SGSI-01

Declaración Política de seguridad

Anexo manual

Versión 2.1

Fecha 14/10/2025

Referencia ISO/IEC 27001: apt 5.1
ENS Art 12

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

CATALOGACIÓN DEL DOCUMENTO

1		Documento interno restringido para		Dirección		Administración		Comercial		Personal Lieres	X	Todo el personal	
2		Documento externo de propuesta técnica y/o económica para un cliente											
3		Documento externo de contrato de prestación de servicios											
4		Documento externo de acuerdo o convenio											
5		Otros documentos externos											

DESTINATARIO DEL DOCUMENTO

Nombre o Razón Social	Gestión Avanzada del Desarrollo Digital

CONTROL DE CAMBIOS

Versión	*Fecha*	*Autor*	*Cambios realizados*
1.0	14-03--2011	-	Primera emisión.
1.1	10-10-2011	Isabel Casasola	Se modifica el texto de la notificación
1.2	17-01-2013	Isabel Casasola	Se crea este nuevo formato y todos los procedimientos se adaptan al mismo.
1.3	16-05-2018	Isabel Casasola	Adaptación al reglamento general de protección de datos
1.4	20/05/2020	Isabel Casasola	Adaptación a la Ley
1.5	16/08/2022	ISabel Casasola	Nuevo formato GADD. GTT adaptación Real Decreto 311/2022
1.6	03/10/2022	Isabel Casasola	Errata faltaba la dimensión de trazabilidad
1.7	22/11/2023	GADD	Adaptación a imagen corporativa
1.8	19/01/2024	GADD	Adaptación art 12 ENS 311/2022
1.9	27/03/2024	GADD	Puntualización renovación de roles
2.0	26/12/2024	GADD	Adecuación ISO 27001:2022
2.1	14/10/2025	GADD	Actualización de Roles conforme guía CCN-801

Realizado y Revisado por la Responsable de Sistemas de Gestión: Isabel Casasola Firmado Fecha 14/10/2025	Aprobado por la Dirección Firmado Rosa Perez 14/10/2025

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Declaración de la política de seguridad

La Dirección de GADD, es consciente de que la preservación de disponibilidad, integridad, autenticidad, trazabilidad y confidencialidad de la información y los datos asociados a las actividades de gestión avanzada para el desarrollo digital y todas las herramientas que se desarrollen en el ámbito de Gadd en todas sus tareas de gestión, administración, desarrollo, mantenimiento y soporte, desarrollados en la sede de la empresa en Lieres, es un factor esencial del negocio.

A través de su Sistema de Gestión basado en la Normativa ISO 27001 y el Real Decreto por el que se regula el Esquema Nacional de Seguridad en el ámbito *de la Administración Electrónica,* la Dirección del GADD adquiere un compromiso firme de satisfacer los requisitos contractuales, legales y reglamentarios aplicables al negocio y de mejorar su eficacia de forma y planificada.

El Comité de Seguridad de la Información aprobará 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 el Comité. Existe un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponderá al Comité de Seguridad de la Información la revisión anual de la presente Política aprobando, en caso de que sea necesario, mejoras de la misma.

Misión

En GADD, nuestra misión es garantizar la seguridad, integridad y disponibilidad de la información que gestionamos, tanto propia como de nuestros clientes.

Estamos comprometidos con la excelencia en la protección de los datos, aplicando de forma rigurosa los principios y controles definidos por la norma ISO/IEC 27001 y el Esquema Nacional de Seguridad (ENS) en su nivel Alto.

Nuestro objetivo es ofrecer soluciones tecnológicas seguras, útiles y adaptadas a las necesidades y normativas de cada cliente, proporcionando herramientas que refuercen su confianza y que contribuyan a su cumplimiento normativo.

En GADD entendemos la seguridad como un valor esencial y un compromiso compartido por todo el equipo, orientado a proteger la información y garantizar la continuidad del negocio.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Visión

Ser un referente en seguridad y cumplimiento normativo, reconocidos por la fiabilidad y robustez de nuestras soluciones y servicios.

Aspiramos a que nuestros clientes perciban a GADD como un socio estratégico en materia de seguridad de la información, capaz de anticiparse a los riesgos y de ofrecer software y servicios que garanticen el cumplimiento, la utilidad y la tranquilidad

Nuestra visión es evolucionar continuamente, integrando las mejores prácticas y tecnologías para mantener un entorno seguro, resiliente y alineado con los más altos estándares de protección, contribuyendo así a un ecosistema digital más seguro y confiable.

Responsabilidades dentro del ESQUEMA NACIONAL de SEGURIDAD

GADD organizará su seguridad comprometiendo a todas las personas integrantes de la organización, mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas

Con carácter general, todos y cada uno de los usuarios de los sistemas de información de la organización son responsables de la seguridad de la información, así como de los recursos y medios puestos a su disposición para el manejo de dicha información. En ellos recae la responsabilidad de un uso correcto, siempre de acuerdo a las atribuciones profesionales y competencias.

Como extensión a la estructura de seguridad, se establecerán relaciones de cooperación en materia de seguridad con las autoridades competentes, autonómicas o estatales, proveedores de servicios informáticos o de comunicación, así como organismos públicos y privados dedicados a promover la seguridad de los sistemas de información.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Funciones del comité de seguridad:

- Atender las solicitudes, en materia de Seguridad de la Información, de la organización y de las diferentes áreas, informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello, se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y, en particular, en materia de protección de datos de carácter personal.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Funciones del responsable de Seguridad

Es la persona responsable de la gestión y el mantenimiento del Sistema de Seguridad de la Información y de proporcionar ayuda y soporte a los propietarios de los activos de información para asegurar que se cumple la Política de Seguridad y que la información y los sistemas están adecuadamente protegidos. A continuación, se describen las responsabilidades principales del Responsable de Seguridad:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, en su ámbito de responsabilidad. Comprobación y supervisión de las medidas de seguridad
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Designar ejecuciones de análisis de riesgos, revisiones de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Determinar las medidas de seguridad aplicables, en función de las valoraciones hechas por los Responsables de la Información y los Servicios.
- Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y del Servicio.
- Determinación de la categoría del sistema, atendiendo a las valoraciones del Responsable de la Información y del Servicio.
- Validar los planes de continuidad.
- Gestionar las revisiones externas o internas del sistema, incluyendo la recogida de indicadores específicos.
- Gestionar los procesos de certificación.
- Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.
- Asegurarse de que el sistema de gestión de la información es conforme con los requisitos de la norma internacional ISO 27001.
- Informar a la alta Dirección sobre el comportamiento del sistema de Gestión de Seguridad de la Información.
- Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.
- En la gestión de los ciberincidentes, contando con los responsables de la información y de los servicios, calificará la peligrosidad de estos de acuerdo a la Guía CCN-STIC 817, actuando como punto de contacto con las autoridades competentes en materia de seguridad y, en función de los roles asignados en la Política podrá notificar los mismos, en su caso, al CCN-CERT. Cuando fuese precisa la notificación al CSIRT de referencia está deberá realizarse sin dilaciones indebidas y con carácter inmediato, sin perjuicio de la remisión de información ampliada de forma paulatina.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Y además:

- Asegurarse de que el software que se utiliza tiene licencia.
- Asegurarse de que los soportes y equipos que contengan información son desechados según lo establecido.
- Implementar las medidas de seguridad necesarias para evitar fraudes, robos o interrupción en los servicios.

La titularidad de esta figura se renovará de manera automática con carácter anual. Podrá ser modificada cuando desde dirección se considere necesario por cuestiones de personal, operativa o estrategia

Funciones del responsable del Sistema

El responsable de Sistemas y comunicaciones es responsable de la seguridad de los sistemas. Entre sus obligaciones están:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
  - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
  - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
  - Aprobar los cambios en la configuración vigente del Sistema de Información.
  - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.

- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

- Cuando la complejidad del sistema lo justifique el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

Además de:

- Gestionar todo el sistema ya asegurares que por directiva se cumplan.
- Administrar y gestionar las cuentas de los usuarios.
- Asegurarse de que sólo las personas autorizadas a tener acceso cuentan con él.
- Asegurarse de que los sistemas tienen los niveles de disponibilidad requeridos por la Organización.
- Incluir en los requisitos para nuevos desarrollos los aspectos de seguridad que apliquen.

La titularidad de esta figura se renovará de manera automática con carácter anual. Podrá ser modificada cuando desde dirección se considere necesario por cuestiones de personal, operativa o estrategia

Funciones del Responsable de la Información y de los Servicios:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, previa propuesta al Responsable de Seguridad, y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- Informar sobre los derechos de acceso al Servicio y a la Información.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.

La titularidad de esta figura se renovará de manera automática con carácter anual. Podrá ser modificada cuando desde dirección se considere necesario por cuestiones de personal, operativa o estrategia

Funciones del delegado de protección de datos:

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Corresponde al Delegado de Protección de Datos de GADD-GTT las funciones atribuidas a tal figura en el Reglamento UE 2016/679, de 27 de abril (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Tales funciones se ejercerán en los términos y condiciones y con el alcance señalados en la citada normativa.

La titularidad de esta figura se renovará de manera automática con carácter anual. Podrá ser modificada cuando desde dirección se considere necesario por cuestiones de personal, operativa o estrategia

Seguridad como proceso Integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- 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 emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean 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.
- Se 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

Este compromiso de la Dirección se articula mediante:

1. La participación de sus empleados/as y su influencia en sus respectivas áreas de responsabilidad.

2. El mantenimiento de las más estrictas normas éticas y profesionales, así como el empleo de códigos de buenas prácticas.

3. La dotación de los recursos humanos y materiales necesarios para su consecución, incluyendo la concienciación, el adiestramiento y la capacitación permanente del personal.

4. La asignación de funciones y responsabilidades específicas que permitan mantener los compromisos de Seguridad de la Información establecidos, así como la definición de roles de las personas Responsables de la información, Responsable de Seguridad, Responsable de Sistema TIC, Delegado/a de protección de datos, así como los responsables de los servicios, los activos que vienen desarrollados en la documentación de seguridad.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Que se han designado personas para dichos roles a la luz del principio de «separación de funciones», existiendo un acta de cada uno de los nombramientos, así como la creación de herramientas de resolución de los entre dichos responsables, asimismo, se ha constituido un Comité de Seguridad de la Información según dispone el ENS y se encuentra desarrollado en el manual y en los procesos.

5. La identificación, análisis, tratamiento y reevaluación de los riegos de seguridad de la información relacionados con sus servicios, sus activos y el negocio, mediante la aplicación de la metodología MAGERIT. Que se ha realizado un análisis de riesgos, y que se prevé su revisión y aprobación anual, o siempre que se den cambios sustanciales. La identificación, análisis, tratamiento y reevaluación de los riegos en materia de protección de datos de forma periódica, así como siempre que se produzcan cambios de relevancia en materia de datos personales dentro de la organización o bien se produzca una brecha de datos personales de acuerdo a la metodología establecida a este fin por parte de la Agencia Española de Protección de Datos. La identificación de estos riesgos y el tratamiento de los mismos tiene por objeto minimizar la posibilidad de que se produzca una brecha y la contención de la misma en caso de que tuviese lugar, reduciendo el impacto de la misma

6. La definición de un sistema de gestión de la seguridad, documentado en el que se intentan definir y procedimentar todas aquellas tareas que interrelacionan con la información y con un proceso regular de aprobación por la dirección, para ello se han tenido en cuenta las recomendaciones de protección descritas en el anexo II del ENS, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.

7. La gestión y el tratamiento responsable de los incidentes de seguridad de la información, previniendo su aparición o repetición.

8. La Revisión periódica y planificada del Sistema de Gestión, mediante auditorías, para incrementar su eficacia; mejorar la satisfacción de las partes interesadas; evaluar la eficacia y adecuación de esta Política; y establecer, seguir y revisar objetivos de seguridad de la información medibles y coherentes con la misma.

9. Vigilancia en cuanto comportamientos anómalos, así como la evolución de posibles vulnerabilidades y deficiencias de configuración. Periódicamente se reevaluará las medidas de seguridad de acuerdo a los riesgos detectados y los sistemas de protección existentes.

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

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adoptando las medidas oportunas para el establecimiento y aplicación de los criterios del deber de información, diferenciando la información básica y la información detallada, con especificación de los diferentes ámbitos de actuación de la organización la definición del procedimiento para el ejercicio de los derechos de los ciudadanos en materia de protección de datos, con establecimiento de procesos tipo para facilitar dicho ejercicio (https://www.gtt.es/gadd-gobierno-digital/) en el apartado intra-gadd, la definición y actualización de una política de privacidad adaptada a la normativa vigente en materia de protección de datos; el establecimiento de cláusulas tipo en materia de protección de datos en el ámbito de la contratación

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

administrativa; el asesoramiento de las diferentes unidades, servicios y órganos municipales en materia de protección de datos, así como el impulso de la conciencia que sobre dicha materia debe tener la Organización.

Incidentes de seguridad prevención, detección, respuesta y conservación

GADD implementará 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, la organización implementará 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, estarán claramente definidos y documentados.

Cuando se produzca 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.

GADD-GTT establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- Para garantizar la disponibilidad de los servicios, la organización dispondrá de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Resolución de conflictos

El Comité de Seguridad de la información se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

Terceras Partes:

Cuando la organización preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información. GADD, 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 actuaciones que lleve a cabo en materia de Seguridad en relación con otros organismos.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Cuando se haga uso de servicios de terceros o se ceda información a terceros, se les hará partícipe de esta Política de Seguridad y del Manual 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.

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 ENS que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

La organización 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.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- 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.

Autorización y control de los accesos

La organización implementa mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones

La organización implementa 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 comunes y críticas. En caso de que estos sean transferidos a un tercero se velará porque cumplan con todos los requisitos de en materia de seguridad establecidos en el real decreto por el que regula el esquema nacional de seguridad que sean de aplicación.

Adquisición de productos de seguridad y contratación de servicios de seguridad

GADD 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.

Todos aquellos terceros que provean servicios de seguridad a la organización o bien accedan a los sistemas o la información de la organización deberán acreditar la tenencia de certificado de acuerdo a Esquema Nacional de seguridad en la categoría de la organización en el alcance de la prestación del servicio, evidenciando además de esto el cumplimiento de los controles del RD 311/2022 que sean de aplicación para la misma.

Protección de la información almacenada y en tránsito y continuidad de la actividad.

La organización implementará mecanismos para proteger la información almacenada o en tránsito, especialmente cuando ésta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

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 desarrollarán procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de la organización. De igual modo, se implementarán mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren los documentos, para garantizar que toda información en soporte no electrónico relacionada estará protegida con el mismo grado de seguridad que la electrónica.

Se dispone así mismo de planes de continuidad de negocio a fin de asegurar planes de actuación en aras de la continuidad del negocio de la organización dentro del marco de la norma ISO 27001 y el real decreto por el cual se regula el esquema nacional de seguridad. En caso de activación de cualquier medida de continuidad, siempre se garantizará que los medios para la operación en degradado cumplen con todas las medidas de seguridad establecidas en los medios habituales de operación.

La organización dispone de políticas de borrado de metadatos y otras propiedades de documentos, así como auditorías periódicas de los mismos a fin de asegurar que no se producen filtraciones de autoría de documentos publicados o de otro tipo de información incrustada en archivos electrónicos puestos a disposición del público.

Registro de actividad y detección de código dañino

La organización habilitará registros de la actividad de los usuarios, 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 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.

En concreto, GADD dispondrá de una solución integral de antivirus, tanto en puestos de trabajo como en servidores, proporcionando de este modo una línea de defensa en todos los activos que dan soporte a los sistemas de información.

Legislación y normativa de aplicación

De manera complementaria a la especificada en este documento de política, GADD GTT recoge en el documento PCGADDGTT_04 Procedimiento legislación todas aquellas leyes, reglamentos, Directivas o Reales Decretos que le son de aplicación.

• Parque Tecnológico de Asturias, Parcela n.º 48, CL. Ablanal, n.º 13, C.P. 33428, Llanera (Asturias) 985193949 – info@gadd.gtt.es

Mejora continua del proceso de seguridad.

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.

La Dirección GADD reconoce que para la consecución de este compromiso es imprescindible la aportación y participación del personal de la empresa, su conocimiento y entendimiento, su sensibilización hacia la excelencia en la preservación de la seguridad de la información, en la satisfacción de terceras partes, en la eficacia y **mejora continua** del Sistema de Gestión y en la consecución de los objetivos y metas propuestos, por lo que difunde esta Declaración de la Política de Seguridad de la Información a todo el personal bajo su responsabilidad.

Periódicamente se realizan revisiones del sistema que lo soporta tanto en las medidas propias de gestión como aquellas de carácter técnico.

GADD. Grupo GTT, es una empresa que presta directamente servicios al Sector Público razón por la cual y en aras de completar su política de seguridad de la información, por ser esta junto con el personal sus principales activos, ha implementado y está en proceso de certificación de la Conformidad con el Esquema Nacional de Seguridad de “Sistema de información propiedad de GADD., para la consultoría, implantación, mantenimiento, soporte y desarrollo de software en modalidad Software como Servicio (SaaS) e instalación en cliente (on premise) para el sector público, en plataformas y servicios de administración electrónica, conforme a los requisitos del Real Decreto por el que se regula el Esquema Nacional de Seguridad y de conformidad con la declaración de aplicabilidad vigente”.
Fdo: Dirección GADD.GTT.

Firmado Rosa Perez