Cabildo de Gran Canaria

INSTITUTO DE ATENCIÓN SOCIAL Y SOCIOSANITARIA

Política de Seguridad de la Información

INSTITUTO DE ATENCIÓN SOCIAL Y SOCIOSANITARIA

APROBACIONES

Elaborado por:	Revisado por:	Aprobado por:
Jacob Arocha Santana Técnico Informático Fecha: 12/12/2023	Gilberto Marquina Reyes Jefe Servicio Informática Fecha: 12/12/2023	Consejo Rector IAS Fecha: 18/12/2023

CONTROL DE CAMBIOS

Versión	Fecha	Páginas	Cambios
1.00	12/12/2023		Versión inicial
1.01	09/05/2024	4	Composición del CSI

Clasificación de la Información	
Tipo:	Información de uso público
Ámbito de difusión:	Todos los empleados y colaboradores externos del IAS
Responsable:	Responsable de Seguridad de la Información del IAS

info@instituto-as.es
www.instituto-as.es

Índice

Aprobación y entrada en vigor

La Política de Seguridad de la Información, en adelante PSI, será aprobada mediante acuerdo del Consejo Rector del Instituto de Atención Social y Sociosanitaria del Cabildo de Gran Canaria, en adelante IAS. Esta PSI será efectiva desde la fecha de aprobación y hasta que sea reemplazada por una nueva política.

El IAS 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.

Composición del Comité de Seguridad

En la siguiente tabla se indican los vigentes responsables y miembros del Comité de Seguridad de la Información (CSI) del IAS:

Comité de Seguridad de la Información comite.seguridad@instituto-as.es		
Rol / Cargo en Comité	**Designado**	**Nombramiento**
Responsable de Gobierno Presidente del CSI	D. Tenesor Perera Sosa Coordinador de Servicios Generales ftenesorps@instituto-as.es	Decreto Presidencia 2024-0510
Responsable de Seguridad de la Información	D. Gilberto Marquina Reyes Jefe de Servicio Informática gilbertomr@instituto-as.es	Consejo Rector CR/2023/8
Responsable del Sistema Secretario del CSI	D. Jacob Arocha Santana Técnico Servicio Informática jacobas@instituto-as.es	Consejo Rector CR/2023/8
Delegado Protección de Datos Miembro sin voto	Audidat 3.0 S.L.U. D. Alejandro Pérez Rocasalbas dpd@instituto-as.es	Contrato con expte. nº 8575/2023

Introducción

La información constituye un activo de primer orden para el IAS 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 (TIC) 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.

El IAS depende de los sistemas TIC para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información, y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

La presente PSI se elabora en cumplimiento de la exigencia del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, que en su artículo 12 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 IAS 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, analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes centros y servicios del IAS 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 la valoración de su coste, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en los pliegos de licitación para proyectos TIC.

Misión del IAS

El Instituto de Atención Social y Sociosanitaria del Cabildo de Gran Canaria promueve la realización en la isla de Gran Canaria de actividades de promoción, prestación y gestión directa o indirecta de recursos y servicios sociosanitarios, docencia e investigación de la atención sociosanitaria y su promoción. Para ello pone a disposición del ciudadano la realización de trámites online con el objetivo de impulsar la tramitación electrónica de los procedimientos administrativos, la mejora en la prestación de los servicios y la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la mejora de la eficacia y eficiencia de la acción pública.

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

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 IAS, 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 éstos o no en instalaciones propias.
- Los sistemas de información del IAS, 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 IAS.
- Las personas afectadas por la presente PSI, que serán:
    - Personal del IAS, sea electo, directivo, eventual, funcionario o laboral que haga uso de los sistemas de información.
    - Personal externo perteneciente a otras entidades que, en virtud de relaciones especiales, como convenios de colaboración, contratos de servicios, de asistencia técnica y de asesoramiento, entre otras, hagan uso de los sistemas de información del IAS.
    - 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 IAS 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.

Marco normativo

Marco normativo general

La base normativa que afecta al desarrollo de las actividades y competencias del IAS, en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (https://www.boe.es/doue/2014/257/L00073-00114.pdf), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- 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 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (archivo).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 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.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (vigente en los apartados señalados en la Disposición Derogatoria Única de la Ley 11/2022, de 28 de junio).
- 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.

- Ley 11/2022, de 28 de junio, General de Telecomunicaciones (según plazos entrada en vigor de Disposición de esta Ley).

Normativa interna

- Creación de la Sede Electrónica y Registro Electrónico del IAS, aprobada por el Consejo Rector del IAS el 23 de mayo de 2018 (Boletín Oficial de la Provincia de Las Palmas, número 67, 04/06/2018).
- Política de Seguridad de la Información del Cabildo de Gran Canaria, aprobada por la Consejería de Función Pública y Nuevas Tecnologías del Cabildo de Gran Canaria el 28 de marzo de 2022 (Boletín Oficial de la Provincia de Las Palmas, número 41, 06/04/2022).

Otra normativa

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del IAS, derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política, entre otras.

El mantenimiento del marco normativo será responsabilidad del IAS, y se mantendrá en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el Real Decreto.

Así mismo, el IAS también será responsable de identificar las Guías de Seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

La Política de Seguridad de la Información y el Plan de Adecuación al ENS del IAS se basan en las siguientes Guías de Seguridad del CCN:

- CCN-STIC 805: Política de Seguridad de la Información

- CCN-STIC 890: Guía de Adecuación al ENS conforme al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.
- CCN-STIC 890C: Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad
- CCN-STIC 806: Plan de Adecuación al ENS
- CCN-STIC 883: Anexo III. Plan de Adecuación al ENS Diputaciones, Cabildos, Consejos Insulares y órganos competentes equivalentes
- CCN-STIC 801: Esquema Nacional de Seguridad. Responsabilidades y funciones
- CCN-STIC 804: ENS. Guía de implantación

La gestión de la seguridad

El IAS, para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al IAS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

1. El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
2. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
3. En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se

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

4. Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Mejora continua en materia de seguridad

La vigilancia continua por parte del IAS 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.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información

Gestión de personal

Todo el personal propio o ajeno relacionado con los sistemas de información del IAS, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

Análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos 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 a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Incidentes de seguridad

El IAS dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, y deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Líneas de defensa

El IAS ha implementado una estrategia de protección de los sistemas de información basada en múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de Información se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Diferenciación de responsabilidades

El IAS ha organizado su seguridad comprometiendo a todos los miembros de la entidad mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "MODELO DE GOBERNANZA" del presente documento.

Autorización y control de los accesos

El IAS ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones

El IAS ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos y servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad, el IAS tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

Protección de la información

El IAS prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de

información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Registro de actividad

El IAS, con el propósito de satisfacer el objeto de esta política, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, se podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de

servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Infraestructuras y servicios comunes

El IAS tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este documento.

Perfiles de cumplimiento específicos

El IAS tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

Datos de carácter personal

El IAS, en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa vigente, entre otra el Reglamento 679/2016, 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-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

Modelo de Gobernanza

Bloques de responsabilidad

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información adaptada a las necesidades y particularidad del IAS, se propone una designación de roles por bloques de responsabilidad: Gobierno, Supervisión y Operación.

De acuerdo con esta estructura, se han asignado las siguientes responsabilidades y funciones de seguridad:

Bloque de Gobierno

El bloque de gobierno es el encargado de determinar los requisitos de seguridad que serán de aplicación a los servicios prestados por el IAS y a garantizar el cumplimiento normativo asociado que le es de aplicación, en concreto el Real Decreto 311/2022, de 3 de mayo, 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, los roles asociados a este bloque, así como sus responsabilidades y funciones:

- **Responsable de la Información.** Es el responsable último de la protección de la información, garantizando su confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad.

  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.

- **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 (requisitos de seguridad) que requieren los servicios prestados, que determinarán las medidas de protección necesarias, así como su intensidad.

  El establecimiento de requisitos se realizará a propuesta del Responsable de Seguridad de la Información, quien contará para definirla con la opinión de los Directores de Área, Directores de Centro o Jefes de Servicio responsables del servicio en cuestión y 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.

  En la actualidad, y por acuerdo del Consejo Rector del IAS, se ha designado un **Responsable de Gobierno**, que integra los roles de Responsable de la Información y Responsable del Servicio, y que será asumido por la Presidencia del IAS o persona en quien delegue.

- **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 IAS 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 de la Información.
- 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 IAS en materia de protección de datos personales.

Bloque de Supervisión

La estructura de supervisión o ejecutiva 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.

Para la coordinación global e integral de la seguridad, así como para la gestión de la integración de la seguridad en los procesos de negocio del IAS y la coordinación general ante incidentes de seguridad que pudieran afectar a la imagen o a la consecución de los objetivos del IAS, se encuentra el Comité de Seguridad de la Información.

Se describen a continuación, los roles asociados a este bloque, así como sus responsabilidades y funciones:

- **Responsable de la 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 funciones son las siguientes:

- 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 IAS.
- Conseguir que se elabore el presupuesto anual de seguridad de TI (tecnologías de la información) del IAS.
- Definir un modelo de gestión de la seguridad alineado con la estrategia del IAS en materia de seguridad.
- Supervisar la implantación práctica de la estrategia de seguridad de la información del IAS.
- 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 a la Unidad de Docencia 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 IAS 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.

- **Delegado de Protección de Datos (DPD).** El 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 las siguientes:

  - Informar y asesorar al IAS 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 IAS.
  - 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 IAS y los encargados del tratamiento.

- **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 o Centros del IAS queden sin el suficiente conocimiento por parte de sus responsables, o sin el suficiente apoyo o compromiso, perjudicando la eficacia.

  Sus funciones son las siguientes:

  - Coordinar las acciones de comunicación y de gestión de la imagen del IAS 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 IAS, 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 IAS.
  - Proponer al órgano superior competente, e impulsarla 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 IAS.

- 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 IAS, 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 IAS 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, elevarla al órgano superior competente posibles modificaciones para su aprobación.
- Aprobar las normativas de seguridad que deban ser observadas y conocidas por el personal del IAS 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 IAS y recomendar posibles actuaciones respecto de ellos.
- Informar al órgano superior competente del desempeño de las funciones de seguridad en el IAS 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.

Composición del Comité de Seguridad de la Información. El CSI estará compuesto por:

- Responsable de Gobierno, como órganos directivos con competencias en materia de seguridad de la información.
- Responsable de Seguridad de la Información.
- Responsable del Sistema.
- 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.

Bloque de Operación

- **Responsable 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 el bloque de supervisión.

  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.

  Este bloque integra el rol de **Responsable del Sistema**, y a continuación se describen sus responsabilidades y funciones:

  - Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información del IAS.
  - 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 las 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.
- Delegación de funciones: podrá designar cuantos Responsables de Sistema delegados considere necesarios, aunque la responsabilidad final sigue recayendo sobre sí mismo. Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con el desarrollo, la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información. Se podrán encargar de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales. Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, que es a quien reporta.

Procedimiento de designación

La designación inicial de los Responsables identificados en esta Política ha sido realizada por acuerdo del Consejo Rector del IAS y comunicada a las partes afectadas.

El Consejo Rector ha facultado a la Presidencia del IAS para que adopte las medidas organizativas necesarias que permitan el desarrollo y la aplicación de los aspectos técnicos previstos en esta Política de Seguridad, incluyendo la facultad de nombrar y cesar al Responsable de Supervisión y Responsable de Operación.

Los roles de seguridad serán revisados cada cuatro años, en el caso de que exista una vacante la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

Resolución de conflictos

Si hubiera conflicto entre los responsables, éste será resuelto por el CSI.

Desarrollo de la PSI

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de la documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad. Para su organización se ha definido una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso.

La revisión anual de la presente Política corresponde al Responsable de Gobierno, proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

Terceras partes

Cuando se presten servicios o se maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información. El IAS definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el IAS lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el IAS utilice servicios o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogidas en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la

Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.

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.