GETAFE AYUNTAMIENTO | Empresa Municipal GETAFE INICIATIVAS | GISA GETAFE

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

Información del documento

Política de Seguridad de la Información

Control de versiones

Versión	Fecha	Descripción de cambios
V1.0	04/09/2020	Versión inicial del documento
V2.0	07/06/2022	Introducción de referencia expresa a requisitos mínimos Artículo 11 ENS

Propiedad del documento

Autor: Responsable de Seguridad

Propietario: Getafe Iniciativas S.A. (en adelante GISA)

Clasificación: Público

Revisión y aprobación

Elaboración	Revisado por	Aprobado por
Responsable de Seguridad	Comité de Seguridad	Consejera Delegada

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

Índice

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

1 Introducción

La organización ha considerado la necesidad de gestionar la seguridad como un todo completo, transversal en la entidad y en cada proceso interno, como una cuestión estratégica de la organización.

La implementación de un sistema de gestión de la seguridad de la información, está condicionada a las necesidades de la actividad y a las líneas marcadas por los objetivos organizacionales, entre los que se encuentran actualmente, los objetivos de seguridad de la organización. Todos los procesos internos y externos, quedan adscritos y afectos, a la presente política de seguridad, o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

La seguridad, por tanto, debe ser entendida como el conjunto de principios básicos y requisitos mínimos requeridos para una protección adecuada de la información tratada y los servicios prestados a los terceros.

Nuestra organización ya ha venido dando pasos en este sentido, y ha considerado prioritario establecer los objetivos de seguridad con plena alineación con los objetivos de negocio que culminará en un sistema de gestión conforme a los requisitos establecidos en el Real Decreto 3/2010 –en su versión consolidada por Real Decreto 925/2015-, y que culminará con la certificación en esta línea y en un sistema de gestión de seguridad de la información.

Por defecto, la Dirección ha considerado que la organización es la responsable de los activos de información y de los recursos de su propiedad, y asume que las tareas relacionadas con la seguridad de la información son una parte fundamental para el desarrollo de la actividad.

Se mantendrán las tres dimensiones clásicas de seguridad, integrándose además las dimensiones referenciadas en el Real Decreto 3/2010: confidencialidad, integridad y disponibilidad, así como las dimensiones de autenticidad y trazabilidad.

La organización considera que la seguridad de la información debe evolucionar continuamente para adecuarse a los requerimientos de negocio, sin impactar injustificadamente en el mismo y teniendo en cuenta la adecuada relación entre costes y beneficios.

Para soportar esta política, se establecerán políticas de seguridad, normas y procedimientos detallados, los cuales serán publicados y comunicados a todos los usuarios, terceros y socios de negocio de GETAFE INICIATIVAS, S.A. (en adelante GISA) cuando los mismos se vean afectados. La presente Política será accesible para las partes internas y externas afectadas.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

1.1 Estándar de Seguridad de la Información

La Dirección ha considerado implantar un estándar de seguridad. Se considerarán todos los elementos de seguridad necesarios, y específicamente el Real Decreto 3/2010 (en su versión consolidada por Real Decreto 951/2015).

En base a este estándar, se ha impuesto un sistema, con los requisitos propios de un sistema de gestión de seguridad de la información, considerando las particularidades del negocio, de la organización y del cliente tipo.

La organización somete sus sistemas a los controles establecidos en el Anexo II de la misma, y en su caso, cuando sea preciso, se incorporarán nuevos controles o se complementaran los mismos.

La organización puede considerar la necesidad de someterse a una certificación de un tercero externo independiente, que permita acreditar la alineación el sistema de gestión implantado a la norma, según descripción de la 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 (ENS). La organización considerará otras normas de uso no obligatorio, pero de referencia, y específicamente la serie de Guías 800 publicadas por el Centro Criptológico Nacional CCN-CERT.

La organización debe cerciorarse que la seguridad es una parte integral de cada etapa del ciclo de vida del sistema y de la información, desde el diseño de un producto o un servicio hasta su retirada. Incluyendo las diferentes fases de desarrollo o adquisición y la propia producción o explotación. El sistema deberá estar diseñado para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad.

2 Estrategia corporativa

Se implanta una estrategia corporativa para garantizar la seguridad del sistema y el adecuado servicio prestado, lo que implica necesariamente que todos los recursos deben disponer y aplicar las medidas mínimas de seguridad exigidas, y en concreto las que sean de aplicación de las contenidas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

3 Objetivo de la Política de Seguridad de la Información

El objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con urgencia a los incidentes para recuperarse lo antes posible y minimizar el impacto.

Este objetivo de la política de la seguridad de la información se complementa por la protección de los activos que soportan el sistema de información de la organización y los procesos internos, implicados en los servicios declarados en este documento, quedando afectadas las tres dimensiones de seguridad –confidencialidad, integridad y disponibilidad-, y cuando fuera preciso, incorporando otras dimensiones –autenticidad y trazabilidad- (por requerimiento legal), quedando alineada plenamente con los objetivos de negocio e integrándose en la estrategia de la organización.

Por último, dicho objetivo deberá alinearse el requerimiento legal del Reglamento UE 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos – Reglamento General de Protección de Datos (RGPD), por lo que se considera a todos los efectos, este documento como el documento de alto nivel que declara la Privacidad como integrada en la Estrategia de Seguridad corporativa y en el Objetivo General de Seguridad.

3.1 Servicios

GISA tiene por objeto:

- Promover y fomentar la actividad económica y el empleo en el Municipio.
- Crear y gestionar empresas de servicios de utilidad pública y social.
- Crear y gestionar Centros de apoyo para las empresas y de servicios a las mismas.
- Prestar servicios de formación y asesoramiento en los diferentes ámbitos empresariales, a empresas y emprendedores, en especial a todos aquellos colectivos con especiales dificultades de inserción laboral o con riesgo de exclusión del mercado de trabajo. Todos los servicios se refieren a la creación, consolidación y puesta en marcha de nuevas empresas y procesos de emprendimiento.
- Gestionar los instrumentos y realizar los trámites que sean necesarios para facilitar la creación de nuevas empresas.
- Promover, gestionar y participar en proyectos que se soliciten a las diferentes Administraciones Públicas a nivel regional, nacional o comunitaria.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

- Promocionar y realizar estudios y análisis orientados a una eficaz movilización de los recursos y promoción del empleo.
- Promover, fomentar y actuar en iniciativas municipales en el ámbito de la economía social y en proyectos que requieran un fuerte impulso tecnológico y económico.
- Promocionar el Municipio de Getafe.
- Patrocinar, celebrar, fomentar e impulsar la celebración de toda clase de Ferias, Certámenes y Exposiciones.
- Promover y gestionar proyectos de interés público, y en este sentido desarrollar, gestionar y explotar suelo en su mayor amplitud, así como edificios y locales, que generen actividad económica y empleo en el Municipio.
- Realizar aquellas otras actividades que el Ayuntamiento de Getafe le encargue en el ámbito de la promoción de la actividad económica y generación de empleo del Municipio.

3.2 Objetivos particulares de seguridad de la información

Los objetivos de seguridad de la información definidos por GISA han sido desarrollados y aprobados por la Dirección, considerando los requerimientos identificados de las partes interesadas (internas y externas), la gestión de los riesgos y para cumplir con los requisitos de seguridad establecidos por la Alta Dirección.

La organización ha establecido como objetivos clave de la seguridad de la información, los siguientes:

- Mantener el pleno cumplimiento legal alineando los procesos y los servicios, a la normativa vigente en cada momento, y que afecta de manera indirecta o directa, al perfil de cliente (privado o administración pública), a la información implicada (pública, restringida o secreta) o en general a la seguridad de la información. Especial referencia al declarado Reglamento Europeo y en obviamente, al Real Decreto 3/2010.
- Mantener una gestión adecuada del sistema de gestión de seguridad, mediante la eficiencia y eficacia de la seguridad, de acuerdo a los estándares de seguridad y las buenas prácticas del sector.
- Alinear el requisito legal y la gestión del sistema con la privacidad y la seguridad.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información.
- Sensibilizar y concienciar de manera estable y permanente al usuario de la organización mediante el impulso de acciones por la Gerencia y la ejemplificación de la misma, en las tareas de seguridad más críticas.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

- Fomentar y mantener el buen nombre de la organización en relación a los servicios desarrollados, saber hacer y respuesta activa –reactiva y proactiva- ante incidentes de seguridad, manteniendo la imagen y reputación.
- Asegurar que los activos de la organización, sólo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, según perfiles definidos o según asignaciones extraordinarias.
- Gestionar la implementación de un sistema de seguridad que proporcione ventajas competitivas en relación a otros agentes del sector, aprovechando la inercia competitiva que puede otorgar la gestión adecuada de la seguridad.
- Proteger la información interna y la relacionada con la prestación de los servicios / clientes, considerando las dimensiones de:
    - Confidencialidad: Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
    - Integridad: Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
    - Disponibilidad: La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.

La organización podrá considerar otras dimensiones relacionadas con la seguridad, derivadas de requerimientos legales (o en su caso, de requerimientos de negocio), considerándose:

- Trazabilidad: Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
- Autenticidad: Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a dudas.

Por defecto la organización mantendrá las tres primeras dimensiones de seguridad. Cuando sea preciso se añadirán los dos restantes.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

4 Requisitos mínimos de Seguridad

4.1 Organización e implantación del proceso de seguridad.

GISA ha organizado su seguridad comprometiendo a todos los miembros de entidad, mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en los apartados Organización de la Seguridad y Anexo 2. Organización de la Seguridad del presente documento.

Se referencian los principios indicados en el apartado Seguridad basada en el liderazgo y en la organización, Seguridad basada en procedimientos y Seguridad como requisito legal.

4.2 Análisis y gestión de los riesgos.

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad de ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.

El Comité de Seguridad procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Se referencia el principio indicado en el apartado Seguridad gestionada en base al riesgo.

Se detalla en el " Procedimiento de Análisis de Riesgos".

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

4.3 Gestión de personal y Profesionalidad.

Todos los miembros de GISA, que se encuentran dentro del ámbito del ENS, recibirán acciones de concienciación en materia de seguridad. Se establecerá un programa de concienciación continua para atender a todos los miembros de GISA, en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

Se referencia el principio indicado en el apartado Seguridad considerando la gestión de recursos.

Se detalla en el **"Procedimiento de Gestión de personal"**.

4.4 Autorización y control de los accesos.

GISA ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Se detalla en el **"Procedimiento de Control de Accesos"**.

4.5 Protección de las instalaciones.

Se detalla en el **"Procedimiento de protección de instalaciones y equipos"**.

Se referencia el principio indicado en el apartado Seguridad de áreas y entorno.

4.6 Adquisición de productos.

GISA tendrá en cuenta, para la adquisición de productos, que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

Se detalla en el **"Procedimiento de Planificación"**.

4.7 Seguridad por defecto.

Se referencia el principio indicado en el apartado Seguridad por defecto.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

4.8 Integridad y actualización del sistema.

GISA ha implementado controles y evaluaciones regulares de la seguridad, para conocer en todo momento el estado de seguridad de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Se detalla en el "Procedimiento de Autorizaciones".

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4.9 Protección de la información almacenada y en tránsito.

GISA ha implementado mecanismos para proteger la información almacenado o en tránsito especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Se detalla en los "Procedimientos de protección de equipos" y "Protección de soportes".

4.10 Prevención ante otros sistemas de información interconectados.

GISA ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

a. Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
b. Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

Se detalla en el "Procedimiento de Protección de las Comunicaciones" y en el "Procedimiento de Protección de Aplicaciones y servicios"

4.11 Registro de actividad.

GISA habilitará los registros de la actividad de los usuarios, que se consideren necesarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del ENS, 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.

Se detalla en el "Procedimiento de Explotación".

4.12 Incidentes de seguridad.

GISA ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, GISA implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

Se detalla en el "Procedimiento de Brechas e incidentes de seguridad".

Se referencia el principio indicado en el apartado Seguridad considerando incidentes.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

4.13 Continuidad de la actividad.

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

Se detalla en el "Procedimiento de Copias de Seguridad".

También ha desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de sus competencias.

4.14 Mejora continua del proceso de seguridad.

GISA actualizará y mejorará de forma continua el proceso de seguridad integral implantado, aplicando los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de las tecnologías de la información.

Se detalla en el "Procedimiento de No Conformidades y Responsabilidad Proactiva".

5 Principios de Seguridad

La Dirección ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad.

El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por la Dirección. Existirá un procedimiento de gestión documental: PRO-DA-ENS-01 Procedimiento de Control de la Documentación, que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Todo el sistema estará enmarcado por los siguientes principios:

5.1 Seguridad por defecto

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde localizaciones o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso.

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

Para mantener el proceso de seguridad integral, se realizará una calificación de la información, conforme a los principios de protección frente a pérdidas, accesos indebidos, divulgación o uso indebido, deterioro de la información o pérdida de disponibilidad. La calificación conllevará necesariamente una política de etiquetado y manipulación.

5.2 Seguridad basada en el liderazgo y en la organización

La seguridad deberá comprometer a todos los miembros de la organización, en base a sus diferentes roles, considerando diferentes responsabilidades.

La Dirección será quien lidere la organización y promueve la cultura de seguridad, asignando los roles requeridos y potenciando la transversalidad de la seguridad en cada proceso desarrollado o servicio a terceros.

La seguridad del sistema será revisada de conformidad a los requisitos, la política y los procedimientos aprobados por la Dirección. Las revisiones serán por parte de la Dirección y por revisiones internas o auditorias del sistema. Específicamente la entidad y el sistema se podrán someter a procesos de certificación externos, conforme a lo establecido por el Esquema Nacional de Seguridad y cualquier otro estándar de seguridad que le pudiera interesar.

5.3 Organización de la Seguridad

Se establece una estructura organizativa en la organización, donde se establecerán roles específicos, pero siempre considerando el principio de separación de funciones. Se designarán a las personas que ocuparán los roles, cada dos años, pudiendo ser renovados automáticamente cuando transcurra el citado plazo y la Dirección no establezca una nueva persona para ocupar el cargo.

Mediante anexo a la presente Política se nombrarán y aceptarán los cargos. Como anexo se incorpora también las tareas preceptivas de cada rol establecido:

A) Comité de Seguridad:

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

Será el órgano encargado de desarrollar las directrices y estrategia de seguridad. Estará formado como mínimo por la Dirección, el Responsable de Seguridad y el Responsable del Sistema.

El Comité, puede recabar regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.

Este Comité será convocado cuando, aparezcan incidentes de seguridad graves y específicamente cuando surjan nuevas necesidades de seguridad.

El Comité se reunirá al menos una vez al año de manera ordinaria y extraordinariamente cada vez que sea necesario, con una convocatoria previa, de al menos 3 días laborales, efectuada por la Dirección, mediante correo electrónico. El Comité podrá ser requerido por el Responsable de Seguridad, en cuyo caso la Dirección deberá convocarlo en un periodo máximo de 15 días laborales.

B) Responsable del Sistema:

Será considerado el operador del sistema. Podrá incluso paralizar o dar suspensión al acceso a la información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

C) Responsable de Seguridad:

Gestionará la seguridad entendida como objetivo transversal u embebido en la estrategia corporativa. Mantendrá y verificará los requisitos de seguridad del sistema y de la información que se pudiera gestionar.

5.4 Seguridad basada en procedimientos

La seguridad del sistema se documentará mediante procedimiento de operación que serán puestos a disposición de los usuarios implicados en el mismo. Los cambios serán gestionados, las capacidades del sistema serán medidas y controladas y los entornos estarán separados. Se desarrollarán procedimientos de protección del sistema, incluyendo procedimientos de copias y restauración, y cuantas vulnerabilidades pudieran tener el sistema. Estas podrán tener forma de procedimiento general o especificaciones técnicas acordes a los operadores del sistema y de la seguridad.

Se documentarán los acuerdos con proveedores y colaboradores formando parte del sistema. La cadena de suministro será controlada con relación a los requisitos de seguridad, la prestación de servicios o los cambios de suministradores.

Las redes serán gestionadas, incluyendo cuando sea necesario, el cifrado o el control de comunicaciones.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

5.5 Seguridad gestionada en base al riesgo

La gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado en el seno de la organización, bajo el liderazgo de la Dirección.

La gestión de riesgos se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema de información y la organización, basándose en una metodología detallada y documentada que permita la repetición de la medición y análisis.

5.6 Seguridad considerando incidentes

El proceso de gestión de incidentes, incluirá la detección y notificación de los incidentes de seguridad, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas –especialmente cuando afecta a terceros- y el registro de las actuaciones ejecutadas.

Los incidentes de seguridad permitirán la recopilación de evidencias, de manera que se podrá identificar, documentar la recogida, la adquisición y preservación de la información.

5.7 Seguridad considerando la gestión de recursos

Todo el personal relacionado con el sistema y con la información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad, debiendo ser controlados y sus acciones supervisadas.

Cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se conozca, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

El usuario con acceso concedido al sistema, pueda o no desarrollar acciones, estará sometido a secreto y reserva, aun cuando finalice su relación con la organización. Ningún usuario accederá al sistema sin estar previamente informado de este extremo.

5.8 Seguridad de áreas y entorno

La organización prevendrá los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante controles físicos de acceso y protecciones generales en áreas.

Las áreas podrán ser de control propio o derivada al propio prestador afectado.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

5.9 Seguridad como requisito legal

La Gerencia ha establecido como requerimiento de seguridad, el pleno cumplimiento de las obligaciones legales y contractuales, ligadas a la información. Los requisitos serán identificados y organizados, para su correcta gestión.

Se incluye en la presente política anexo de detalle de normativa aplicable.

6 Alcance

La política de seguridad de la información, será de aplicación a toda la información del sistema con independencia del soporte o medio en el que se encuentre, tipología o categoría, a todo el personal de GISA y también a terceros colaboradores, que accedan al sistema y/o presten servicios a la organización, así como a cualquier activo de información propiedad de la organización, o en régimen de uso y que afecte al sistema, considerándose en cualquier momento del ciclo de vida del sistema de seguridad, de manera que cuando el sistema se encuentre en fase de actualización, el activo no registrado se vea obligado por la política.

Con respecto a los sistemas de información afectados por el Real Decreto 3/2010, la organización ha decidido, que el *alcance* de su sistema de SGSI-ENS, será:

"Sistemas de información que gestiona Getafe Iniciativas S.A. respecto a los servicios de asesoramiento a emprendedores y empresas; y desarrollo económico del municipio de Getafe, incluidos los Proyectos Europeos que puedan afectar al Municipio"

7 Cumplimiento

La Política de Seguridad de la Información tendrá vigencia desde la aprobación por el Comité de Seguridad y mientras no se apruebe una posterior, se mantendrá vigente. La Política de Seguridad será puesta en conocimiento de todos los afectados –internos y externos-.

La Política de Seguridad será alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al Responsable del sistema.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

Toda violación de la presente política o aquellas que la desarrollen, de las normas y procedimientos, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos que serán tramitados por su procedimiento oportuno.

8 Aprobación de la Dirección

La Dirección de GISA asume el compromiso de proveer todos los recursos y medios para la implementación la presente Política.

La Dirección demostrará su compromiso, mediante la revisión y aprobación de la Política y otras normas que desarrollaran el sistema, revisando los riesgos y aprobando el riesgo residual, participando en el Comité de Seguridad, promoviendo la cultura de seguridad, promoviendo la seguridad y especialmente, dotando de asignación efectiva a esta política mediante recursos y medios.

9 Anexos

9.1 Anexo 1. Legislación aplicable

Quedan implicadas todas las normas del sector, normas internacionales, comunitarias, nacionales, autonómicas y locales que sean de aplicación, pero específicamente por su relevancia en el tema, se detallan:

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. (Cuando sea de aplicación)

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (Cuando sea de aplicación)

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

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 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

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.

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

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 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril

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

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Real Decreto de 24 de julio de 1889, texto de la edición del Código Civil.

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

9.2 Anexo 2. Organización de la Seguridad

9.2.1 Responsable de Seguridad de ENS

Su función es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que lo establecido, se ha llevado a cabo.

Perfil:

Persona con visión de negocio, que pueda comprender los riesgos que afronta la organización, alineando los requisitos de seguridad con los requisitos de negocio.

Funciones:

a) Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, en su ámbito de responsabilidad.

b) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

c) Designar ejecuciones de análisis de riesgos, revisiones de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.

d) Validar los planes de continuidad.

e) Gestionar las revisiones externas o internas del sistema, incluyendo la recogida de indicadores específicos.

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

f) Gestionar los procesos de certificación.

g) Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.

Delegación de funciones:

GISA podrá designar cuantos Responsables de Seguridad Delegados considere necesarios, según lo establecido en la *Guía de Seguridad (CCN-STIC-801) Esquema Nacional de Seguridad - Responsabilidades y Funciones*. La designación corresponde al Responsable de la Seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable de la Seguridad. Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad. Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

9.2.2 Responsable del sistema

Su función es desarrollar las operaciones sobre el sistema que mantengan la plena seguridad.

Perfil:

Persona con perfil que pueda comprender la ejecución y el desarrollo de las operaciones sobre el sistema y con capacidad de servicio, desde una parcela más práctica y operativa, que conozca la arquitectura de la organización y las tecnologías aplicadas.

Responsabilidades:

a) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

d) El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos, previa consulta con el Comité y el Responsable de Seguridad, antes de ser ejecutada.

e) Llevar a cabo las funciones del administrador de la seguridad del sistema.

Delegación de funciones:

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

GISA podrá designar cuantos Responsables de Sistema Delegados considere necesarios, según lo establecido en la *Guía de Seguridad (CCN-STIC-801) Esquema Nacional de Seguridad - Responsabilidades y Funciones*. La designación corresponde al Responsable del Sistema. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable del Sistema. Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema. Cada delegado tendrá una dependencia funcional directa del Responsable del Sistema, que es a quien reportan.

9.2.3 Matriz de funciones

FUNCIÓN	RESPONSABLE	
Determinación de los niveles de seguridad requeridos en cada dimensión	Comité de Seguridad (Actuará cuándo sea necesario como Responsable de Servicio e Información)	
Análisis de riesgos	Responsable de Seguridad	
Declaración de aplicabilidad	Responsable de Seguridad	
Medidas de seguridad adicionales	Responsable de Seguridad	
Configuración de seguridad	Elabora	Responsable de Seguridad
	Aplica	Responsable de Sistema
Implantación de las medidas de seguridad	Responsable de Seguridad	
Aceptación del riesgo residual	Comité de Seguridad	
Documentación de seguridad del sistema	Responsable Seguridad	
Política de seguridad	Elabora	Responsable Seguridad
	Aprueba	Comité de Seguridad
Normativa de seguridad	Elabora	Responsable Seguridad
	Aprueba	Comité de Seguridad
Procedimientos operativos de seguridad	Elabora	Responsable del Sistema
	Aprueba	Responsable Seguridad
	Aplica	Responsable de Sistema
Estado de la seguridad del sistema	Monitoriza	Responsable de Seguridad
	Reporta	Responsable de Seguridad
Planes de mejora de la seguridad	Elabora	Responsable de Seguridad y Responsable del Sistema
	Aprueba	Comité de Seguridad
Planes de concienciación y formación	Elabora	Responsable de Seguridad
	Aprueba	Comité de Seguridad
Planes de continuidad	Elabora	Responsable del Sistema
	Valida	Responsable de Seguridad
	Aprueba	Comité de Seguridad

C/ Padre Blanco, 2
28901 Getafe (MADRID)
Tel. 91 665 36 20 - Fax 91 683 77 44
gisa@getafeiniciativas.es - getafeiniciativas.es

	Ejercicios	Responsable del Sistema
Suspensión temporal del servicio	Responsable del Sistema	
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	Elabora	Responsable del Sistema
	Aprueba	Responsable de Seguridad

9.2.4 Designaciones

El Comité de Seguridad, constituido válidamente y con plenas funciones, procede a designar los cargos derivados de la Política de Seguridad.

CARGO DESIGNADO	PERSONA DESIGNADA
Responsable de Seguridad ENS (Supervisión)	Gerente
Responsable de Seguridad Delegada	Directora Área Jurídica
Responsable del Sistema	Responsable Área de Nuevas Tecnologías y Comunicación
Presidente	Gerente
Responsables funcionales de Tratamiento	Se aprueban en las correspondientes actas de Aceptación.

En las convocatorias del Comité, el Presidente puede solicitar la asistencia en el Orden del Día, del personal Técnico interno o externo que considere oportuno.

DOCUMENTO FIRMADO ELECTRÓNICAMENTE