que manejen información vinculada a dichos servicios.

2. PRINCIPIOS DE SEGURIDAD

Según la legislación vigente, los operadores de servicios esenciales, deberán aprobar unas políticas de seguridad de las redes y sistemas de información, atendiendo a los **principios de seguridad integral**, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.

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 311/2022, de 3 de mayo. Asimismo, la presente política también incluye los requisitos de protección de infraestructuras críticas relativos a la legislación de aplicación recogida en el Registro de requisitos legales.

El objeto último de la seguridad de la información es garantizar que la Organización cumple sus objetivos, desarrolla sus funciones y ejerce sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información se tienen en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.

b) Gestión de la seguridad basada en los riesgos.

c) Prevención, detección, respuesta y conservación.

d) Existencia de líneas de defensa.

e) Vigilancia continua.

f) Reevaluación periódica.

g) Diferenciación de responsabilidades

La política de seguridad se establece de acuerdo con los principios básicos antes señalados y se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos propios y de terceros.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de la actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

3. DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD, SU GESTIÓN Y ACCESO

Esta política será el eje central del cuerpo normativo de seguridad de la información del Ayuntamiento de Santa Cruz de Tenerife para todos los sistemas de información en alcance del ENS. El cuerpo normativo se compone de la Política de Seguridad, las normas y los procedimientos definidos en el Inventario de documentos del Sistema de Gestión de Seguridad

de la Información (SGSI), indicando el público objetivo de cada una de ellas y por tanto marcando quienes podrían acceder.

Esta política actuará también como referencia para futuros desarrollos normativos relativos a la seguridad integral de los activos que soportan los servicios esenciales por los que el Ayuntamiento de Santa Cruz de Tenerife ha sido designado operador crítico.

Respecto a infraestructuras críticas, el tratamiento de la documentación tendrá la clasificación de "Difusión Limitada" y deberá estar regido conforme a las orientaciones publicadas por la Autoridad Delegada para la Seguridad de la Información Clasificada (Oficina Nacional de Seguridad del Centro Nacional de Inteligencia), en lo que se refiere al manejo y custodia de información clasificada con grado de Difusión Limitada. Las orientaciones de referencia se encuentran recogidas en el documento "Normas de la Autoridad Nacional para la Protección de la Información Clasificada".

4. 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.

5. JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD

Se define la necesidad de elaborar la presente Política de Seguridad para cumplir con la legislación vigente y de aplicabilidad tanto en el ámbito de la seguridad física, la seguridad de la información y la ciberseguridad.

5.1 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.

5.2 Necesidad de la seguridad en las infraestructuras críticas

El Ayuntamiento de Santa Cruz de Tenerife presta servicios a la ciudadanía que han sido considerados servicios esenciales desde ciertas instalaciones designadas como infraestructuras críticas. Consecuentemente, los activos e infraestructuras que soportan estos servicios deben ser particularmente analizados y protegidos con medidas organizativas, operativas y técnicas con un carácter holístico, enfocadas a responder a ataques terroristas y ciber-terroristas.

La estrategia que definirá las medidas necesarias se basará en un análisis de riesgos integral y se plasmará en los Planes de Protección Específicos que servirán de base para la definición de las medidas de seguridad a implantar.

5.3 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 lo dispuesto por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, detectar y corregir las vulnerabilidades, así como preparar una respuesta efectiva ante los incidentes para garantizar la continuidad de los servicios prestados.

Asimismo, se deberá garantizar que la seguridad y privacidad de la información sea 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 formación y 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, responder, conservar los datos e información en soporte electrónico y recuperarse de incidentes, de acuerdo con el artículo 8 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Las medidas se seguridad respecto a sus infraestructuras críticas toman asimismo como referencia el Esquema Nacional de Seguridad (Real Decreto 311/2022), según se recoge en el artículo 6 del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

6. MARCO NORMATIVO

El marco normativo que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Santa Cruz de Tenerife está constituido por normas jurídicas estatales, autonómicas y/o sectoriales, orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, la seguridad física de las instalaciones, así como a la protección de datos de naturaleza personal.

Las normas que constituyen dicho marco se encuentran recogidas en el Registro de requisitos legales, el cual se mantiene actualizado según señala el correspondiente Procedimiento de gestión de requisitos legales.

También podrán formar parte del referido marco, aquellas normas aplicables a la Administración Electrónica del Ayuntamiento, que sean desarrollo de las anteriores o estén relacionadas, pudiendo ser adicionalmente publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

7. ORGANIZACIÓN DE LA SEGURIDAD

La estructura organizativa de la seguridad 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.

7.1 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 y privacidad de la información.

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

7.2 Comité de Seguridad

Es el órgano presidido por el/la Alcalde/sa-Presidente/a, actuando el Concejal/a que ostente la delegación de competencias en materia de Tecnología como Vicepresidente/a, que coordina la seguridad de la información, ciberseguridad y la seguridad física de los órganos, unidades administrativas y demás entidades públicas vinculadas o dependientes del Ayuntamiento de Santa Cruz de Tenerife.

Estará constituido, como vocales miembros con derecho a voz y voto, por los Responsables de la Información y del Servicio, el/la Responsable de Seguridad de la Información, el/la Responsable del Sistema, el/la Administrador/a de la Seguridad del Sistema, el/la Responsable de Seguridad y Enlace, el/la Responsable de Seguridad Física y el/la Delegado/a de Protección de Datos.

A las sesiones del Comité de Seguridad podrán asistir, con voz, pero sin voto, personal interno o externo que, por razón de sus funciones, conocimiento o especialización, sean convocados por la Presidencia.

Sus funciones serán las siguientes:

- Establecer la estrategia de ciberseguridad, seguridad de la información, seguridad física y protección de datos personales del Ayuntamiento de Santa Cruz de Tenerife.
- Coordinar todas las iniciativas del Ayuntamiento de Santa Cruz de Tenerife en materia de ciberseguridad, seguridad de la información, seguridad física y protección de datos personales.
- Definir los objetivos anuales en materia de seguridad y privacidad 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.
- Aprobar la normativa de desarrollo de la Política de Seguridad.

- 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 y aquellos de otra naturaleza que puedan afectar a las infraestructuras críticas.
- 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 y en los que puedan afectar a la seguridad de las infraestructuras críticas, 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 de la Información y al Responsable de Seguridad y Enlace 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 ciberseguridad, seguridad de la información, seguridad física y protección de datos personales.

El Responsable de Seguridad de la Información actuará como secretario del Comité de Seguridad 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.

El Comité se deberá reunir con carácter ordinario, al menos, dos veces al año, y con carácter extraordinario cuando lo decida su Presidente. Las normas de convocatoria y celebración de las sesiones se encuentran definidas en el Reglamento de funcionamiento del Comité de Seguridad.

7.3 Comité de Crisis

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, encargado de tomar las decisiones y coordinar las acciones necesarias para la resolución de los incidentes de seguridad que hayan sido calificados como crisis.

Estará constituido como vocales por los miembros del Comité de Seguridad y el personal directivo de Organización, Recursos Humanos, Servicio Jurídico, Hacienda y Gabinete de Prensa.

Adicionalmente, se podrá requerir la participación de forma consultiva de otros miembros de la organización o personal externo, como personal directivo de otros servicios afectados, los Delegados/as de Seguridad de la infraestructura afectada, los/las responsables de seguridad de proveedores, etc. con voz, pero sin posibilidad de voto.

Las funciones del Comité de Crisis serán las siguientes:

- Comprender el estado de situación y realizar una previsión de escenarios, evaluando toda la información recibida sobre el incidente y realizando una valoración del impacto y consecuencias para el Ayuntamiento.
- Coordinar acciones y tomar decisiones, dando apoyo a los equipos, supervisando la implementación de las medidas adoptadas, y activando en su caso la movilización de recursos.
- Actuar como centro de referencia de información durante la respuesta al incidente y su posterior recuperación, tanto ante los agentes internos como externos.
- Definir la estrategia de comunicación interna y externa. Designar el portavoz y asegurar que se llevan a cabo las medidas de comunicación previamente diseñadas, ya sea en medios, redes sociales, marcos asociativos, etc. Velar por salvaguardar la confianza, la reputación y la imagen.

El Comité de Crisis se deberá reunir con carácter ordinario, al menos, una vez al año para la realización de simulacros, y con carácter extraordinario cuando lo decida su Presidente ante una situación de crisis en la organización según lo definido en el Procedimiento de gestión de crisis.

7.4 Roles de seguridad

La Política de Seguridad, de conformidad con el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, deberá describir los roles o funciones de seguridad y privacidad de la información, 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, protección de datos y protección de infraestructuras críticas:

- Responsable de la Información.
- Responsable del Servicio.
- Responsable de Seguridad de la Información.
- Responsable del Sistema.
- Administrador/a de la Seguridad del Sistema.
- Delegado/a de Protección de Datos.
- Responsable de tratamiento.
- Encargado/a de tratamiento.
- Responsable de Seguridad y Enlace.
- Responsable de Seguridad Física.
- Delegado/as de Seguridad.

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 del Servicio podrán ser asumidos por la misma persona en razón de la materia de su competencia.

7.4.1 Responsable de la Información

Las funciones del Responsable de la Información en el Ayuntamiento de Santa Cruz de Tenerife serán asumidas por la persona titular de la Dirección General de Organización o unidad administrativa equivalente que gestione cada información.

Sus funciones serán las siguientes:

- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad, integridad, trazabilidad y autenticidad.
- Valorar y categorizar el nivel de la información y de los servicios pertenecientes a su sistema de información, según el impacto que tendría un incidente que afectara a la seguridad de la información con perjuicio para las dimensiones de seguridad,

siguiendo el procedimiento y dentro del marco establecido en el Anexo I del Real Decreto 311/2022, por el que se aprueba el Esquema Nacional de Seguridad.

- Determina los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Para lo anterior, podrá recabar una propuesta al Responsable de la Seguridad de la Información y escuchar la opinión del Responsable del Sistema y con asistencia del administrador de seguridad.
- Acepta los niveles de riesgo residual que afecten a la información.
- Propone al Responsable de Seguridad la categoría de su información y/o de su sistema/s de información, dentro de su ámbito competencial.

7.4.2 Responsable del Servicio

Las funciones del Responsable del Servicio en el Ayuntamiento de Santa Cruz de Tenerife serán asumidas por la persona titular de la Dirección General de Organización o unidad administrativa equivalente que gestione cada servicio.

Sus funciones serán las siguientes:

- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- Es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Proponer al responsable de información para su aprobación definitiva: la valoración de su servicio y de la información tratada en el mismo.
- Establece los requisitos de los servicios en materia de seguridad. Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Para lo anterior, podrá recabar una propuesta al Responsable de la Seguridad de la Información y escuchar la opinión del Responsable del Sistema.
- Acepta los niveles de riesgo residual que afecten al servicio.

7.4.3 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 persona titular de la Dirección General de Tecnología.

Este rol dará respuesta a los requisitos legales impuestos por el Esquema Nacional de Seguridad y el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (Reglamento de la transposición de la directiva NIS), unificando la figura de Responsable de Seguridad de la Información del ENS y Responsable de Seguridad de la Información del operador de servicios esenciales. De igual manera existirá un sustituto del Responsable de Seguridad de la Información, que asumirá sus funciones en casos de ausencia, vacante o enfermedad.

Sus funciones serán las siguientes:

- Reportar directamente al Presidente del Comité de Seguridad.

- Convocar al Comité de Seguridad, recopilando la información pertinente.
- Mantener 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.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Recopilar los requisitos de seguridad del Responsable de Información y del Servicio y determinará la categoría del Sistema.
- Realizar el Análisis de Riesgos y el plan de tratamiento de los mismos.
- Elaborar y firmar 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.
- Facilitar 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.
- Coordinar la elaboración de la documentación de seguridad del Sistema.
- Participar en la elaboración de la Política de Seguridad.
- Dirigir la elaboración y aprobación de la normativa de seguridad de la información.
- Elaborar y aprobar los procedimientos operativos de seguridad de la información.
- Facilitar 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).
- Constituir el punto de contacto especializado para la coordinación con el CSIRT (equipo de respuesta a incidentes de seguridad informática) de referencia. Notificar a la autoridad competente sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.
- Dirigir y coordinar la respuesta a los incidentes de seguridad junto a otras unidades del Ayuntamiento.
- Elaborar, junto al Responsable de Sistema, los Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad.
- Elaborar los Planes de Formación y Concienciación del personal en Seguridad de la Información, que someterá a la aprobación del Comité de Seguridad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Validar los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que someterá a la aprobación del Comité de Seguridad, que serán probados periódicamente por el Responsable del Sistema.
- Analizar los informes de auditoría para presentar sus conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.

- Aprobar 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.
- Analizar y propondrá salvaguardas que prevengan incidentes en un futuro, en caso de ocurrencia de incidentes de seguridad de la información.

7.4.4 Responsable del Sistema

Las funciones del Responsable del Sistema de Información del Ayuntamiento de Santa Cruz de Tenerife serán asumidas por el titular de 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.
- 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.
- Realizar las pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
- Elaborar 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.
- Planificar 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.

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 de la Información y el Responsable de Seguridad y Enlace antes de ser ejecutada.

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 del Sistema que delega sus funciones, no responsabilidad.
- 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.

7.4.5 Administradores/as de la Seguridad del Sistema

Las funciones del Administrador/a de la Seguridad del Sistema en el Ayuntamiento de Santa Cruz de Tenerife serán asumidas por el titular de 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:

- Implementar, gestionar y mantener 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.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- 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.

7.4.6 Delegado/a de Protección de Datos

El/la Delegado/a 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.

En particular, el/la Delegado/a de Protección de Datos del Ayuntamiento de Santa Cruz de Tenerife asesorará al responsable o el/la encargado/a del tratamiento en la realización de un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

Sus funciones serán las siguientes:

- Informar y asesorar al responsable o al encargado/a del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras normas o disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en la normativa de protección de datos y de las políticas del Responsable o del encargado/a del tratamiento, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo aplicable del RGPD.
- Cooperar con la Autoridad de Control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 RGPD y realizar consultas, en su caso, sobre cualquier otro asunto.

7.4.7 Responsables de tratamiento

Se trata de la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

En el caso de los datos de carácter personal tratados para atender las solicitudes y consultas realizadas a través de la sede electrónica, la gestión de solicitudes, reclamaciones, quejas y sugerencias y en general realizar cualquier trámite y prestar los servicios municipales y competencias propias, el responsable del tratamiento es el propio Ayuntamiento de Santa Cruz de Tenerife, como así se refleja en su Política de Privacidad.

Entre sus funciones se encuentran:

- Determinar los fines y medios del tratamiento.
- Decidir y aplicar las medidas técnicas y organizativas de seguridad adecuadas a los tratamientos de datos que se encuentren bajo su responsabilidad.
- Realizar los correspondientes análisis de riesgos y evaluaciones de impacto cuando sean necesarios de acuerdo con el RGPD, y con carácter general desempeña el resto de las funciones que le asigne la normativa de protección de dato.
- Desarrollar la actualización del registro de actividades de tratamiento.

7.4.8 Encargados de tratamiento

El encargado/a de tratamiento será aquella persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable del Tratamiento.

Las empresas concesionarias que realicen tratamiento de datos personales en virtud de una prestación de servicios contratada con el Ayuntamiento de Santa Cruz de Tenerife, tendrán la consideración de encargadas del tratamiento.

Los encargados de tratamiento tendrán las siguientes funciones:

- Asistir al responsable del tratamiento, teniendo cuenta la naturaleza del tratamiento, para el cumplimiento de las medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de las personas interesadas.
- Ayudar a la persona responsable del tratamiento a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del RGPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición de la persona encargada de tratamiento.
- A elección de la persona responsable del tratamiento, suprimir o devolver todos los datos personales una vez finaliza la prestación de los servicios de tratamiento, y suprime las copias existentes, a menos que se requiera la conservación de los datos personales.
- Poner a disposición de la persona responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones.
- Informar inmediatamente a la persona responsable del tratamiento si de acuerdo a su criterio, una instrucción o actividad infringe cualquier disposición en materia de protección de datos.
- Cuando un encargado del tratamiento recurra a otro para tratar datos por cuenta del

Responsable, se impondrá a este subencargado, mediante acto jurídico, las mismas obligaciones que las estipuladas entre el Responsable y el encargado principal. En caso de incumplimiento del subencargado, el encargado principal responderá ante el Responsable de los perjuicios causados.

7.4.9 Responsable de Seguridad y Enlace

El Ayuntamiento de Santa Cruz de Tenerife, de acuerdo con los requerimientos del CNPIC para el cumplimiento de la Ley de Protección de infraestructuras críticas, ha designado y comunicado oficialmente un Responsable de Seguridad y Enlace y un sustituto del mismo, que será el encargado de liderar las iniciativas de seguridad integral destinadas a proteger las infraestructuras críticas.

El Responsable de Seguridad y Enlace deberá estar habilitado por el Ministerio del Interior como Director de Seguridad, en virtud de lo dispuesto en el Reglamento de Seguridad Privada vigente.

Sus funciones serán las siguientes:

- Representar al operador crítico ante la Secretaría de Estado de Seguridad:
  - En materia relativas a la seguridad de sus infraestructuras.
  - En materia relacionada con los diferentes planes especificados en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Impulsar los planes de seguridad y planes de protección, que garanticen la protección de la actividad, personas, bienes e información, así como medidas y procedimientos de actuación en materia de seguridad de infraestructuras críticas.
- Impulsar el desarrollo de la normativa aplicable en el ámbito de infraestructuras críticas.
- Evolucionar de las situaciones de riesgo que puedan afectar a la actividad de la organización, sistemas de información e integridad de las personas, así como participar en la resolución de incidentes de seguridad y situaciones de crisis.
- Canalizar las necesidades operativas e informativas que surjan.

7.4.10 Delegados/as de Seguridad

El cumplimiento de la Ley de Protección de infraestructuras críticas requiere la designación de un Delegado/a de Seguridad y un sustituto para cada una de las infraestructuras críticas designadas. Las funciones de Delegado/a de Seguridad en el Ayuntamiento de Santa Cruz de Tenerife serán asumidas por la persona titular designada por el Ayuntamiento.

Sus funciones serán las siguientes:

- Ser el enlace operativo y el canal de información con las autoridades competentes en materias relativas a la seguridad de sus infraestructuras.
- Participar en la realización del análisis de riesgo que puedan afectar a la actividad del Ayuntamiento de Santa Cruz de Tenerife, sistemas de información e integridad de las personas y en la gestión de incidentes de seguridad dentro su infraestructura crítica.

- Participar en la elaboración de los planes de seguridad y planes de protección, que garanticen la protección de la actividad, personas, bienes e información.
- Participar en el desarrollo de la normativa aplicable en el ámbito de infraestructuras críticas.
- Canalizar las necesidades operativas e informativas que surjan.

7.4.11 Responsable de seguridad física

Las funciones del Responsable de seguridad física en el Ayuntamiento de Santa Cruz de Tenerife serán asumidas por la persona titular de la Dirección General de Organización.

Sus funciones serán las siguientes:

- El seguimiento y control de los contratos de seguridad en las dependencias y en eventos municipales.
- Coordinar las acciones y toma de decisiones en materia de seguridad física y seguridad de los equipos (control de accesos, incendios, climatización, alimentación eléctrica, alarmas, CCTV, etc.).

7.5 Jerarquía 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 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.

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

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

El Responsable de la Seguridad de la Información informará, asimismo, al Responsable de la Información y del Servicio y al Delegado/a de Protección de Datos de los incidentes relativos a la información y al servicio, así como de las decisiones en materia de seguridad y privacidad 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 la Información 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.

El Responsable de Seguridad y Enlace informará la Comité de Seguridad de cualquier cuestión relativa a la seguridad de sus infraestructuras críticas.

El Responsable de Seguridad Física y/o los Delegados/as de Seguridad informarán la Comité de Seguridad de cualquier cuestión relativa a la seguridad física.

En caso de discrepancia en la toma de decisiones entre el Responsable de Seguridad de la Información y el Responsable del Sistema, existiendo dependencia jerárquica entre ambos, la decisión final será adoptada por el Comité de Seguridad, como medida compensatoria para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y el artículo 7 apartado 4.d de Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, garantizando así una solución imparcial y alineada con los objetivos de seguridad de la Organización.

8. 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 estos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas técnicas, organizativas y legales necesarias para el cumplimiento de la normativa vigente en materia de protección de datos. Es decir, tratará la información y los datos personales bajo su responsabilidad conforme a los principios de protección de datos, enumerados en el artículo 5 del Reglamento (UE) 2016/679:

- Licitud, lealtad y transparencia: Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.
- Limitación de la finalidad: Los datos personales serán recogidos para cumplir exclusivamente con las finalidades determinadas. El tratamiento ulterior con fines de archivo de interés público, o fines estadísticos, no se considerará incompatible con las mismas.
- Minimización de datos: Los datos tratados deberán ser adecuados, pertinentes y limitados lo necesario en relación con los fines para los que son tratados.
- Exactitud: Los datos deberán ser exactos y, si fuera necesario, actualizados.
- Limitación del plazo de conservación: Los datos se almacenarán de forma que se permita la identificación de los interesados durante el tiempo necesario para el cumplimiento de la finalidad. Tras esto solo podrán conservarse para fines de archivo en interés público o fines estadísticos.
- Integridad y confidencialidad: Los datos deberán ser tratados de forma que se garantice una seguridad adecuada de los mismos en todas sus dimensiones.

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.

9. GESTIÓN DE RIESGOS

9.1 Justificación

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

Todo sistema de información y activo que soporte servicios esenciales del Ayuntamiento de Santa Cruz sujeto a esta Política deberá contar con un análisis de riesgos debidamente actualizado, que identifique las amenazas y evalúe los riesgos a los que este expuesto.

El análisis de riesgos será la base para determinar las medidas de seguridad a implantar según lo previsto en el Artículo 7 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y lo establecido en la legislación de servicios esenciales e infraestructuras críticas.

9.2 Evaluación de riesgos

Para la aceptación de los niveles de riesgo, el Comité de Seguridad del Ayuntamiento de Santa Cruz establecerá y cuantificará 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 gestionarse, al menos, 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, aquellos que puedan provocar el incumplimiento de una regulación, cuyo impacto se haya apreciado como grave o muy grave.

9.3 Gestión de riesgos

La gestión de los riesgos de todo sistema de información y activo que soporte servicios esenciales del Ayuntamiento de Santa Cruz sujeto a esta Política permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables.

La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos físicos y lógicos a los que estén expuestos.

Cuando se utilicen sistemas de información suministrados por terceros, estos deberán proporcionar el análisis y la gestión de los riesgos que seguirá el mismo proceso de aceptación de los niveles de riesgo, el Comité de Seguridad del Ayuntamiento de Santa Cruz.

9.4 Recursos para el tratamiento de riesgos

El Comité de Seguridad del Ayuntamiento de Santa Cruz evaluará y gestionará la asignación de recursos personales y materiales para atender a las necesidades del análisis y gestión de riesgos de los sistemas de información sujetos a esta Política, promoviendo el uso de

herramientas especializadas y la asignación de profesionales competentes que garantice el rigor y la homogeneidad de los informes de riesgos realizados.

9.5 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 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad 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 para su revisión y aprobación, en su caso.

Los niveles de riesgo residual respecto a las infraestructuras críticas, serán presentados por el Responsable de Seguridad y Enlace al Comité de Seguridad para su revisión y aprobación.

9.6 Actualización de las evaluaciones de riesgos

El análisis de los riesgos y su tratamiento, según lo establecido en el Artículo 7 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, deberán ser actualizados 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 detecten actividades o comportamientos anómalos.
- Cuando se reporten vulnerabilidades graves.
- Cuando el Nivel de Alerta de Infraestructuras Críticas (NAIC) cambie y así lo estime la Autoridad Competente.

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

10.1 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 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, 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.
- Evaluar permanente del estado de la seguridad de los activos para detectar vulnerabilidades e identificar deficiencias de configuración.
- Reevaluar y actualizar periódicamente las medidas de seguridad, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.
- Revisar periódicamente por terceros con el fin de obtener una evaluación independiente.

10.2 Monitorización continua 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 10 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

La monitorización es especialmente relevante cuando se establecen líneas de defensa, de acuerdo con el Artículo 9 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

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.

10.3 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 actuarán 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 tal y como se establece en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Notificar e intercambiar la información necesaria con el CCN-CERT relacionada con los incidentes de peligrosidad o impacto: alto, muy alto o crítico tal y como se establece en la legislación citada en el punto anterior. Dicha comunicación debe recoger los contenidos mínimos indicados en la guía nacional de notificación de incidentes del Gobierno de España y enviarse en los plazos indicados en la legislación de aplicación.
- 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 tal y como se indica en el Procedimiento de gestión de brechas de seguridad de datos personales.

- Notificar los incidentes de seguridad física de las infraestructuras críticas al CSIRT de referencia, que a su vez informarán a los Cuerpos y Fuerzas de Seguridad del Estado.
- Las consultas con otras autoridades con competencia en materia de seguridad pública y seguridad ciudadana, previstas en Real Decreto-ley 12/2018, de 7 de septiembre, se realizarán a través de la Oficina de Coordinación de Ciberseguridad (OCC).

10.4 Recuperación y planes de continuidad

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

11. OBLIGACIONES DEL PERSONAL

Las personas empleadas públicas del Ayuntamiento de Santa Cruz de Tenerife y de sus entidades públicas vinculadas o dependientes deberán seguir lo dispuesto en la presente Política de Seguridad, así como por la normativa que la desarrolla, siendo responsabilidad del Comité de Seguridad gestionar los medios y llevar a cabo las actuaciones necesarias para que su difusión.

Toda persona empleada pública del Ayuntamiento de Santa Cruz de Tenerife asistirá, al menos, a una sesión anual de formación y concienciación en materia de seguridad de la información y protección de datos personales.

Al inicio del empleo, se impartirán las acciones formativas necesarias para tener conocimiento de la presente Política de Seguridad, así como por la normativa que la desarrolla y durante el empleo se llevarán a cabo acciones planificadas para mantener actualizados de concienciación y formación en materia de seguridad y privacidad de la información, de acuerdo con un plan de concienciación y formación continua.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información y comunicaciones recibirán una 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 aplica, asimismo, al personal externo que lleve a cabo actividades competencia del Ayuntamiento de Santa Cruz de Tenerife, y su eventual incumplimiento podrá constituir una infracción grave o muy grave de conformidad con la normativa laboral.

12. MEJORA CONTINUA

El proceso integral de seguridad implantado por el Ayuntamiento de Santa Cruz de Tenerife deberá ser actualizado y mejorado de forma continua.

Para ello, el Comité de Seguridad supervisará la aplicación de los criterios, normas y metodologías reconocidas nacional y/o internacionalmente para la gestión de los procesos de seguridad y privacidad de la información.

El Comité de Seguridad, asimismo, incentivará la participación de las personas empleadas públicas, así como de los usuarios finales (ciudadanía, autónomos, empresas, etc.) de los sistemas de información en la mejora de las medidas de seguridad de la información manejada en los procedimientos administrativos de su competencia.

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

13. TERCERAS PARTES

Cuando otras organizaciones presten servicios al Ayuntamiento de Santa Cruz de Tenerife, se les remitirá la presente Política de Seguridad y la normativa que la desarrolla que les sea de aplicación.

Así mismo, se les solicitará la designación de un Punto o Persona de Contacto (POC) para la seguridad de la información tratada y el servicio prestado, que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito del servicio prestado, de conformidad con el Artículo 13 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional 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 en materia de protección de datos personales, 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 y privacidad de la 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 el Comité de Seguridad, en caso de que el nivel de riesgo este por encima del aceptable, antes de seguir adelante.

14. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad será revisada por el Comité de Seguridad 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 deberán ser aprobados por la Junta de Gobierno de la Ciudad, de acuerdo con el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

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

15. POLÍTICAS RELACIONADAS

Esta Política de Seguridad 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.

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 física o lógica.

Información: Todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.

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

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

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

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

Responsable de Seguridad y Enlace: persona responsable de las funciones de enlace entre el Ayuntamiento y las autoridades competentes, así como lo referente a las infraestructuras críticas (Coordinación, impulso, planes de seguridad).

Delegado de Seguridad: persona responsable de participar en la elaboración de los Planes de Seguridad y Planes de Protección, que garanticen la protección de la actividad, personas, bienes e información.

Responsable de Seguridad Física: persona responsable de coordinar las acciones y toma de decisiones en materia de seguridad física y seguridad de los equipos (control de accesos, incendios, climatización, alimentación eléctrica, alarmas, CCTV, etc.).

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.

Infraestructuras Críticas: Infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Servicio Esencial: Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.””

La Junta de Gobierno de la Ciudad de Santa Cruz de Tenerife 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 Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, aprobado por Real Decreto 2568/1986, de 28 de noviembre, 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 - 29/10/2024 1:00:26

GLADIS DE LEON LEON - Concejala - 28/10/2024 19:46:46