sobre su denegación no serán susceptibles de recurso […]". De igual modo, indica el artículo 35 de la mencionada Ley, que "[…] serán motivados con sucinta referencia de hechos y fundamentos de derecho: […] e) los acuerdos de aplicación de la tramitación de urgencia, de ampliación de plazos y de realización de actuaciones complementarias".

SEXTO. De conformidad con lo establecido en la de Ordenanza Específica, del Excmo. Cabildo Insular de Fuerteventura, reguladora de las bases generales que han de regir la concesión de subvenciones, en régimen de concurrencia competitiva, destinadas a autónomos y pymes de la isla de Fuerteventura, al objeto de consolidar el tejido productivo esencial insular, aprobadas en sesión plenaria de fecha 30 de julio de 2021, publicada en el B.O.P. número 94, de fecha 6 de agosto de 2021, le corresponde a la Consejera de Área Insular con competencias en materia de Promoción Económica iniciar el procedimiento mediante convocatoria pública en el Boletín Oficial de la Provincia de Las Palmas.

SÉPTIMO. En virtud de lo establecido en el artículo 172 y 175 del Real Decreto 2568/1986 de 28 de noviembre, Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales, y del artículo 48 del Reglamento Orgánico del Cabildo de Fuerteventura, aprobado en sesión plenaria el 25 de Octubre de 2019 y el Decreto de la Presidencia número 1.183, de 12 de marzo de 2021 de desconcentración de competencias, modificado por el Decreto de la Presidencia número 1.233, de fecha 19 de marzo de 2021, por los que se nombra a doña Dolores Alicia García Martínez, Consejera del Área Insular de Presidencia, Planificación, Hacienda, Promoción Económica y Gestión Medioambiental.

PROPONGO

PRIMERO. Ampliar en TRES (3) MESES el plazo de resolución y notificación del procedimiento recogido en la convocatoria pública de subvenciones, en régimen de concurrencia competitiva, destinadas a autónomos y pymes de la isla de Fuerteventura, contados a partir del día siguiente a la finalización del plazo inicial, según lo establecido en la base sexta de la convocatoria.

SEGUNDO. Publicar la resolución adoptada mediante anuncio en el Boletín Oficial de la Provincia de Las Palmas.

Contra la presente resolución no cabe recurso alguno, de conformidad con establecido en el artículo 23.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Así lo manda y firma la Consejera de Área Insular del Cabildo de Fuerteventura.

En Puerto del Rosario, a treinta de marzo de dos mil veintidós.

LA CONSEJERA DE ÁREA INSULAR DE PRESIDENCIA, ECONOMÍA, HACIENDA, PROMOCIÓN ECONÓMICA Y SOSTENIBILIDAD MEDIOAMBIENTAL, Dolores Alicia García Martínez.

LA SECRETARIA TÉCNICA ACCIDENTAL DEL CONSEJO DE GOBIERNO INSULAR, María del Pino Sánchez Sosa.

114.462

EXCMO. CABILDO INSULAR DE GRAN CANARIA

Consejería de Función Pública y Nuevas Tecnologías

Servicio de Tecnologías de la Información y Administración Electrónica

ANUNCIO

796

La Sra. Consejera de Área de Función Pública y Nuevas Tecnologías del Cabildo Insular de Gran Canaria, con fecha 28 de marzo de 2022, ha tenido a bien dictar la Resolución del Servicio de Tecnologías de la Información y Administración Electrónica número 20/22, relativa a la resolución de aprobación de la política de seguridad de la información del Cabildo de Gran Canaria, cuyo tenor literal a continuación se expresa:

Visto que el artículo 42.2 de la antigua Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (derogada por la disposición derogatoria única 2.b) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas), dispuso la creación del vigente Esquema Nacional de Seguridad, lo cual tuvo

lugar por medio del Real Decreto 3/2010, de 8 de enero, por el que se regula el vigente Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en lo sucesivo, R.D. 3/2010), y que está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información; dichos principios deberán ser aplicados por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Visto que el Esquema Nacional de Seguridad 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 al conocimiento de personas no autorizadas.

Visto lo dispuesto en el artículo 11 del R.D. 3/2010, referente a que "todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos.

h) Seguridad por defecto.

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 actividad.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad".

Vista la vigencia de la Resolución del Servicio de Tecnologías de la Información y Administración Electrónica número 35/17[1], de 29 de agosto de 2017, por el que se aprobó la política de seguridad de la información del Cabildo de Gran Canaria (Boletín Oficial de la Provincia de Las Palmas, número 109, de 11 de septiembre de 2017).

1

http://verifirma.grancanaria.com/verifirma/code/RqVhGxZms/xDrD+I+fF9Gg==

RESULTANDO que los artículos 10, 15 y 16.1.c) del vigente Reglamento de Gobierno y Administración del Excelentísimo Cabildo Insular de Gran Canaria (Boletín Oficial de la Provincia de Las Palmas, número 148, lunes 9 de diciembre de 2016), dotan a la Presidencia de la Corporación, como órgano superior, de la potestad de establecer las directrices generales de la acción de gobierno insular y asegurar su continuidad. En consonancia con lo establecido en el dispositivo segundo, apartado cuarto, del Decreto número 42/19, de 24/07/19, de delegación de competencias del Sr. Presidente en los Consejeros, en cuanto al dictado de instrucciones para dirigir la acción de los órganos insulares en su ámbito competencial, y en cumplimiento de los dispuesto en el artículo 131 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en relación a la publicidad de las disposiciones administrativas.

Por todo ello, RESUELVO:

Primero: APROBAR el documento que figura a continuación en todos y cada uno de los puntos que en el mismo se contemplan.

Segundo: Por la presente, se deroga la Resolución del Servicio de Tecnologías de la Información y Administración Electrónica número 35/17, de 29 de

agosto de 2017, por la que se aprueba la política de Seguridad de la Información del Cabildo de Gran Canaria.

Tercero: La presente resolución entrará en vigor el día siguiente de su publicación en el Boletín Oficial de la Provincia de Las Palmas.

Dado por la Consejera de Área de Función Pública y Nuevas Tecnologías, en Las Palmas de Gran Canaria, a fecha de firma electrónica, de todo lo cual, como Titular del Órgano de Apoyo al Consejo de Gobierno Insular, y en ejecución de lo previsto en la Disposición Adicional Octava d) de la Ley 7/1985 de 2 de abril, reguladora de las Bases de Régimen Local, modificada por la Ley 57/2003, de 16 de diciembre, doy fe.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Clasificación de la Información:

Tipo: Información de uso público.

Ámbito de Difusión: Todos los empleados y colaboradores externos de CGC.

Responsable: Responsable de Seguridad de la Información de CGC.

1. Aprobación y entrada en vigor.

La Política de Seguridad de la Información, en adelante, PSI, será aprobada mediante resolución de la persona titular del órgano superior con competencias en la gestión de la seguridad de la información del Cabildo de Gran Canaria (en adelante, CGC). Esta PSI, será efectiva desde la fecha de aprobación y hasta que sea reemplazada por una nueva política.

El CGC dispondrá de los medios para publicar, dar a conocer y facilitar el cumplimiento de esta política y de los documentos que la desarrollan, así como para verificar su aplicación y efectividad. Asimismo, habilitará canales de participación que permitan, a los destinatarios de esta política y de los documentos complementarios, participar en su revisión y mejora.

2. Introducción.

La información constituye un activo de primer orden para el CGC desde el momento en que resulta esencial para la prestación de gran parte de los servicios. Por otro lado, las tecnologías de la información y las comunicaciones se han hecho cada vez más necesarias para las administraciones públicas. Sin embargo, las indiscutibles mejoras que aportan al tratamiento de la información vienen acompañadas de nuevos riesgos y, por lo tanto, es necesario introducir medidas específicas para proteger tanto la información como los servicios que dependan de ella.

La seguridad de la información tiene como objetivo proteger la información y los servicios reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable. Dentro de cada organización sólo sus máximos directivos tienen las competencias necesarias para fijar dicho nivel, ordenar las actuaciones y habilitar los medios para llevarlas a cabo. En este sentido, establecer una PSI, y hacer el subsiguiente reparto de tareas y responsabilidades, son actuaciones prioritarias, puesto que son los dos instrumentos principales para el gobierno de la seguridad y constituyen el marco de referencia para todas las actuaciones posteriores.

La presente PSI se elabora en cumplimiento de la exigencia del 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, que en sus artículos 4 y 11 establece la obligación para las Administraciones Públicas de disponer de una PSI e indica los requisitos mínimos que debe cumplir y los principios básicos de seguridad que han de regirla.

Esta PSI sigue también las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional (CCN), centro adscrito al Centro Nacional de Inteligencia (CNI).

La finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La adaptación al ENS implica que el CGC y su personal deben aplicar las medidas mínimas de seguridad exigidas por el propio ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades

reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes unidades de gestión del CGC deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y los costes asociados deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos del área de tecnología de la información y comunicación.

Las unidades de gestión del CGC deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS y siempre en función de la categorización que se haga de los sistemas conforme al anexo I del ENS.

3. Ámbito de aplicación.

El ámbito de aplicación del presente documento está constituido por:

- La información, que será la tratada por los sistemas de información, es decir, toda la información que utilizan, custodian o generan los cargos, personal propio, externo o colaboradores del CGC, tanto en soportes magnéticos, como ópticos, papel o cualquier otro soporte; bien resida en sus puestos de trabajo de forma local, como en servidores multiusuario, estén estos o no en instalaciones propias.

- Los sistemas de información del CGC, considerando todos los componentes necesarios para el correcto funcionamiento de los mismos, así como los propios componentes hardware y software que los componen.

- Los procesos organizativos referentes al uso e implantación de los sistemas de información que afectarán a los miembros del CGC.

- Las personas afectadas por la presente PSI, que serán:

*Personal del CGC, sea electo, directivo, eventual, funcionario o laboral que haga uso de los sistemas de información.

*Personal externo perteneciente a otras entidades del que, en virtud de relaciones especiales, como contratos de servicios, de asistencia técnica y de asesoramiento, entre otras, hagan uso de los sistemas de información CGC.

*Personal que desarrolle alguna función que afecte a los sistemas de información, como las personas que se ocupan del mantenimiento de las áreas seguras.

*En general, cualquier otra persona con algún tipo de vinculación con el CGC y que utilice o posea acceso a sus sistemas de información.

Por ello, la presente PSI debe ser conocida y aplicada por todo el personal aquí reflejado, y su cumplimiento debe considerarse obligatorio para todo el personal implicado.

4. Marco normativo.

4.1. Marco normativo general.

El marco general del régimen jurídico del CGC se encuentra recogido y publicado en el apartado "Marco jurídico" de la web institucional del CGC accesible mediante la dirección electrónica http://cabildo.grancanaria.com/ y se resume a continuación:

*Normativa Estatal:

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

- Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.

- Real Decreto Legislativo 781/1986, de 18 de abril, por el que se aprueba el Texto Refundido de las Disposiciones Legales vigentes en materia de Régimen Local.

- Ley 57/2003, de 16 de diciembre, de medidas para la modernización del Gobierno Local.

- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

- Ley 9/2017, de 8 de noviembre, de Contratos del

Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

*Normativa Autonómica:

- Ley Orgánica 1/2018, de 5 de noviembre, de reforma del Estatuto de Autonomía de Canarias.

- Ley 14/1990, de 26 de julio, de Reforma de la Ley 8/1986, de 18 de noviembre, de Régimen Jurídico de las Administraciones Públicas de Canarias.

- Ley 8/2015, de 1 de abril, de Cabildos Insulares.

*Normativa propia del CGC:

- Reglamento de Organización y Funcionamiento del Pleno y sus Comisiones del Excmo. Cabildo Insular de Gran Canaria.

- Reglamento Orgánico de Gobierno y Administración del CGC.

- Reglamento regulador de la Información y Atención al Ciudadano en el CGC.

- Reglamento regulador del funcionamiento del proceso de sugerencias y reclamaciones en el CGC.

- Reglamento de la Relación de Puestos de Trabajo (RPT).

- Reglamento Orgánico por el que se crea el Tribunal Administrativo del CGC sobre Contratos Públicos.

4.2. Marco normativo de la Administración Electrónica.

El marco del régimen jurídico del CGC en el ámbito de la Administración Electrónica se encuentra recogido y publicado en el apartado "Normativa" de la Sede Electrónica del CGC que puede ser consultada en la dirección electrónica https://sede.grancanaria.com/ y se resume a continuación:

*Normativa reguladora general:

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- 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 3/2010, de 8 de enero, por el que se regula el ENS 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.

- 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).

- 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.

*Normativa reguladora específica:

- Creación de la Sede Electrónica del CGC, aprobada en la sesión de Pleno del 3 de octubre de 2014 (Boletín Oficial de la Provincia de Las Palmas, número 137, 24/10/2014).

- Ordenanza reguladora de la creación del Registro Electrónico del CGC, aprobada en la sesión de Pleno del 28 de noviembre de 2014 (Boletín Oficial de la Provincia de Las Palmas, número 13, 28/01/2015).

5. Organización de la seguridad.

A nivel organizativo, el desempeño de la seguridad CGC se estructurará en tres niveles:

- Estructura de especificación, que es la que se encarga de establecer los requisitos de seguridad asociados a los servicios prestados.

- Estructura de supervisión, que es la que se encarga

de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continuo con los objetivos de la organización.

- Estructura de operación, que se encarga de implantar las medidas de seguridad identificadas.

5.1. Estructura de especificación.

Esta estructura es la encargada de determinar los requisitos de seguridad que serán de aplicación a los servicios prestados por el CGC y a garantizar el cumplimiento normativo asociado que le es de aplicación, en concreto el Real Decreto 3/2010 de 8 de enero por el que se regula el ENS y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Se describen a continuación las funciones y responsabilidades de los roles asociados a la especificación.

5.1.1. Responsable de la información.

Es el responsable último de la protección de la información, garantizando su disponibilidad, confidencialidad e integridad.

Tiene la potestad de establecer los requisitos de seguridad de la información, en el sentido de asignarle a la misma una valoración que determinará el nivel de protección que requiere. El establecimiento de requisitos podrá realizarlo a propuesta del Responsable de Seguridad de la Información y contando con la opinión del Responsable del Sistema.

Este rol podrá recaer en una o varias personas, e incluso en un órgano colegiado, pudiendo coincidir con el Responsable del Servicio.

5.1.2. Responsable del servicio.

Se define servicio como la función o prestación desempeñada destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Este rol es el responsable de establecer los niveles de seguridad (o requisitos de seguridad) que requieren los servicios prestados, que determinarán las medidas de protección necesarias, así como su intensidad.

El establecimiento de requisitos podrá realizarse a propuesta del Responsable de Seguridad de la Información y contando con la opinión del Responsable del Sistema. Los requisitos del servicio deben tener en cuenta los requisitos de la información que manejan.

Este rol podrá recaer en una o varias personas, e incluso en un órgano colegiado, pudiendo coincidir con el Responsable de la Información.

5.1.3. Responsable del Tratamiento.

El Responsable del Tratamiento es la persona física o jurídica sobre la que recaen las funciones genéricas recogidas en la normativa de protección de datos aplicable y vigente en cuanto a responsabilidad última de los tratamientos de datos personales que se lleven a cabo.

En general, esta figura determina los fines y los medios relacionados con el tratamiento de los datos personales.

Sus funciones son las siguientes:

- Garantizar el cumplimiento de principios relativos al tratamiento recogidos en la normativa vigente en materia de protección de datos personales.

- Garantizar el cumplimiento de las normativas existentes en el CGC en materia de protección de datos personales.

- Garantizar el mantenimiento adecuado, y conforme a la legislación vigente, del Registro de Actividades de Tratamiento.

- Garantizar el cumplimiento del deber de información al interesado recogido en la normativa vigente en materia de protección de datos personales.

- Establecer los mecanismos necesarios para recibir, gestionar y resolver solicitudes de ejercicio de derechos por parte de los interesados.

- Evaluar el riesgo para los derechos y libertades de los afectados en las brechas de seguridad y la posible notificación a las autoridades de control y a los afectados.

- Determinar las medidas técnicas y organizativas apropiadas que se debe aplicar a fin de garantizar y acreditar que el tratamiento es conforme con la normativa vigente de protección de datos personales.

- Actuar como punto de contacto con las autoridades de control, conjuntamente con el Delegado de Protección de Datos.

- Implantar y seguir los programas de formación y sensibilización del personal del CGC en materia de protección de datos personales.

5.2. Estructura de supervisión.

La estructura de supervisión de la seguridad se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.

En la supervisión global de todas las actividades relativas a la seguridad de la información se encuentra el Responsable de Seguridad de la Información.

En la supervisión global de las actividades relativas a la seguridad física se encuentra el Responsable de Seguridad Física.

Para la coordinación global e integral de la seguridad se encuentra el Comité de Seguridad de la Información.

Para la gestión de la integración de la seguridad en los procesos de negocio del Cabildo y la coordinación general ante incidentes de seguridad que pudieran afectar a la imagen o a la consecución de los objetivos de la encomienda de gestión del CGC, se encuentra el Comité de Seguridad de la Información.

Las funciones y responsabilidades de cada una de las figuras se describen a continuación:

5.2.1. Responsable de Seguridad de la Información

La responsabilidad de la seguridad de la información estará segregada de la responsabilidad sobre los sistemas y la prestación de los servicios.

Este Responsable forma parte del Comité de Seguridad de la Información y, por tanto, es el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad de la información.

Sus responsabilidades comprenden:

- Hacer que se establezcan unos objetivos de seguridad de la información corporativos alineados con la gestión encomendada al organismo, determinar las acciones para conseguirlos y seguir su cumplimiento.

- Verificar que los requisitos de seguridad de la información y de los servicios, establecidos por los responsables correspondientes se materializan en medidas de seguridad adecuadas para satisfacerlos, supervisando su implantación y eficacia.

- Coordinar la implantación y controlar las medidas de seguridad de la información del organismo.

- Conseguir que se elabore el presupuesto anual de seguridad de TI (tecnologías de la información) del organismo.

- Definir un modelo de gestión de la seguridad alineado con la estrategia del organismo en materia de seguridad.

- Supervisar la implantación práctica de la estrategia de seguridad de la información del organismo.

- Promover la realización de análisis de riesgos de seguridad de la información, así como los planes para mitigarlos, de forma periódica, elevando las conclusiones al Comité de Seguridad de la Información para su aprobación.

- Solicitar al Servicio de Formación y Prevención la realización de programas de formación y sensibilización en materia de seguridad de la información.

- Definir indicadores de seguridad para medir la eficacia y eficiencia de las medidas implantadas.

- Medir los indicadores de seguridad definidos, interpretando sus valores y tomando las acciones pertinentes.

- Analizar los incidentes de seguridad de la información reflejados en los registros de estos y verificar que se han establecido los planes para su resolución.

- Elaborar la normativa de seguridad, alineada con la PSI, para su aprobación por parte del CSI.

- Velar por que se elaboren procedimientos operativos para la realización de las actividades que se encuentren reguladas por la normativa de seguridad, elevándolos al CSI para su aprobación.

- Verificar el cumplimiento de las normas y procedimientos establecidos.

- Mantener actualizada la documentación asociada a la gestión de la seguridad de la información: normativas, procedimientos y registros.

- Autorizar la ejecución de procedimientos de recuperación de datos en los casos en que se requiera.

- Velar por la inclusión de cláusulas de seguridad en los contratos con terceras partes y por su cumplimiento.

- Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación.

- Evaluar las necesidades de recursos requeridos para el cumplimiento de los planes de actuación derivados de la aplicación de la PSI, priorizando las actuaciones de acuerdo con los recursos disponibles o solicitando nuevos recursos, en caso necesario, para su aprobación por el CSI.

- Impulsar la realización de las auditorías ordinarias regulares, al menos cada dos años, que permitan verificar el cumplimiento de las obligaciones del CGC en materia de seguridad.

- Colaborar con las auditorías externas/internas en materia de seguridad de la información, revisarlas y encargar a los responsables de los sistemas la implantación de las correcciones que se deriven.

- Analizar, junto con el Comité de Seguridad, el desempeño de las actividades de gestión de la seguridad, identificando oportunidades de mejora.

- Para llevar a cabo las funciones encomendadas, el Responsable de Seguridad de la Información se podrá apoyar en la Oficina de Seguridad de la Información, como órgano operativo de la seguridad.

5.2.2. Responsable de Seguridad Física

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de seguridad física en el organismo.

Este Responsable forma parte del Comité de Seguridad de la Información y, por tanto, es el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad física de los locales y las infraestructuras.

Sus responsabilidades comprenden:

- Identificación de necesidades de seguridad física.

- Conseguir la elaboración de un presupuesto anual de inversiones y actuaciones en seguridad física.

- Supervisar la instalación y el mantenimiento posterior de los elementos y servicios destinados a la seguridad física.

- Analizar los incidentes de seguridad física que se puedan haber producido y establecer actuaciones para dar respuesta a los mismos.

- Participar en el Comité de Seguridad de la Información.

5.2.3. Delegado de Protección de Datos.

El Delegado de Protección de Datos (DPD), es la figura que actúa como asesor, supervisor e interlocutor del Responsable del Tratamiento en el ámbito de las competencias marcadas por la normativa en materia de protección de datos vigente.

Sus funciones son:

- Informar y asesorar al CGC y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.

- Supervisar el cumplimiento del Reglamento General de Protección de Datos en el CGC.

- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la Autoridad de Control.

- Actuar como punto de contacto de la Autoridad de Control conjuntamente con el Responsable del Tratamiento.

Además, asesorará al Responsable del Tratamiento o, en general, a aquella figura que lo necesite, en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos.

- Identificación de las bases jurídicas de los tratamientos.

- Valoración de la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.

- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.

- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.

- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.

- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación entre el CGC y los encargados del tratamiento.

5.2.4. Comité de Seguridad de la Información.

La misión del Comité de Seguridad de la Información, en adelante, CSI, es la coordinación general de las actividades que tienen relación con la seguridad integral.

Un objetivo fundamental del CSI es la puesta en común de aspectos importantes de la seguridad entre todos los responsables. Con ello se evitará que actividades referentes a la seguridad, que puedan afectar a varios o todos los Servicios y Órganos del CGC, queden sin el suficiente conocimiento por parte de sus responsables, o sin el suficiente apoyo o compromiso, perjudicando la eficacia.

El CSI asume las siguientes funciones y responsabilidades:

- Coordinar las acciones de comunicación y de gestión de la imagen del Cabildo de Gran Canaria en caso de incidentes de seguridad de la información, haciendo partícipe al órgano superior competente en caso necesario.

- Facilitar y aprobar la dotación de recursos para las actividades que se identifiquen que permitan mejorar la seguridad de la información en los procesos del Cabildo de Gran Canaria, de forma alineada con el órgano superior competente.

- Proponer al órgano superior competente la aprobación del presupuesto anual de seguridad de la información para el Cabildo de Gran Canaria.

- Proponer al órgano superior competente la aprobación del presupuesto anual de seguridad física para el Cabildo de Gran Canaria.

- Proponer al órgano superior competente, e impulsar la creación y utilización, de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de TIC

- Establecer unos objetivos de seguridad de la información corporativos alineados con las competencias y obligaciones del organismo

- Supervisar y coordinar las actuaciones de las diferentes áreas del Cabildo de Gran Canaria durante la resolución de situaciones provocadas por incidentes de seguridad de la información o de discontinuidad de las operaciones del Cabildo.

- Velar por el cumplimiento de la normativa legal respecto a la seguridad de la información y protección de datos personales.

- Elaborar e impulsar estrategias y nuevas líneas de trabajo en lo que respecta a la seguridad de la información.

- Interpretar y resolver los conflictos surgidos en materia de seguridad de la información, en particular los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización.

- Comunicar a los diferentes órganos la necesidad del cumplimiento de la Política de Seguridad de la Información y las normativas derivadas e instar, en su caso, a la adopción de las medidas disciplinarias, o de cualquier otra índole, correspondientes en caso contrario.

- Coordinar las actuaciones en materia de seguridad que se puedan estar realizando en diferentes áreas del CGC, con objeto de evitar esfuerzos duplicados o desalineados con la Política de Seguridad.

- Alinear las actuaciones en seguridad con los objetivos estratégicos establecidos por el órgano superior competente.

- Asumir el papel de dueño de los riesgos de seguridad de la información (quien tiene la potestad para aceptar los riesgos residuales sobre los activos), aprobando las apreciaciones de riesgos realizadas y aceptando el riesgo residual resultante, en su caso.

- Aprobar planes de mejora de la seguridad de la información del CGC y los planes de tratamiento de riesgos que surjan a raíz de las apreciaciones de riesgos realizadas. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

- Supervisar los incidentes de seguridad que se puedan producir y plantear las estrategias y salvaguardas ante los mismos, velando por la adecuada coordinación de los diferentes actores involucrados en la gestión de estos incidentes.

- Participar y colaborar en el seguimiento y en la respuesta a los incidentes de seguridad que se hayan podido producir, estableciendo las medidas de contención y remediación cuando sea necesario.

- Divulgar la PSI, las normativas y procedimientos de seguridad de la información aprobados.

- Elaborar y revisar regularmente la PSI, elevando al órgano superior competente posibles modificaciones para su aprobación.

- Aprobar las normativas de seguridad que deban ser observadas y conocidas por el personal del CGC a propuesta del Responsable de Seguridad de la Información.

- Aprobar los procedimientos operativos de seguridad, a propuesta de los responsables de los diferentes servicios o del Responsable de Seguridad de la Información.

- Colaborar en el seguimiento de los principales riesgos residuales asumidos por el CGC y recomendar posibles actuaciones respecto de ellos.

- Informar al órgano superior competente del desempeño de las funciones de seguridad en el CGC y del estado de la seguridad.

- Promover la mejora continua de la seguridad de la información.

- Cualquier otra función relacionada con la seguridad de la información que pueda ser encomendada por el órgano superior competente.

5.2.4.1. Composición del Comité de Seguridad de la Información.

El CSI estará compuesto por:

- Órganos directivos con competencias en materia de seguridad de la información o, en su defecto, la persona designada por el titular de la Consejería con competencias en este ámbito.

- El Responsable de Seguridad de la Información.

- El Responsable de Seguridad Física.

- Delegado de protección de datos, con voz, pero sin voto.

La presidencia y secretaría del CSI serán determinadas por el órgano superior competente.

El CSI se reunirá con carácter ordinario, como mínimo, una vez cada seis meses y extraordinariamente cuantas veces estime necesario su Presidencia.

A requerimiento del CSI se podrá convocar, con voz, pero sin voto, a las personas cuya intervención sea precisa por ser afectados por el ENS o en calidad de asesores.

5.3. Estructura de Operación.

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.

Se describen a continuación las funciones y responsabilidades de las figuras asociadas a la estructura de operación.

5.3.1. Responsable de los Sistemas de Información.

Sus funciones y responsabilidades son:

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Organización.

- Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticación, control de acceso, auditoría y registro.

- Garantizar que la seguridad física y lógica de los sistemas de información satisfacen requisitos de seguridad sobre la información y los servicios establecidos por el CSI.

- Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada, siguiendo el principio de seguridad por defecto.

- Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.

- Verificar el funcionamiento de mecanismos de control de acceso que eviten que un usuario acceda a datos o recursos con derechos distintos de los autorizados, sin que en ningún caso se puedan desactivar.

- Seguir los foros de vulnerabilidades y elaboración del calendario de aplicación de actualizaciones para los sistemas de información, en función de los que surjan y el impacto que tengan en la seguridad (las actualizaciones mismas los aplicarán los administradores de sistemas).

- Implantar las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.

- Proporcionar datos para la alimentación de indicadores de seguridad de la información.

- Elaborar los procedimientos operativos necesarios para describir las operaciones sobre los sistemas, elevándolos al Responsable de Seguridad de la Información o al CSI para su aprobación.

- Supervisar los procedimientos de copia de seguridad.

- Realizar auditorías técnicas periódicas de la infraestructura, sistemas y aplicaciones.

5.3.2. Oficina de Seguridad de la Información.

La Oficina de Seguridad de la Información es un grupo de apoyo al Responsable de Seguridad para el cumplimiento de sus funciones.

Asumirá cualquier otra tarea que le sea encomendada por el Responsable de Seguridad tanto en el ámbito de la seguridad de la información como de la protección de datos de carácter personal.

Los componentes de la Oficina de Seguridad se determinarán por el Responsable de Seguridad, de entre el personal adscrito a los servicios con competencias en materia de seguridad, pudiendo coordinar al personal público del CGC o mediante la supervisión y control de contratos de prestación de servicios

5.4. Designación de roles de las estructuras de seguridad.

Se establece que, en el CGC, los roles organizativos en los que se apoya la seguridad de la información recaerán en los siguientes cargos:

Los roles de Responsable de la Información, Responsable del Servicio y Responsable del Tratamiento recaerán en la persona titular del órgano superior o directivo con responsabilidad sobre el servicio de información afectado directamente por el ENS, que podrá delegar la función en la Jefatura de Servicio correspondiente.

El rol de Responsable de Seguridad de la Información recaerá en la persona titular del órgano superior o directivo con competencias en la gestión de la seguridad de la información.

El rol de Responsable de Seguridad Física recaerá en la persona titular del órgano superior o directivo con competencias en la gestión de la seguridad física.

El rol de Delegado de Protección de Datos recaerá en la persona física o jurídica asignada, mediante decreto del Presidente del CGC, como Delegado en Protección de Datos del CGC.

El rol de Responsable del Sistema de Información

recaerá en la persona titular del Servicio con responsabilidad sobre la operatividad del sistema de información afectado por el ENS.

5.5. Procedimientos de designación.

Se establece que el órgano superior competente es el órgano con potestad para modificar la designación de roles establecida anteriormente. En caso de modificación, se recogerá la misma en el acta de la sesión correspondiente, que constituirá el documento justificativo en tanto se realice una revisión del presente documento de PSI.

El desempeño de las responsabilidades definidas en esta PSI vendrá determinado por el acceso a los diferentes perfiles que se han vinculado a ellas. En el caso de que desapareciese o cambiara de denominación de alguno de estos perfiles será competencia del CSI elevar una propuesta al órgano superior competente con los cambios necesarios en la PSI.

5.5.1. Mecanismos de coordinación y de resolución de conflictos.

La coordinación entre los diferentes roles participantes de las actividades de seguridad, así como la resolución de conflictos que pudieran surgir entre ellos se llevará a cabo en el CSI.

6. La gestión de la seguridad.

La seguridad de la información es el resultado de un proceso que depende de todos y cada uno de los elementos humanos, técnicos, materiales y organizativos que intervienen en el tratamiento. Quienes participen en cualquier fase del tratamiento deberán responder, en la medida de sus responsabilidades, de la seguridad y buen uso de la información. De manera especial, deberán colaborar en la prevención, detección y control de los riesgos derivados de actuaciones negligentes, ignorancia de las normas, fallos técnicos, de organización o de coordinación, o instrucciones inadecuadas.

El CGC, a través de los distintos agentes con responsabilidades específicas en materia de seguridad de la información, se encargará de proporcionar los canales de participación adecuados que hagan efectiva la colaboración mencionada en el párrafo anterior. Del mismo modo, el CGC, se ocupará de mantener permanentemente informados, a todos los destinatarios de esta política, del propósito y contenido de la misma, así como de los documentos que la desarrollan y de los canales de participación habilitados.

El proceso de gestión de la seguridad de la información deberá estar sometido a monitorización, control y mejora continuos para confirmar su eficiencia ante la constante evolución de los riesgos y de los sistemas de protección.

La política del CGC es la de contrarrestar las amenazas de seguridad con los medios suficientes, dentro de las posibilidades presupuestarias. Para este fin, se establecerá una estructura de seguridad, junto con los mecanismos apropiados para su gestión, y un conjunto de instrumentos de apoyo de forma que se garantice:

- el cumplimiento de los objetivos de su misión y de prestación de servicios

- el cumplimiento de la legislación y normativa aplicables

- la protección de las infraestructuras de las tecnologías de la información y las comunicaciones frente a ataques deliberados

Para ello,

- se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo las infraestructuras.

- se diseñarán medidas de respuesta ante incidentes de seguridad, física o lógica, de forma que se minimice el impacto de los mismos, en caso de que ocurrieran.

Como norma general, se tendrá un enfoque de orientación al riesgo a la hora de diseñar las medidas de seguridad necesarias, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo.

Las distintas áreas del CGC bajo cuya responsabilidad se encuentran los servicios prestados deberán contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad prescritas por el ENS para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de los servicios y de la información.

Los requisitos de seguridad de los sistemas, las necesidades de formación de los usuarios, administradores y operadores y las necesidades de financiación deben

ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las TIC.

Se deben articular mecanismos de prevención, detección, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

6.1. Prevención.

El CGC debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la organización debe:

- Autorizar los sistemas antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

6.2. Detección.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

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

6.3. Reacción.

El CGC debe:

- Establecer mecanismos para realizar la gestión de incidentes de seguridad de forma eficaz.

- Designar puntos de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con el CGC.

- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT) reconocidos a nivel nacional como Iris-CERT, CCN-CERT y otros equivalentes.

6.4. Recuperación.

Para restaurar la disponibilidad de los servicios, se deberán desarrollar planes de contingencia de los sistemas TIC que incluyan actividades de recuperación de la información que contribuyan a la continuidad del servicio.

6.5. La gestión de riesgos.

Todos los sistemas sujetos a la presente PSI deberán ser objeto de un análisis de riesgos que evalúe las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá regularmente, al menos una vez al año, elevando las conclusiones al CSI. Se realizará un análisis de riesgos de los sistemas de información en periodos inferiores a un año cuando:

1. Se modifique la información manejada.

2. Se modifiquen los servicios prestados.

3. Ocurran incidentes graves de seguridad.

4. Se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Responsable de la Información y el Responsable del Servicio establecerán una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El CSI dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La reducción de los niveles de riesgo se realizará mediante la aplicación de controles. La selección y aplicación de los controles ponderarán el valor de los activos con los niveles de riesgo y el coste de la seguridad.

Los controles deberán ser eficaces antes, durante o

después de que ocurra un incidente de seguridad. Su objetivo es evitar que sucedan incidencias y controlar los daños si es que finalmente llegan a producirse.

El CSI establecerá los niveles aceptables de riesgo y aprobará las actuaciones a llevar a cabo en caso de que se incurra en niveles de riesgo no aceptables.

El análisis y la gestión de riesgos deberán estar presentes en todas las fases del ciclo de vida de las aplicaciones y servicios relacionados con el tratamiento de la información, empezando por la del estudio de viabilidad.

La selección y aplicación de los controles de seguridad, así como la evaluación de su eficiencia, deberán tenerse en cuenta durante el diseño, construcción, contratación, adquisición, explotación, cierre, terminación, cancelación o enajenación de las aplicaciones y servicios mencionados.

Los órganos competentes del CGC valorarán en las contrataciones aquellas empresas, productos y servicios que puedan acreditar un nivel de calidad o seguridad. El cumplimiento de un nivel mínimo determinado podrá ser un requisito imprescindible.

6.6. Planificación y coordinación.

Los objetivos a medio plazo para la mejora de la seguridad de la información se explicitarán en los correspondientes planes estratégicos. Estos planes contendrán una descripción de las líneas de actuación previstas, proyectos, indicadores de cumplimiento y de progreso, así como métricas para evaluar la efectividad. Estos planes se revisarán anualmente teniendo en cuenta los resultados de las auditorías y de las evaluaciones de riesgos. Los planes estratégicos, los informes de seguimiento y las revisiones anuales elaborados por el CSI serán elevados al órgano superior competente.

La coordinación entre todos los agentes de los que depende la seguridad de la información debe formar parte de todas las iniciativas y actuaciones. El CGC, habilitará los medios técnicos necesarios para facilitar esa coordinación. El CSI actuará de manera coordinada con el órgano superior competente para la aplicación y control de las medidas de seguridad.

Las empresas de servicios, organizaciones y entidades con acceso a información situada bajo la responsabilidad del CGC, deberán nombrar un Responsable de Seguridad que actúe como interlocutor válido a los efectos de la coordinación en esta materia.

6.7. Acceso a la información.

Quienes traten información que no haya sido clasificada de acceso público deberán estar debidamente identificados y tener los privilegios de acceso a la información estrictamente imprescindibles para desempeñar su cometido.

Cada intento de acceso deberá quedar registrado con el suficiente nivel de detalle.

6.8. Registro de actividad.

Las actuaciones de las personas, en tanto que formen parte de determinado tratamiento de información, podrán ser registradas en cumplimiento de las exigencias legales de trazabilidad. También podrán serlo para monitorizar el cumplimiento de la presente política. En todo caso, el registro de tales actuaciones se realizará preservando los derechos de los afectados y respetando la normativa laboral aplicable.

6.9. Confidencialidad y deber de secreto.

Quienes por razón del ejercicio de sus funciones accedan a datos que no sean de acceso público deberán observar la necesaria reserva, confidencialidad y sigilo respecto a estos datos, incluso después de haber cesado en sus funciones o finalizado la relación contractual o laboral.

6.10. Uso de instalaciones y equipamiento.

El CGC dotará los puestos de trabajo con el equipamiento informático y de comunicaciones necesario para el desempeño de las funciones encomendadas. Dichos equipos no están destinados al uso personal.

El equipamiento mencionado en el párrafo anterior no podrá utilizarse para actividades ilícitas o irregulares, o que afecten negativamente al funcionamiento de la administración o sean contrarias a los intereses de esta.

La instalación o utilización de elementos hardware o software ajenos a los que forman parte de la configuración del puesto de trabajo requerirán de una autorización previa por parte del órgano competente en materia de tecnologías de la información que corresponda.

Las infraestructuras informáticas y de comunicaciones que no formen parte de los puestos de trabajo deberán ubicarse en áreas separadas, de acceso restringido y suficientemente protegidas de acuerdo con la naturaleza de la información y los servicios en que intervengan.

6.11. Características de los sistemas de información.

Los sistemas de información proporcionarán la funcionalidad estrictamente necesaria para cumplir los propósitos declarados, y ninguna más.

El uso ordinario de los sistemas de información ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Las funciones de operación, administración, mantenimiento y registro de actividad serán las mínimas necesarias, deberán estar descritas y documentadas y sujetas a controles estrictos.

6.12. Protección de la información almacenada y en tránsito.

El CGC, a través de los distintos agentes con responsabilidades específicas en materia de seguridad de la información, establecerá las condiciones para la protección en el tratamiento de la información fuera de sus locales y sistemas.

El CGC garantizará, del mismo modo que en el párrafo anterior, la conservación y recuperación de la información mientras perdure su vigencia.

La información en soporte no electrónico que haya sido causa o consecuencia directa de tratamiento automatizado de información deberá protegerse con el mismo grado de seguridad que esta.

6.13. Datos de carácter personal.

El CGC solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la legislación vigente en materia de Protección de Datos.

7. Desarrollo de la PSI.

Esta PSI se desarrollará mediante la elaboración de normativas de seguridad que aborden aspectos específicos. A raíz de dichas normativas se podrán desarrollar procedimientos que describan la forma de llevar a cabo las actividades observando las normas establecidas.

La documentación de normativas de seguridad y procedimientos, así como esta Política de Seguridad se encontrará a disposición de todo el personal de la organización que necesite conocerla y, en particular, el personal que utilice opere o administre los sistemas de información y comunicaciones, la información misma albergada en dichos sistemas o los servicios prestados por el CGC.

La aprobación y revisión de los documentos anteriormente reseñados se hará conforme a lo siguiente:

- PSI: será aprobada por el órgano superior competente, siendo responsabilidad del CSI su revisión para elevar una propuesta de modificación cuando sea necesario.

- Normativa de seguridad: será aprobada por la Consejería competente o, en su caso, por el CSI por delegación de la mencionada Consejería, siendo responsabilidad del CSI su revisión cuando sea necesario.

- Procedimientos operativos: serán aprobados por la Consejería competente o, en su caso, por el CSI por delegación de la mencionada Consejería, a propuesta de los responsables de los diferentes sistemas o del Responsable de Seguridad de la Información.

La distribución de la documentación del marco normativo de seguridad deberá atender también a criterios de seguridad según el contenido de dicha documentación. El marco normativo contendrá documentos de difusión pública y documentos de uso interno. Los documentos de uso interno serán albergados en áreas de control de acceso restringido y serán consultables sólo por personal pertinente bajo el principio de mínimos privilegios. La información de difusión pública se albergará en la Sede Electrónica del CGC accesible al público mediante la dirección electrónica https://sede.grancanaria.com/.

Toda nueva versión de un documento aprobado dentro del marco normativo será comunicada según el alcance de uso del documento y el nivel de difusión requerido, de forma que el personal pueda descartar las versiones de los documentos obsoletas.

8. Obligaciones del personal.

Todo el personal del CGC tiene la obligación de conocer y cumplir esta PSI y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del CSI disponer los medios necesarios para que la información llegue a los afectados.

Así mismo, el personal deberá asistir a las sesiones de concienciación y formación en materia de seguridad para las que sea designado como asistente.

9. Terceras partes.

Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por el CGC serán hechos partícipes de esta Política. Las terceras partes quedarán obligadas al cumplimiento de esta Política y a las normativas que se puedan derivar de ella.

Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer la Política.

Se deberán establecer procedimientos específicos de comunicación de incidencias para que los terceros afectados puedan comunicarlas.

El personal de las Terceras Partes deberá recibir sesiones de concienciación, tal como se exige para el personal propio.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, el Responsable de Seguridad deberá realizar un informe del riesgo en que se incurre. Ese riesgo deberá ser aceptado por el CSI.

10. Formación y Concienciación.

De manera sistemática se realizarán acciones de formación y concienciación en materia de seguridad.

El objetivo de la acción formativa y de concienciación es doble:

- mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, configuración segura de equipos, desarrollo seguro, gestión de incidentes de seguridad, riesgos, etc.

- concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

El primer objetivo se asocia a Formación y el segundo a Concienciación.

Todo el personal deberá asistir a una sesión de concienciación en materia de seguridad de la información con la periodicidad que se determine por parte del CSI.

Se establecerá un plan de concienciación para impartir las anteriormente mencionadas sesiones.

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

Las áreas responsables determinarán el formato de la acción de formación, así como sus contenidos.

ANEXO A: Glosario de términos.

A

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

C

CCN. Centro Criptológico Nacional.

CERT. Computer Emergency Reaction Team.

D

Datos de carácter personal. Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

E

ENS. Esquema Nacional de Seguridad.

G

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.

I

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

Información. Caso concreto de una categoría específica de información (por ejemplo, datos de carácter personal, médicos, financieros, investigaciones, contratos, información delicada…). Estos tipos los define una organización y, en algunos casos, vienen definidos por alguna normativa de carácter legal.

P

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.

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

S

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

Sistemas 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.

STIC. Seguridad TIC

T

TIC. Tecnologías de la Información y la Comunicación.

En Las Palmas de Gran Canaria, a veintinueve de marzo de dos mil veintidós.

LA CONSEJERA DE ÁREA DE FUNCIÓN PÚBLICA Y NUEVAS TECNOLOGÍAS, Margarita González Cubas.

114.177

Consejería de Sector Primario y Soberanía Alimentaria

Servicio Administrativo de Agricultura, Ganadería y Pesca

ANUNCIO

797

Por Resolución número 22/102 R-AGP, de 1 de abril de 2022, del Consejero de Sector Primario y Soberanía Alimentaria, por delegación del Consejo de Gobierno Insular, mediante acuerdo de fecha 31 de julio de 2019, se procedió a la aprobación de las "BASES REGULADORAS PARA EL USO DE LOS ESPACIOS DESTINADOS A LA PROMOCIÓN, EXPOSICIÓN Y VENTA COMERCIAL DEL RECINTO FERIAL, DEL "XXIX CONCURSO-EXPOSICIÓN DE GANADO, AÑO 2022", encontrándose las mismas en el Tablón de Anuncios del Servicio Administrativo de la Granja Agrícola Experimental y publicadas en la página web www.grancanaria.com

Contra el citado anuncio podrá interponerse Recurso Potestativo de Reposición ante el Consejo de Gobierno Insular, en el plazo de UN (1) MES a contar desde el día siguiente al de su publicación en el Boletín Oficial de la Provincia, o en su defecto, y en el plazo de DOS (2) MESES, contados de la misma forma, interponer directamente Recurso Contencioso-Administrativo ante el Juzgado de lo Contencioso-Administrativo de Las Palmas de Gran Canaria.

En Arucas, a uno de abril de dos mil veintidós.

EL PRESIDENTE, P.D. EL CONSEJERO DE SECTOR PRIMARIO Y SOBERANÍA ALIMENTARIA, Miguel Hidalgo Sánchez.

116.042