Política de Seguridad
(ENS Y TISAX)

01/10/2025



Objetivo y ámbito de aplicación 3
Los objetivos y misión de GRUPO DSA 3
Legislación y normativa de referencia 4
Principios y directrices 4
Prevención 4
Detección 5
Respuesta 5
Recuperación 5
REQUISITOS MÍNIMOS, PROCESO INTEGRAL Y DIRECTRICES 5
Organización e implantación del proceso de seguridad 6
Análisis y gestión de riesgos 6
Gestión de personal 6
Profesionalidad 7
Autorización y control de accesos 7
Protección de las instalaciones 7
Adquisición de productos y contratación de servicios de seguridad 7
Mínimo privilegio 8
Integridad y actualización del sistema 8
Protección de la información almacenada y en tránsito 8
Prevención ante otros sistemas de información interconectados 8
Registro de la actividad y detección de código dañino 8
Incidentes de seguridad 9
Continuidad de la actividad 9
Mejora continua del proceso de seguridad 9
Organización de la Seguridad de la Información 9
Estructura por Niveles de Responsabilidad 10
Dirección 10
Comité de Gestión de la Seguridad de la Información 10
Responsable de Seguridad 12
Responsables de la Información y de los Servicios 13
Responsable del Sistema de Información 13
Resolución de conflictos 13
Obligaciones del Personal 13
Asesoramiento Especializado en Materia de Seguridad 14
Asesoramiento especializado 14
Revisión independiente de la Seguridad de la Información 14
Protección de Datos de Carácter Personal 14
Formación y concienciación 14
Análisis y gestión de riesgos 15
Estructura normativa 15
Primer nivel: Política de Seguridad 15
Segundo Nivel: Normativas y Procedimientos de Seguridad 15
Tercer Nivel: Instrucciones Técnicas de Seguridad 15
Cuarto Nivel: Informes, registros y evidencias electrónicas 16
Calificación de la información. 16

Aprobación 16
Revisión de la documentación 17
Categorías de seguridad. 17
Otra documentación 17
Publicación de la política de seguridad 18
Entrada en vigor 18

Introducción

Desarrollo de Sistemas Avanzados, Advanced Mechanical Systems Xerez y Digital Energy System, en adelante GRUPO DSA, como muestra de compromiso con la seguridad de la información de sus sistemas ha desarrollado la presente Política de Seguridad de la Información, en adelante Política de Seguridad, de conformidad con lo establecido en el Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y el estándar TISAX solo para Desarrollo de Sistemas Avanzados, SL.

La Política de Seguridad es una declaración ética, responsable y de estricto cumplimiento en toda GRUPO DSA, la cual es desplegada a través de las diferentes Normativas y Procedimientos con los que se procura que los riesgos sean tratados adecuadamente.

El uso de los Activos de información debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información y los servicios.

Objetivo y ámbito de aplicación

- El objetivo de la Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales que puedan afectar a los sistemas de información necesarios para la prestación de los servicios, a información de nuestros clientes o la información propia considerada como confidencial.
- Este documento constituye el establecimiento de un marco organizativo y tecnológico en GRUPO DSA.
- Debe ser conocida y cumplida por todo el personal de GRUPO DSA, independientemente del puesto, cargo y responsabilidad dentro del mismo.
- Toda persona cuya actividad pueda, directa o indirectamente, verse afectada por los requisitos del Sistema de Gestión, está obligada al cumplimiento estricto de la Política de Seguridad.

Los objetivos y misión de GRUPO DSA

GRUPO DSA tiene como misión las siguientes actividades: diseño y fabricación de maquinaria especial y utillaje, fabricación de paneles eléctricos y mecanizado de piezas, diseño, desarrollo y mantenimiento de aplicaciones a medida, consultoría (e implementación de medidas) en ciberseguridad, consultoría energética e implementación de proyectos energéticos; siendo la misión para Desarrollo de Sistemas Avanzados, SL para TISAX la actividad de diseño y fabricación de maquinaria especial y utillaje.

Dentro de la visión, GRUPO DSA aspira a ser actores de referencia en los sectores de actividad a los que se dedica, garantizando la seguridad de la información manejada.

GRUPO DSA aspira a construir una empresa que se guíe fundamentalmente por los siguientes valores:

- Liderazgo: cada trabajador debe sentirse capaz de impulsar desde su posición el crecimiento, las oportunidades y el trabajo con visión de futuro.
- Flexibilidad: adaptándonos al cambio de forma ágil y buscando la productividad desde la responsabilidad y la autogestión.
- Confianza: interna y externa, guiándonos por la honestidad y la transparencia de nuestras acciones.

Legislación y normativa de referencia

El marco normativo de las actividades del GRUPO DSA en el ámbito de esta Política de Seguridad está integrado por requisitos legales del ámbito de la ciberseguridad y seguridad de la información, protección de los datos personales, comercio electrónico, propiedad intelectual, etc. La sistemática para la identificación y análisis de dichos requisitos legales se realiza a través del PMA02 Obligaciones y evaluación del cumplimiento.

Principios y directrices

Se entenderá la Seguridad como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

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

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes no se materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

Prevención

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

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

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

Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

Se deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar 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).

Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

REQUISITOS MÍNIMOS, PROCESO INTEGRAL Y DIRECTRICES

Se entenderá la Seguridad como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

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

- La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.
- La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción hasta su procesamiento, comunicación, transporte, almacenamiento, difusión a terceros y su eventual destrucción.
- (LA EMPRESA) protegerá la información de la difusión o manipulación no autorizada o pérdida de la misma.
- Los terceros que puedan acceder a la información propiedad de (LA EMPRESA) han de estar sometidos al control de los estándares definidos en cuanto a la seguridad de la información.

GRUPO DSA aplicará los siguientes requisitos mínimos:

Organización e implantación del proceso de seguridad

La seguridad de los sistemas de información deberá afectar a todos los miembros de la organización. Todos los integrantes de GRUPO DSA a través de la presente Política conocerán e identificarán los distintos roles y responsabilidades en materia de seguridad de la información.

Análisis y gestión de riesgos

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

Gestión de personal

Se implementarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos. Se deberá asegurar que todo el personal que tenga acceso a información recibe formación y concienciación periódica (personal propio como externo) en materia de Seguridad de la Información y protección de datos personales, especialmente en materia de confidencialidad de la información y detección, respuesta y prevención de incidentes o brechas de seguridad.

Profesionalidad

La seguridad de los sistemas de información estará a cargo, así como será revisada y auditada por personal cualificado, dedicado y formado en todas las fases del ciclo de vida. GRUPO DSA determinará los requisitos de información y experiencia del personal para el desarrollo del puesto de trabajo.

Autorización y control de accesos

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

Protección de las instalaciones

Tanto los sistemas de información como la infraestructura de comunicaciones asociada permanecerán en áreas controladas y dispondrán de mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

Adquisición de productos y contratación de servicios de seguridad

La contratación o adquisición de productos o servicios de seguridad deberá hacerse de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados.

Mínimo privilegio

Se deberá diseñar y configurar el sistema otorgando los privilegios mínimos para el desempeño de su puesto de trabajo.

Integridad y actualización del sistema

Deberán mantenerse actualizados todos los elementos, requiriendo autorización para su modificación y manteniendo una evaluación y monitorización continua.

Protección de la información almacenada y en tránsito

Se debe mantener una protección adecuada para los equipos o dispositivos portátiles, estableciendo procedimientos que permitan garantizar la recuperación y la conservación de este. Los dispositivos deberán mantener el mismo grado de seguridad que la entidad.

Prevención ante otros sistemas de información interconectados

Se debe mantener un perímetro de protección del sistema de información, dando una especial atención a la prevención, detección y respuestas a los incidentes de seguridad.

Registro de la actividad y detección de código dañino

Se debe mantener el tiempo estrictamente necesario la información que resulte adecuada para documentar las actividades indebidas o no autorizadas, con el fin de monitorizar la actividad del posible código dañino. Los usuarios que accedan a los sistemas deben estar identificados.

Incidentes de seguridad

Se deben disponer de procedimientos de gestión de incidentes de seguridad conforme a lo establecido en la normativa, debiendo establecer mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución.

Continuidad de la actividad

Se deben garantizar la existencia de copias de seguridad que actúen como mecanismo de restablecimiento del sistema en caso de ser necesario.

Mejora continua del proceso de seguridad

Se debe mantener un proceso de mejora continua de los procedimientos y mecanismos establecidos para garantizar el funcionamiento adecuado del sistema de seguridad.

Organización de la Seguridad de la Información

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 del ENS y según se detalla en la sección 3.1 del anexo II del ENS, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento.

Se establece una estructura jerárquica clara para la gobernanza y aplicación del principio de diferenciación de responsabilidades en materia de seguridad, complementando los roles ya definidos en el borrador:

Estructura por Niveles de Responsabilidad

Nivel	Rol / Órgano	Ubicación Jerárquica
Nivel 1	Órganos de Gobierno (Alta Dirección)	Responsable de la Información, Comité de Seguridad de la información, Responsable del Servicio (opcional)
Nivel 2	Dirección Ejecutiva (Gerencias)	Responsable de la Seguridad, Responsable del Servicio (opcional)
Nivel 3	Operacional	Responsable del Sistema

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la seguridad de la información de GRUPO DSA está compuesta por los siguientes agentes:

a) Dirección
b) El Comité de Gestión de la Seguridad de la Información.
c) El Responsable de Seguridad.
d) Responsables de la Información y de los Servicios.
e) Responsables del Sistema de Información.

Dirección

Es el responsable de aprobar la política de seguridad.

Comité de Gestión de la Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Gestión de la Seguridad de la Información, en adelante el Comité de Seguridad, dentro del ámbito de la presente Política de Seguridad formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en GRUPO DSA y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad.

Son funciones del Comité de Seguridad las siguientes:

a) Identificar los objetivos de GRUPO DSA en el ámbito de la Seguridad de la Información.

b) Elaborar la Política de Seguridad, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento.

c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en GRUPO DSA.

d) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnicos y de control, los sistemas y servicios de GRUPO DSA.

e) Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

f) Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a los exigidos en el ENS.

g) Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información.

h) Valorar el grado de conformidad de los procedimientos implantados en GRUPO DSA con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.

i) Supervisar la existencia e idoneidad de normativas y procedimientos de seguridad que se definan para dar cumplimiento y desarrollo a la Política de Seguridad.

j) Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

k) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.

l) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de Seguridad.

m) Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.

n) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de GRUPO DSA.

o) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en GRUPO DSA.

El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez al año, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

Responsable de Seguridad

Es el responsable de que los servicios y sistemas de información de GRUPO DSA se mantengan con el mayor grado de seguridad atendiendo a los principios de:

a) Confidencialidad: la información asociada a los servicios electrónicos al ciudadano solo debe poder ser conocida por las personas autorizadas para ello.
b) Integridad: la información asociada a los servicios electrónicos al ciudadano no debe ser alterada por personas no autorizadas.
c) Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios relativos a la Administración Electrónica permanecerán disponibles.

Son funciones del Responsable de Seguridad:

a) Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
b) Asunción de las funciones incluidas en los artículos 11, 28, 31.5, y Anexo III (apartados 2.1.b y 2.2.b) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
c) Asesorar en materia de seguridad a los integrantes de GRUPO DSA que así lo requieran.
d) Coordinar la interacción con otros organismos especializados.
e) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
f) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
g) Asesorar, en colaboración con el Responsable del Sistema, los Responsables de los Servicios y de la Información en la realización de los análisis y gestión de riesgos, elevando el informe resultado al Comité de Seguridad.
h) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
i) Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
j) Aprobar la categorización de los sistemas.

Respecto a la documentación, son funciones del Responsable de Seguridad:

a) Revisar y aprobar o escalar, la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
b) Supervisar la documentación de tercer nivel (Instrucciones técnicas) de obligado cumplimiento.
c) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

El responsable de Seguridad será nombrado y cesado por el Comité de Seguridad.

Responsables de la Información y de los Servicios

Son los responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS.

Son los responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

Son los encargados, contando con la participación y asesoramiento del responsable de Seguridad y del Responsable del Sistema de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

Son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Responsable del Sistema de Información

Personal designado cuyas responsabilidades son:

a) Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
c) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
d) Elaborar procedimientos técnicos de seguridad de los sistemas de información.
e) Podrá acordar la suspensión del manejo de determinada 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. Esta decisión deberá ser acordada con el Responsable de la Información y servicio afectados y el Responsable de Seguridad antes de ser ejecutada.

Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de protección de datos y seguridad de la información corresponderá, en última instancia, al Comité de Dirección, asistida por el Comité de Seguridad de la Información.

Obligaciones del Personal

Todo el personal, interno y externo, de GRUPO DSA tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, el Código Ético e incluso el Manual de

Gestión, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Asesoramiento Especializado en Materia de Seguridad

Asesoramiento especializado

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en GRUPO DSA con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

Revisión independiente de la Seguridad de la Información

El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en GRUPO DSA reflejan adecuadamente sus disposiciones.

Protección de Datos de Carácter Personal

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el 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).

Se exige la realización obligatoria de la Evaluación de Impacto relativa a la protección de los datos (EIPD) en los siguientes tratamientos:

- Evaluación sistemática y exhaustiva de aspectos personales que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente.
- Tratamiento a gran escala de las categorías especiales de datos (artículo 9.1 RGPD), o de los datos personales relativos a condenas e infracciones penales.
- Observación sistemática a gran escala de una zona de acceso público.

Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal de GRUPO DSA y a todas las actividades de acuerdo al principio de seguridad integral recogido en el art. 5 del ENS. A estos efectos, GRUPO DSA, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Análisis y gestión de riesgos

GRUPO DSA asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigente bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad.

Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, los Responsables de los Sistemas de Información realizarán, con periodicidad al menos anual, análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario.

Se realizará un análisis de riesgos:

- Regularmente, una vez al año.
- cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- cuando ocurra un incidente de seguridad grave.
- cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y éste al Comité de Seguridad.

Estas conclusiones, entre las que se incluirán los residuales y el riesgo objetivo, deberán ser aceptados y aprobados por el Comité de Seguridad.

Estructura normativa

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad de la Información.
- Segundo nivel: Normativas y Procedimientos de Seguridad.
- Tercer nivel: Instrucciones Técnicas de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de GRUPO DSA, recogido en el presente documento y aprobado por el Comité de Dirección.

Segundo Nivel: Normativas y Procedimientos de Seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad bajo la supervisión del Comité de Seguridad.

Tercer Nivel: Instrucciones Técnicas de Seguridad

Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión del Responsable de Seguridad. En caso de que los procedimientos afectarán a varios sistemas de información será responsabilidad del Responsable de Seguridad el aprobarlos.

Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito.

Calificación de la información.

Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.

Se establecen mecanismos para calificar la información en función de su naturaleza, estableciendo requisitos de acceso y control para el acceso a la misma y clasificándose de la siguiente forma:

La Política de Seguridad establece la clasificación de la información manejada por GRUPO uno según su **sensibilidad** para garantizar de manera efectiva la **confidencialidad**, **integridad** y **disponibilidad** de la misma. Esta clasificación determinará el conjunto de medidas de seguridad aplicables a los sistemas que la tratan.

Se definen los siguientes niveles de sensibilidad:

- **Restringida:** Información de **máxima sensibilidad** para GRUPO uno, cuya difusión, modificación o indisponibilidad no autorizada podría suponer un **perjuicio muy grave** (Nivel ALTO) para la organización o los individuos. Requiere las medidas de protección más rigurosas.
- **Interna:** Información menos sensible, de **uso exclusivo interno** de GRUPO uno. Si bien su difusión no autorizada está prohibida, no se espera de la misma un impacto negativo serio (Nivel BAJO a MEDIO) sobre las funciones de la organización.
- **Pública:** Información que ha sido **explícitamente aprobada** por la Dirección General de GRUPO uno para su divulgación al público general.

Aprobación

La documentación que es susceptible de necesidad de aprobación contará con una sección dentro del documento definida a tal fin donde quede contenida la firma del aprobador.

La versión aprobada será almacenada en la estructura de carpetas y el Responsable del Sistema de Información velará por la seguridad de sus metadatos a fin de prevenir modificaciones no autorizadas.

Revisión de la documentación

La documentación que es susceptible de necesidad de aprobación tendrá definidos los plazos y métodos de revisión y actualización de documentos.

Las versiones siguientes a la documentación inicial identificarán los cambios y el estado de la versión vigente de los documentos.

Los documentos se mantendrán accesibles, identificables y legibles de acuerdo a su calificación para los miembros autorizados que así lo requieran.

Para la documentación de origen externo, como resultados de auditorías externas, se llevará a cabo el control de su distribución.

Prevenir el uso de documentos obsoletos y aplicarles una identificación adecuada en el caso de que se mantengan por razones de utilidad para la Organización.

La documentación informal de los sistemas cuando vaya a servir de evidencia documental del cumplimiento de los controles se reestructurará de conformidad con lo descrito en la política de seguridad, de este modo la documentación contará con la aprobación del responsable del sistema y será sometida al mismo trato que el resto de documentación del ENS.

El Responsable de Seguridad, junto con los Responsables de la información y de los servicios velarán por el cumplimiento de la política de seguridad.

Categorías de seguridad.

La categoría de seguridad del sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I del ENS.

- Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

El responsable de cada información seguirá los criterios determinados anteriormente para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo con lo descrito anteriormente.

Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC.

Publicación de la política de seguridad

El presente documento se incluirá dentro del Sistema de Gestión de Seguridad de la Información del GRUPO DSA.

Entrada en vigor

La Política de Seguridad que se aprueba en este documento será aplicable a partir del día siguiente al de su firma.

Jerez de la Frontera 01 de octubre de 2025.

Director General (Jacob Jiménez Garrido)