LA OROTAVA

ANUNCIO

6332 **192627**

Por el Alcalde-Presidente en fecha 3 de diciembre de 2021, se dictó resolución 2021-10525, de 3 de diciembre de 202 resolviendo Aprobar la Política de Seguridad de la Información, codificado con la siguiente identificación "ENS.PO.SEG.00-Política de Seguridad de la Información-rev 1.0", del Ayuntamiento de la Villa de La Orotava.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Índice.

10. Formación y concienciación.

11. Deber de colaboración en la implantación.

12. Publicidad y entrada en vigor.

1. Introducción.

El marco de relación entre las administraciones públicas y los ciudadanos a través de los medios electrónicos se encuentra establecido por las leyes 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas y la 40/2015 de Régimen Jurídico del Sector Público.

Dicho marco de relación se establece a través de la Administración Electrónica, compuesta principalmente tanto por los sistemas de tecnologías de la información y comunicaciones destinados a este fin, como por el tratamiento y almacenamiento automatizado de la información que reside en los mismos.

La Administración Electrónica debe ser confiable para que los ciudadanos realicen los trámites administrativos correspondientes a través de la misma con total seguridad y fiabilidad. Para ello, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, determinado por el artículo 156 de la Ley 40/2015, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Mediante 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, se establecen cuatro grandes objetivos: mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica.

La Política de Seguridad de la Información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el Real Decreto 3/2010, de 8 de enero.

Del mismo modo, determina que la Política de Seguridad de la Información debe ser coherente con lo establecido en la normativa de RGPD y LOPDGGD de protección de datos de carácter personal.

1.1. Objeto y ámbito de aplicación.

1. Constituye el objeto de la presente, la aprobación de la Política de Seguridad de la Información en el ámbito de la Administración Electrónica del Ayuntamiento de La Orotava, así como del marco organizativo y tecnológico de la misma.

2. La Política de Seguridad de la Información será de obligado cumplimiento para todos los departamentos del Ayuntamiento de La Orotava, siendo aplicable a los activos empleados en la prestación de los servicios de la Administración Electrónica.

3. La Política de Seguridad de la Información será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada, con independencia de cuál sea su destino, adscripción o relación con el mismo.

2. Alcance.

Esta Política será de aplicación y de obligado cumplimiento para todo el Ayuntamiento de La Orotava, a sus recursos y a los procesos afectados por el ENS, el RGPD y la legislación derivada, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

3. Marco legal y regulatorio.

El marco normativo en que se desarrollan las actividades del Ayuntamiento de La Orotava en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone, sin carácter exhaustivo, de:

- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Ley 6/2020, de 11 de noviembre, reguladora de los servicios electrónicos de confianza.

- Real Decreto 2/2004, de 5 de marzo, por el que

se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales.

- 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.

- 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.

- 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.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

- Ley 19/2013, de 9 de diciembre de transparencia, acceso a la información pública y buen gobierno.

- Ley 12/2014, de 26 de diciembre, de transparencia y de acceso a la información pública en la Comunidad Autónoma de Canarias.

- Ley 27/2013, de 27 de diciembre, de Racionalización y Sostenibilidad de la Administración Local.

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- Real Decreto-ley 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.

- Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.

- 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-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

- 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.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- 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.

- Ordenanza Reguladora de la Administración Electrónica del Excmo. Ayuntamiento de La Orotava.

Del mismo modo, forman parte del marco regulatorio las normas aplicables a la Administración Electrónica del Ayuntamiento que desarrollen o complementen las anteriores y que se encuentren dentro del ámbito de aplicación de la Política de Seguridad de la Información, particularmente aquellas dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados por la Corporación igualmente en el ejercicio de sus competencias.

4. Revisión de la Política.

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la misma.

La política será propuesta y revisada por el Comité de Seguridad de la Información, aprobada por el representante legal de la corporación y difundida para que la conozcan todas las partes afectadas.

5. Principios de la seguridad de la información.

5.1. Principios básicos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los

niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un todo coherente y eficaz.

b) Responsabilidad diferenciada: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del área/servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

c) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

e) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

g) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

5.2. Principios particulares y responsabilidades específicas.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales y que garantizan el cumplimiento de los principios básicos de la Política de Seguridad de la Información. Se establecen los siguientes:

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

b) Gestión de activos de información: Los activos de información del Ayuntamiento se encontrarán inventariados y categorizados y estarán asociados a un responsable.

c) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas y ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar

su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

6. Estructura organizativa.

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información del Ayuntamiento de La Orotava son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales.

Para una mejor respuesta a incidentes de seguridad, el Ayuntamiento de La Orotava mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

En particular, la gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y Comités con funciones concretas, definidas y documentadas.

6.1. Funciones y responsabilidades

A continuación, se identifican y se detallan las atribuciones de cada responsable, así como los mecanismos de coordinación y resolución de conflictos.

6.1.1. Representante legal

En materia de seguridad de la información, el representante legal del Ayuntamiento de La Orotava tiene las siguientes funciones:

- Aprobar la Política de Seguridad de la Información del Ayuntamiento de La Orotava y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento de los Esquemas Nacionales de Seguridad e Interoperabilidad y las normativas de Protección de Datos.

- Aprobar el desarrollo normativo propuesto por el Comité de Seguridad de la Información.

- Nombramiento y cese de los integrantes del Comité de Seguridad de la Información.

- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta del Comité de Seguridad de la Información.

6.1.2. Comité de Seguridad de la Información.

El Comité de Seguridad de la Información asumirá las competencias en materia de seguridad de la información, y en concreto:

- Elaborar y proponer la Política de Seguridad de la Información del Ayuntamiento de La Orotava, para su posterior aprobación.

- Elaborar y proponer la normativa de seguridad para el cumplimiento de los Esquemas Nacionales de Seguridad e Interoperabilidad y las normativas de Protección de Datos.

- Velar por que la seguridad de la información sea parte del proceso de planificación del Ayuntamiento de La Orotava.

El comité tiene las siguientes funciones:

- Atender las inquietudes del representante legal de la entidad y de los diferentes departamentos.

- Informar regularmente del estado de la seguridad de la información al representante legal del Ayuntamiento.

- Promover la mejora continua del sistema de gestión de la seguridad de la información.

- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación.

- Elaborar la Normativa de Seguridad de la información.

- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.

- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.

- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.

- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos 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 TIC.

- 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.

El Comité de Seguridad de la Información estará compuesto por:

- Presidente: Responsable de la Información.

- Secretario: Responsable de la Seguridad.

- Vocal: Responsable del Área de Recursos Humanos.

- Vocal: Responsable del Sistema.

- Vocal: Administrador de la Seguridad del Sistema.

Roles acordes a lo establecido en la Guía de Seguridad (CCN-STIC-801) por la que se regulan las responsabilidades y funciones en el Esquema Nacional de Seguridad.

7. Gestión de los riesgos.

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).

- Cuando ocurra un incidente grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

El nivel de riesgo máximo aceptable se establecerá en base a la metodología elegida, en este caso Magerit. El nivel máximo de riesgo aceptable se utilizará como objetivo de mejora en los planes de mitigación de riesgo que se desarrollen.

8. Desarrollo de la Política de Seguridad de la Información.

8.1. Instrumentos de desarrollo.

La Política de Seguridad de la Información del Ayuntamiento de La Orotava se complementará por medio de instrucciones de servicio y circulares que afronten aspectos específicos. Dichas instrucciones y circulares podrán adoptar alguna de las siguientes modalidades:

Se usarán los siguientes instrumentos:

- Normas técnicas de seguridad: Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

- Guías de seguridad: Tienen un carácter informativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos en los casos en los que no existan procedimientos precisos. Ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

- Procedimientos operativos de seguridad (POS): Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.

- Instrucciones técnicas (IT): Desarrollan los POS llegando al máximo nivel de detalle, indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas.

La normativa técnica de seguridad estará disponible en la Intranet, a disposición de todos los miembros del Ayuntamiento de La Orotava que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

8.2. Aprobación de las normas de seguridad.

La aprobación de las normas técnicas de seguridad se hará a propuesta del Comité de Seguridad de la Información, por el representante legal del Ayuntamiento de La Orotava.

8.3. Sanciones previstas por incumplimiento.

Del incumplimiento de la Política de Seguridad de la Información y normas que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la normativa sobre régimen disciplinario de los empleados públicos, así como, en su caso, a lo prevenido en el Acuerdo de Funcionarios y Convenio Colectivo vigentes en cada momento.

9. Protección de datos de carácter personal.

Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ayuntamiento de La Orotava las medidas de seguridad determinadas en las siguientes normativas:

- Anexo II del 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.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (GDPR).

- Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

10. Formación y concienciación.

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Ayuntamiento de La Orotava, así como a la difusión entre los mismos de la Política de Seguridad de la Información y de su desarrollo normativo.

2. Comité de Seguridad de la Información se encargarán de promover las actividades de formación y concienciación en materia de seguridad.

11. Deber de colaboración en la implantación.

Todos los órganos y unidades del Ayuntamiento de La Orotava prestarán su colaboración en las actuaciones de implementación de esta Política de Seguridad de la Información.

12. Publicidad y entrada en vigor.

La presente entrará en vigor el día siguiente de su publicación en el Boletín Oficial de la Provincia. Se dará publicidad en el Tablón de Anuncios Electrónico, Web corporativa municipal, así como en la Intranet Municipal.

En La Orotava, a nueve de diciembre de dos mil veintiuno.

EL ALCALDE-PRESIDENTE, Francisco Linares García.

LA SECRETARIA ACCIDENTAL GENERAL, Pino María González Sánchez.