Política de Seguridad ENS

Contenido

0 Versiones de este documento

Versión	Fecha	Descripción	Aprobación
3	06/07/2023	Se completan los principios básicos del ENS	Director general
2	01/02/2023	Adecuación al RD 311/2022	Director general
1	15/03/2021	Primera emisión	Director general

1 Misión y alcance

La misión y visión de la organización están recogidos en la "*Política del Sistema Integrado de Gestión*" que está publicada en la web de la organización.

Como parte de su política estratégica para el desarrollo de sus actividades**, INERZA S.A.** (en adelante **INERZA**), ha desarrollado e implementado un *Sistema Integrado de Gestión (SIG)* que abarca calidad, medioambiente, seguridad de la información y gestión de servicios TI, y que se encuentra basado en el análisis, la prevención y la mejora continua.

2 Marco normativo

2.1 Identificación

La sistemática utilizada por **INERZA** para la identificación, análisis y cumplimiento de la legislación y normativa vigentes se recoge en el procedimiento interno "*Manual del SIG*".

2.2 Datos de carácter personal

En el ámbito de los datos de carácter personal, **INERZA** ha realizado la adecuación a la "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales".

2.3 Esquema nacional de seguridad

En el ámbito del Esquema Nacional de Seguridad, está política está integrada por las siguientes normas:

- 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 (en adelante ENS).
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3 Principios básicos

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el *artículo 5* del ENS, por el que se regula el Esquema Nacional de Seguridad. Estos principios garantizarán que la organización cumplirá con sus objetivos, desarrollará sus funciones y ejercerá sus competencias.

3.1 Seguridad como proceso integral

La seguridad debe entenderse como un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

Se promoverá la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

3.2 Gestión de la seguridad basada en los riesgos

El análisis de los riesgos es parte esencial y continua del proceso de seguridad. La gestión de esos riesgos permitirá el mantenimiento de un entorno controlado, con dichos riesgos a niveles aceptables, y se realizará mediante la aplicación de medidas de seguridad de manera proporcionada a la naturaleza de la información tratada y de los servicios a prestar.

3.3 Prevención, detección, respuesta y conservación

La seguridad del sistema contempla medidas que implementen los aspectos de prevención, detección y respuesta ante incidentes de seguridad, y de conservación de la información y servicios en caso de que el incidente se produzca.

3.4 Existencias de líneas de defensa

INERZA implementa 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.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

3.5 Vigilancia continua y reevaluación periódica

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

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

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

Las medidas de seguridad se evaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

3.6 Diferenciación de responsabilidades

INERZA ha organizado su seguridad comprometiendo a todos los miembros de la organización mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge más adelante en este documento.

En los sistemas de información se diferenciará 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 seguridad, que determina las decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamiento de datos personales además se identificará el responsable de tratamiento y, en su caso, el encargado de tratamiento.

4 Requisitos mínimos de seguridad

a) Los responsables de velar por el cumplimiento de la política de seguridad están adecuadamente identificados y son conocidos por todos los miembros de la organización. *(Art. 13)*
b) El análisis y gestión de riesgos es parte esencial del proceso de seguridad y se mantiene permanentemente actualizado. *(Art. 14)*
c) La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de la organización deben protegerla, por lo que están adecuadamente formadas e informadas sobre sus deberes, obligaciones y responsabilidades en materia de seguridad. *(Art. 15)*
d) El personal encargado de atender, revisar y auditar la seguridad de los sistemas dispone de la cualificación necesaria y cumplen con los requisitos de formación y experiencia que establece la organización. *(Art. 16)*
e) Los sistemas de información son protegidos contra accesos y alteraciones no autorizadas. *(Art. 17)*
f) Todos aquellos activos (sistemas de información, infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside, se transporta o se procesa información, están debidamente protegidos. *(Art. 18)*
g) Para la adquisición de productos de seguridad y/o contratación de servicios de seguridad, se atenderá a las directrices marcadas por el Centro Criptológico Nacional (CCN), priorizando en todo caso aquellos productos y/o servicios que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. *(Art. 19)*

h) Todos los sistemas se diseñan y configuran de forma que garanticen el mínimo privilegio, proporcionando la funcionalidad imprescindible para lograr los objetivos de la organización. *(Art. 20)*
i) Todo elemento físico o lógico es autorizado previamente tanto a su instalación como a su modificación y son evaluados y monitorizados permanentemente con el fin de mantener un estado de seguridad de los sistemas óptimo. *(Art. 21)*
j) La información en formato físico o electrónico almacenada o en tránsito a través de entornos inseguros está debidamente protegida para garantizar su recuperación y conservación. *(Art. 22)*
k) Los sistemas de información están debidamente protegidos en todo su perímetro en general y en su conexión con redes públicas en particular. *(Art. 23)*
l) La monitorización y análisis de actividades indebidas o no autorizadas se realiza sobre la base de un registro de actividad respetuoso con el derecho al honor, intimidad personal y familiar y a la propia imagen de los usuarios, y de acuerdo con la normativa aplicable en protección de datos. *(Art. 24)*
m) La organización tiene debidamente implantados los procedimientos internos necesarios para una correcta gestión de los incidentes de seguridad. *(Art. 25)*
n) La organización dispone de un plan de continuidad del negocio y de un plan de copias de seguridad que garantizan la continuidad de los servicios. *(Art. 26)*
o) La Seguridad de la Información no es algo estático, está constantemente controlada y es periódicamente revisada dentro del ciclo de mejora continua PDCA de la organización. *(Art. 27)*
p) El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes la Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales.

4.1 Niveles de seguridad

Los niveles de seguridad requeridos para los diferentes sistemas de información vienen determinados por la categorización del sistema. **INERZA** desarrolla dicha categorización en el procedimiento interno "*ENS Categorización de los Sistemas*".

INERZA dispone de procedimientos internos donde se desarrollan las medidas de seguridad del ANEXO II del RD 311/2022 conforme al nivel de categorización vigente.

5 Organización de la seguridad

5.1 Roles y responsabilidades

La estructura organizativa, roles y responsabilidades de **INERZA** están definidos en el procedimiento interno "*Organigrama y funciones*". En el marco del ENS, la gestión de la seguridad de la información implica la existencia de una estructura organizativa que defina unas responsabilidades diferenciadas en relación a requisitos de información, requisitos del servicio y requisitos de seguridad, *(Art. 11)*.

INERZA articula esta diferenciación en el ámbito del alcance del ENS según la guía *CCN-STIC 801 ANEXO B. ESTRUCTURAS POSIBLES DE IMPLANTACIÓN*, a través de los siguientes roles:

- *Gobierno*: Comité *SIG*.
- *Supervisión*: Responsable de Seguridad.
- *Operación*: Responsable del Sistema.

5.2 Coordinación, nombramiento y resolución de conflictos

La coordinación se lleva a cabo en el seno del Comité de Dirección que podrá delegar en el Comité del *SIG*.

Los nombramientos los establece la Dirección de la organización y se revisan cada 2 años o cuando un puesto queda vacante.

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité del *SIG* y prevalecerá en todo caso el criterio de la Dirección.

6 Formación y concienciación

Las acciones específicas de concienciación y formación relativas al ENS se gestionan, sin distinción alguna, conjuntamente con las del *SIG*.

Dentro del marco del *SIG*, **INERZA** desarrolla su metodología en el procedimiento "*Manual del SIG*".

7 Análisis y gestión de riesgos

Un correcto análisis, identificación y gestión de los riesgos a los que se encuentran sometidos tanto los datos personales que trata la organización como los activos de información que sustentan los servicios de **INERZA**, es primordial para la correcta toma de decisiones de la Dirección.

La metodología de Análisis y Gestión de Riesgos adoptada por **INERZA** está basada en *MAGERIT v3* y se desarrolla en el procedimiento interno "*IT Análisis y gestión del riesgo*". Para su aplicación, **INERZA** emplea una herramienta propia.

8 Documentación de seguridad

La documentación relativa a la Seguridad de la Información estará clasificada en tres 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*: Informes, registros y evidencias electrónicas.

La aprobación de la documentación de seguridad depende de su nivel:

- *Primer nivel*: Alta Dirección
- *Segundo nivel*: Responsables de departamento
- *Tercer nivel*: n/a

8.1 Acceso

Las directrices para conceder accesos a la documentación se desarrollan en el procedimiento interno "*27001 – Control de accesos*".

8.2 Primer nivel: Política de seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente, desarrollados por **INERZA** en el marco de su *SIG* en los que se han incluido los aspectos específicos del ENS para cumplir con los requisitos mínimos de seguridad que marca su *artículo 12*, tal y como indica la guía *CCN-STIC 825 ENS – ESQUEMA NACIONAL DE SEGURIDAD CERTIFICATIONES 27001*, apartado 5.1. CUADRO RESUMEN.

Para facilitar la trazabilidad entre las medidas de seguridad requeridas por el ENS y su implantación en **INERZA** en el marco del SGSI, en la Declaración de Aplicabilidad del ENS se ha procedido a mapear las medidas de seguridad aplicables del Anexo II con los controles del Anexo A de ISO 27001. Realizado de acuerdo con la guía *CCN-STIC 825 ENS – ESQUEMA NACIONAL DE SEGURIDAD CERTIFICATIONES 27001*.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité del *SIG*.

8.3 Segundo nivel: Normativa y procedimientos de seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente, desarrollados por **INERZA** en el marco de su *SIG* en los que se han incluido los aspectos específicos del ENS para cumplir con los requisitos mínimos de seguridad que marca su *artículo 12*, tal y como indica la guía *CCN-STIC 825 ENS – ESQUEMA NACIONAL DE SEGURIDAD CERTIFICATIONES 27001*, apartado 5.1. CUADRO RESUMEN.

Para facilitar la trazabilidad entre las medidas de seguridad requeridas por el ENS y su implantación en **INERZA** en el marco del SGSI, en la Declaración de Aplicabilidad del ENS se ha procedido a mapear las medidas de seguridad aplicables del Anexo II con los controles del Anexo A de ISO 27001. Realizado de acuerdo con la guía *CCN-STIC 825 ENS – ESQUEMA NACIONAL DE SEGURIDAD CERTIFICATIONES 27001*.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité del *SIG*.

8.4 Tercer nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen evidencias generadas durante todas las fases del ciclo de vida de los sistemas de información, así como amenazas y vulnerabilidades de los sistemas de información.

8.5 Otra documentación

Se tendrán en cuenta, durante todo el ciclo de vida de los sistemas de información, los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC que publique el Centro Criptológico Nacional (*CCN*).

9 Documentación

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo a los requisitos generales del *SIG* que se desarrolla en el procedimiento interno "*Manual del SIG*".

10 Proceso de aprobación y revisión

Esta Política de Seguridad ENS es aprobada por el Director general y es revisada junto a la Política de los Sistemas de Gestión de forma periódica o cuando las circunstancias técnicas u organizativas lo requieran.

42867618B RUPERTO JOSE SANTANA (R: A35464452)

Firmado digitalmente por 42867618B RUPERTO JOSE SANTANA (R: A35464452)
Fecha: 2023.07.06 17:27:14 +01'00'