GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Política de Seguridad de la Información y Calidad de INCIBE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017 TU AYUDA EN CIBERSEGURIDAD

ÍNDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 05 de septiembre de 2022 por la Dirección General de la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE).

Esta Política de Seguridad de la Información y Calidad de INCIBE es efectiva desde dicha fecha y lo será, hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

El Instituto Nacional de Ciberseguridad de España, en adelante INCIBE, depende de los sistemas TIC (Tecnologías de la Información y las Telecomunicaciones) para alcanzar sus objetivos. El uso de estos sistemas exige el establecimiento de un conjunto de actividades y procedimientos para el tratamiento y la gestión de los riesgos asociados a la seguridad de la información. La gestión de la seguridad de los sistemas de información es un proceso complejo que incluye a personas, tecnologías, normas y procedimientos.

INCIBE tiene presente que la ciberseguridad es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad, calidad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para todos los proyectos.

La aprobación de esta política manifiesta el interés y compromiso de INCIBE en cumplir con los requisitos aplicables y de mejora continua en la gestión de la seguridad de la información y la calidad en la prestación de sus servicios. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada, o a los servicios prestados.

Para INCIBE, el objetivo de la seguridad de la información es también garantizar la calidad de la información y la prestación adecuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el artículo 8 del Esquema Nacional de Seguridad (ENS), para lo que establecerá las medidas técnicas, organizativas y de control que garanticen la consecución de estos objetivos.

Por lo anterior, INCIBE establecerá un Sistema de Gestión Integrado (SGI) en sus vertientes de Seguridad de la Información y Calidad como instrumento necesario y facilitador de las operaciones del Instituto para atender las atribuciones y competencias de las que se dota al Instituto en el ámbito de actuación del Real Decreto-ley 12/2018, el Real Decreto-ley 43/2021, el Real Decreto 311/2022, el Plan de Choque de Ciberseguridad, el Plan España Digital 2025 y el propio Plan Estratégico de INCIBE; así como en el marco normativo que se recoge en el apartado 8 de esta Política.

El SGI de INCIBE resulta una necesidad para saber cómo gobernar y gestionar la tecnología utilizando estándares y buenas prácticas que nos ayuden a dar respuesta a los retos y desafíos de la realidad digital en la que estamos inmersos y que actuará tomando como base los siguientes principios y directrices, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que se maneja ni a los servicios prestados. Para ello actuará en 4 direcciones fundamentales:

2.1. Prevención

Para que la información o los servicios no se vean perjudicados por incidentes de seguridad, INCIBE implementará las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que identifique 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.

Para garantizar el cumplimiento de la Política, INCIBE se compromete formalmente a:

- 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.
- Velar por el mantenimiento y mejora constante de la gestión de la seguridad y la calidad, aportando los recursos necesarios.
- Asumir el establecimiento y revisión periódica de los objetivos de la seguridad de la información y la calidad, persiguiendo el alineamiento con la estrategia, la excelencia, la garantía en la prestación de servicios, la aportación de valor para las partes interesadas y la optimización de costes.
- Asegurarse de que esta Política es comunicada y entendida por todo el personal del Instituto y puesta a disposición de las partes interesadas, según sea apropiado.

2.2. Detección

INCIBE establecerá medidas de detección en sus sistemas de información con el objetivo de descubrir la presencia de ciberincidentes y anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS. Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

2.3. Respuesta

INCIBE establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en las diferentes áreas del Instituto o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con los incidentes. Esto incluye comunicaciones, en ambos sentidos, con INCIBE-CERT.

2.4. Conservación y recuperación

El sistema de información garantizará la conservación de los datos e información en soporte electrónico y para garantizar la disponibilidad de los servicios, INCIBE dispondrá de los medios, técnicas y procedimientos necesarios que permitan garantizar la recuperación de los servicios más críticos.

3. ALCANCE

3.1. Alcance subjetivo

Los sujetos obligados por esta Política son todo el personal de INCIBE y todas aquellas personas, instituciones, entidades o unidades y servicios, sean internos o externos, que presten servicios TIC al Instituto, sea en las instalaciones de INCIBE o en remoto.

3.2. Alcance objetivo

El alcance objetivo de esta Política comprende todos los sistemas de información[1] de INCIBE que den soporte a sus servicios y procesos, y afecta a todos los activos de información sustentados en ellos, así como a las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

4. REQUISITOS MÍNIMOS DE SEGURIDAD

La Política de Seguridad de la Información y Calidad de INCIBE articula la gestión continuada de la seguridad, siendo aprobada por la Dirección General. Esta Política se ha establecido de acuerdo con los principios básicos señalados en el capítulo II del ENS y se desarrolla teniendo en cuenta la aplicación de los siguientes requisitos mínimos de seguridad:

- Organización e implantación del proceso de seguridad (art. 13).
- Análisis y gestión de los riesgos (art. 14).
- Gestión del personal (art.15).
- Profesionalidad (art. 16).
- Autorización y control de los accesos (art. 17).
- Protección de las instalaciones (art. 18).
- Adquisición de productos de seguridad y contratación de servicios de seguridad (art.19).
- Mínimo privilegio (art. 20).
- Integridad y actualización del sistema (art. 21).
- Protección de información almacenada y en tránsito (art. 22).
- Prevención ante otros sistemas de información interconectados (art. 23).
- Registro de actividad y detección de código dañino (art. 24).
- Incidentes de seguridad (art. 25).
- Continuidad de la actividad (art. 26).
- Mejora continua del proceso de seguridad (art. 27).

Para dar cumplimiento a estos requisitos mínimos, INCIBE aplicará las medidas de seguridad indicadas en el Anexo II del ENS[2], teniendo en cuenta:

- Los activos que constituyen el sistema de información del Instituto.
- La categoría de seguridad del sistema, según lo previsto en el art. 40.

[1] El concepto "sistema de información" debe entenderse en sentido amplio, como "aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información." (UNE-EN ISO/IEC 27000:2021).

[2] Las medidas de seguridad referenciadas en el Anexo II podrán ser remplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos.

- Las decisiones que se adopten para gestionar los riesgos identificados.

5. PRINCIPIOS BÁSICOS

La Política de Seguridad de la Información y Calidad de INCIBE establece los siguientes principios básicos como directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información:

- Alcance estratégico: la seguridad de la información cuenta con el compromiso y apoyo de todos los niveles directivos de INCIBE, de forma que estará coordinada e integrada con el resto de las iniciativas estratégicas del Instituto para conformar un todo coherente y eficaz.
- Responsabilidad determinada: en los sistemas TIC se identifican el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- Seguridad integral: la seguridad es entendida como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información es considerada como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de riesgos: el análisis y gestión de riesgos es parte esencial del proceso de seguridad. La gestión de riesgos permite el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realiza mediante el despliegue de medidas de seguridad, estableciéndose un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se tienen en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- Proporcionalidad: el establecimiento de medidas de protección, detección y recuperación será proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: las medidas de seguridad son reevaluadas y actualizadas periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información es atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- Seguridad por defecto: los sistemas se diseñan y configuran de forma que se garantice su grado suficiente de seguridad por defecto.

6. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

INCIBE establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.

- Gestión de activos de información: los activos de información de INCIBE se encuentran inventariados y categorizados y están asociados a un responsable.
- Seguridad ligada a las personas: INCIBE implanta 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, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: INCIBE emplaza los activos de información en áreas seguras, protegidas por controles de acceso físico adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas están suficientemente protegidos frente a amenazas físicas o ambientales.
- Seguridad en la gestión de comunicaciones y operaciones: INCIBE establece los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmite a través de redes de comunicaciones está adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- Control de acceso: INCIBE limita 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, queda registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad del Instituto.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: INCIBE contempla los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los ciberincidentes: INCIBE implanta los mecanismos apropiados para la correcta identificación, registro y resolución de los ciberincidentes que se produzcan en sus sistemas de información.
- Garantizar la prestación continuada de los servicios: INCIBE implanta los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades del nivel de servicio de sus usuarios.
- Protección de datos: INCIBE adopta las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.
- Cumplimiento: INCIBE adopta las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

7. MISIÓN DE INCIBE

La S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas, y especialmente, para sectores estratégicos.

Como señala el Plan Estratégico 2021-2025, la misión de INCIBE es ser un motor para la transformación digital de la sociedad, protegiendo a ciudadanos, menores y empresas privadas en España y fomentando la industria de la ciberseguridad, el I+D+i y el talento.

De forma estrechamente relacionada con el cumplimiento de esta misión, INCIBE desea manifestar la necesidad de disponer y mantener una infraestructura TIC que prime y fomente servicios ciberseguros y de calidad para la consecución de sus objetivos estratégicos.

Fruto de este compromiso, INCIBE tiene implantado y certificado un Sistema de Gestión Integrado (en adelante, SGI) asentado en dos vertientes:

- La **seguridad de la información**, basada en un conjunto de medidas técnicas y organizativas que se integran en el marco de gestión **UNE-EN ISO/IEC 27001:2017**[3] y en el **Certificado de Conformidad con el ENS "categoría media"**[4], respecto a los requisitos regulados con el RD 3/2010, con objeto de analizar y tratar periódicamente los riesgos y alcanzar una adecuada gestión de la seguridad en sus dimensiones (C, I, D, A, T).
- La **calidad**, basada en un modelo de mejora continua en todos los procesos y resultados del Instituto, conforme a la norma **UNE-EN ISO 9001:2015**[5], como marco que implica el estricto cumplimiento de los requisitos establecidos por sus partes interesadas, y que promueve la búsqueda de la excelencia tanto en la aptitud y actitud de sus profesionales, como en la prestación de los servicios y en la ejecución de proyectos.

8. MARCO NORMATIVO

El marco normativo, sin carácter exhaustivo[6], en el que se desarrollan las actividades de INCIBE, y, en particular, la prestación de sus servicios electrónicos a los usuarios, está integrado por las siguientes normas:

- Ley 19/1988, de 12 de Julio, de auditoría de Cuentas y Real Decreto 1156/2005, de 30 de septiembre, por el que se modifica el Reglamento que desarrolla la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas, aprobado por el Real Decreto 1636/1990, de 20 de diciembre.
- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales y Ley 54/2003, de 12 de diciembre, de reforma del marco normativo de la prevención de riesgos laborales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto 1098/2001, de 12 de octubre Reglamento general de la Ley Contratos de las Administraciones Pública.
- Ley 17/2001, de 7 de diciembre, de Marcas. RD 687/2002 de 12 de julio por el que se aprueba el Reglamento de ejecución, y RD 306/2019 por el que se modifica este Reglamento.

[3] https://www.incibe.es/sites/default/files/certificado_sgsi_26102021.pdf

[4] https://www.incibe.es/sites/default/files/certificado_ens_25102021.pdf

[5] https://www.incibe.es/sites/default/files/certificado_sgc_08112021.pdf

[6] El detalle ampliado y en permanente actualización puede consultarse en el "Registro de Legislación Aplicable".

- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI).
- Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
- Ley 47/2003, de 26 de noviembre, General Presupuestaria.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y Real Decreto 1671/2009 de 6 de noviembre por el que se desarrolla parcialmente.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información.
- Real Decreto 1514/2007, de 16 de noviembre, por el que se aprueba el Plan General de Contabilidad.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 8/2011, de 28 de abril, por la que se establecen Medidas para la Protección de las Infraestructuras Críticas.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 36/2015, de 28 de septiembre de Seguridad Nacional.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- Real Decreto-ley 12/2018, de 7 de septiembre de seguridad de las redes y sistemas de información.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Ley 11/2020, de 30 de diciembre, de Presupuestos Generales del Estado para el año 2021.
- Real Decreto-ley 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

- Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.

Asimismo, cabe citar como complemento de este marco normativo:

- A nivel internacional, los siguientes estándares de referencia:
  - UNE-EN ISO 9001:2015 Sistemas de Gestión de la Calidad.
  - UNE-EN ISO/IEC 27001:2017 Sistemas de Gestión de Seguridad de la Información.
  - UNE-EN ISO/IEC 27002:2017 Código de prácticas para los controles de seguridad de la información.
- A nivel nacional, los siguientes marcos:
  - Estrategia Nacional de Ciberseguridad 2019 aprobada por el Consejo de Seguridad Nacional mediante Orden PCI/487/2019, de 26 de abril.
  - Estrategia de Seguridad Nacional 2021 aprobada por Real Decreto 1150/2021, de 28 de diciembre.
  - Agenda España Digital 2025 del Ministerio de Asuntos Económicos y Transformación Digital.
  - Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2019-2023.
  - Guía nacional de notificación y gestión de ciberincidentes.
  - Plan de Recuperación, Transformación y Resiliencia “España Puede”.
  - Foro Nacional de Ciberseguridad[7].

9. CUMPLIMIENTO DE ARTÍCULOS

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

El cumplimiento del articulado del ENS se recoge detalladamente en el documento *SOA ENS* (clasificación: DIFUSIÓN LIMITADA).

10. DESARROLLO DE LA POLÍTICA

El Comité de Dirección de INCIBE ha aprobado el desarrollo de un Sistema de Gestión Integrado, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad y calidad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad, ISO 27001 e ISO 9001. El sistema será documentado y permitirá generar evidencias de las salvaguardas y del cumplimiento de los objetivos marcados. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad y calidad del sistema, su gestión y acceso.

[7] El 22/02/2022 el FNC presenta los primeros resultados de sus grupos de trabajo. Los informes se centran en el estudio de la cultura de la ciberseguridad en España, el apoyo a la Industria e I+D+i y la definición de un **Esquema Nacional de Certificación para responsables**. https://www.incibe.es/sala-prensa/notas-prensa/el-foro-nacional-ciberseguridad-presenta-los-primeros-resultados-sus-grupos

Corresponde al Comité de Dirección de INCIBE la revisión anual de la presente Política proponiendo, en caso de que sea necesario, mejoras de la misma para su aprobación por parte de la Dirección General de INCIBE.

La Política de Seguridad de la Información y Calidad es de obligado cumplimiento y se estructura, a nivel documental, en los siguientes niveles relacionados jerárquicamente:

a) **Primer nivel**: Política de seguridad de la información y calidad.
b) **Segundo nivel**: Normativas y procedimientos de seguridad de la información y calidad.
c) **Tercer nivel**: Instrucciones técnicas operativas de seguridad de la información y calidad.

Esta estructura documental permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos de INCIBE. La Política se complementa con otras políticas, normativas y procedimientos de seguridad en diferentes materias.

El personal de INCIBE y terceras empresas que vayan a prestar sus servicios al Instituto tendrán la obligación de conocer y cumplir, además de la política de seguridad de la información y calidad, todas las normativas, procedimientos e instrucciones técnicas operativas de seguridad de la información y calidad que puedan afectar a sus funciones en el desempeño de su trabajo y/o prestación de los servicios; en particular, para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones que desarrollarán las Instrucciones Técnicas Operativas pertinentes y necesarias para su operativa, y cuyo conocimiento, uso obligado y difusión limitada aplicará a estos equipos de trabajo.

10.1. Primer nivel: Política

La Política de Seguridad de la Información y Calidad recogida en el presente texto y aprobada por la Dirección General de INCIBE constituye el primer nivel de la estructura documental de seguridad de la información y calidad del Instituto del que emana la documentación del segundo y tercer nivel.

10.2. Segundo nivel: Normativas y procedimientos

El segundo nivel desarrolla la Política mediante normativas y procedimientos específicos que abarcan un área o aspecto determinado de la seguridad de la información y la calidad.

Las normativas y procedimientos de seguridad de la información y calidad serán aprobados por el responsable de las áreas de conocimiento en materia de seguridad lógica y física, y desarrollarán, al menos:

- Gestión de activos de información inventariados, categorizados y asociados a un responsable.
- 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.
- Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

- Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que sea transmitida a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y criticidad, mediante mecanismos que garanticen su seguridad.
- Control de acceso, limitando 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.
- Adquisición, desarrollo y mantenimiento de los sistemas de información, contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información.
- Gestión de los incidentes de seguridad, implantando los mecanismos apropiados para la correcta identificación, registro y resolución.
- Gestión de la continuidad, implantando los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

10.3. Tercer nivel: Instrucciones Técnicas Operativas

El tercer nivel está constituido por directrices de carácter técnico que se deben observar en tareas o actividades relacionadas con la seguridad de la información y la calidad y la protección de los servicios, y que serán aprobadas por los responsables de su ámbito de competencia.

Dependiendo del aspecto tratado, se aplicarán a un ámbito específico o a un sistema determinado.

11. ESTRUCTURA ORGANIZATIVA[8]

Para garantizar que todas las etapas del ciclo de vida de protección de la información sean realizadas de manera apropiada y las responsabilidades para su ejecución sean asignadas adecuadamente, INCIBE establece una estructura organizativa que permite promover la aplicación consistente de la presente Política y acomodar efectivamente los cambios tecnológicos y organizativos.

La estructura organizativa que articula INCIBE diferencia niveles de responsabilidad de acuerdo con el principio básico de "**diferenciación de responsabilidades**" que recoge el artículo 11 del ENS, estableciéndose para cada nivel los siguientes **Comités** y **Roles** en la gestión y supervisión de la seguridad de la información y la calidad.

12. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables de información o de servicio que componen la estructura organizativa de la Política de Seguridad de la Información y Calidad de INCIBE, éste será resuelto por el superior jerárquico de los mismos[9].

[8] Guía CCN-STIC-801 sobre responsabilidades y funciones en el ENS (versión actualizada marzo 2019) y CCN-STIC-201 Organización y gestión para la seguridad de las TIC (versión actualizada enero 2021).

[9] Como establece la Guía CCN-STIC-801 en su párrafo 20, y de conformidad con lo dispuesto en el artículo 3 de la Ley 40/2015, las Administraciones Públicas, sirviendo los intereses generales, desarrollarán su actividad con plena observancia

13. DATOS PERSONALES

- INCIBE solo recogerá datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan recabado.
- INCIBE adoptará las medidas de índole técnica y organizativas, necesarias para el cumplimiento de la normativa de protección de datos vigente en cada caso.
- La gestión corporativa para el cumplimiento de la normativa de protección de datos corresponde al Departamento Jurídico de INCIBE. La Política de Protección de Datos Personales está publicada en el portal web de INCIBE.

14. GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política están sujetos a una gestión de riesgos[10] con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos la información, los servicios y dichos sistemas. El análisis de riesgos se repetirá regularmente[11]:

- Al menos una vez al año.
- Cuando cambien la información o los servicios manejados de manera significativa.
- Cuando ocurra un incidente de seguridad que ocasione un perjuicio grave[12], entendiéndose como tal lo especificado en el Anexo I del RD 311/2022.
- Cuando se reporten vulnerabilidades que pudieran ocasionar perjuicios graves, entendiéndose como tal lo especificado en el Anexo I del RD 311/2022.

Las fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, y siguiendo las normas, instrucciones, guías del CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el CCN.

En particular, para realizar el análisis de riesgos se utilizará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos elaborada por el Consejo Superior de Administración Electrónica).

15. REVISIÓN DE LA POLÍTICA

El marco normativo en materia de seguridad y calidad de INCIBE será revisado, al menos, anualmente. Toda nueva versión de un documento aprobado dentro del marco normativo será comunicada según el alcance de uso del documento y el nivel de difusión requerido

de los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación. Los conflictos entre distintos elementos de la organización serán resueltos por el superior jerárquico.

[10] Art. 7 del ENS: Gestión de la seguridad basada en los riesgos.

[11] Art. 10 del ENS: Reevaluación periódica.

[12] Anexo I del RD 311/2022, se entenderá por perjuicio grave:

1. La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2. Causar un daño significativo por los activos de la organización.
3. El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4. Causar un perjuicio significativo a algún individuo, de difícil reparación.
5. Otros de naturaleza análoga.

de forma que el personal que deba conocerlo maneje la versión válida y vigente en cada momento.

16. TERCERAS PARTES

- **Cuando INCIBE preste servicios a otros organismos o maneje información sensible de los mismos**, se les hará partícipe de esta Política, se establecerán canales de comunicación y colaboración entre los respectivos órganos de coordinación de la seguridad de la información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
- **Cuando INCIBE utilice soluciones y/o servicios de terceros[13], o ceda información a terceros**, se les hará partícipes de esta Política y de la Normativa de Buenas Prácticas para Entidades.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias[14]. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política. La entidad prestataria de los servicios externalizados designará un ***POC (Punto o Persona de Contacto)***.[15]

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad reguladas en la segunda disposición adicional del RD 311/2022, y en consideración a 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, *los operadores del*

[13] Como señala el artículo 2.3: "el RD 311/2022 también es de aplicación a los sistemas de información de las entidades del sector privado cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos".

[14] Como establece el art. 33.7 RD 311/2022 señala que: "Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien, sin perjuicio de sus competencias y de lo previsto en los artículos 9, 10 y 11 del Real Decreto 43/2021, de 26 de enero, en relación con la Plataforma de Notificación y Seguimiento de Ciberincidentes, lo pondrá inmediatamente en conocimiento del CCN-CERT.

[15] El art. 13.5 RD 3/2022 establece que: "en el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que CANALICE y SUPERVISE, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios".

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

17. MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario para INCIBE implantar un proceso permanente que comportará, entre otras acciones:

- Revisión de la Política de Seguridad de la Información y Calidad.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realización de auditorías internas o, cuando proceda, externas.
- Revisión de las medidas de seguridad.
- Revisión y actualización de las normas y procedimientos.

Para INCIBE, la gestión adecuada de la ciberseguridad constituye un reto continuo y colectivo al que necesariamente se ha de enfrentar.