Política de Seguridad ENS

Revisión	Fecha	Motivo del Cambio
1	15/03/2021	Primera Emisión
Realizado y revisado Responsable de Seguridad		Aprobado Director General

Contenidos

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 "M *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 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- 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 Y DIRECTRICES

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el artículo 4 del RD 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, 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.

3.1. Prevención

INERZA evita que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos tienen implementadas 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, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **INERZA**:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, los servicios monitorizan 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 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS.

Están establecidos mecanismos de detección, análisis y reporte que llegan a las personas responsables regularmente y cuando se produce una desviación significativa de los parámetros preestablecidos como normales.

3.3. Respuesta

Se dispone de mecanismos para responder eficazmente a los incidentes de seguridad. El punto de contacto para las comunicaciones con respecto a incidentes es servicedesk@inerza.com. El protocolo para el intercambio de información relacionada con el incidente se establece por medio del procedimiento interno "*P Resolución y ejecución*".

Las comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CCN-CERT) se recogen en el procedimiento interno "*P Comunicaciones*".

3.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, **INERZA** dispone de un plan de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3.5. Requisitos mínimos de seguridad

a) Las personas responsables de velar por el cumplimiento de la política de seguridad están adecuadamente identificadas y son conocidas por todos los miembros de la organización.

b) El análisis y gestión de riesgos es parte esencial del proceso de seguridad y se mantiene permanentemente actualizado.

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 y concienciadas.

d) La formación es vital para mantener unos niveles de profesionalidad adecuados y un personal cualificado e instruido.

e) La información es protegida contra accesos y alteraciones no autorizadas, manteniéndola confidencial e íntegra.

f) Asimismo, La información está disponible, y se permite su acceso autorizado, siempre que sea necesario.

g) Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, es transportada o es procesada, están adecuadamente protegidos.

h) La seguridad en la adquisición de productos y contratación de servicios debe estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella.

i) Todos los sistemas se diseñan y configuran de forma que garantizan la seguridad por defecto, proporcionando la mínima funcionalidad requerida para lograr los objetivos de la organización.

j) Todo elemento físico o lógico es autorizado previamente a su instalación en el sistema.

k) La información almacenada o en tránsito a través de entornos inseguros está adecuadamente protegida.

l) Los sistemas de información están adecuadamente protegidos en su perímetro, en particular, en su conexión con redes públicas.

m) 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.

n) Los sistemas de detección y reacción frente a código dañino están adecuadamente implantados y son revisados permanentemente.

o) La continuidad de la actividad se garantiza protegiendo y asegurando la información contra pérdidas de disponibilidad e integridad a través de la política de copias de seguridad.

p) La Seguridad de la información no es algo estático, está constantemente controlada y periódicamente revisada dentro del ciclo de mejora continua PDCA de la organización.

q) 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. ORGANIZACIÓN DE LA SEGURIDAD

4.1. Roles y responsabilidades

La estructura organizativa, roles y responsabilidades de **INERZA** están definidos en el procedimiento interno "*M 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 con los requisitos de información, requisitos del servicio y requisitos de seguridad, (art. 10).

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

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

4.2. 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 General.

5. FORMACIÓN Y CONCIENCIACIÓN

Las acciones específicas de concienciación y formación relativas al ENS se gestionan, sin distinción con las del Sistema de Gestión de Seguridad de la Información, por el departamento de desarrollo de RRHH.

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

6. ANÁLISIS Y GESTIÓN DE RIESGOS

Un correcto análisis, identificación y gestión de los riesgos a los que se encuentran sometidos los activos de información, que sustentan los servicios de **INERZA**, es primordial para la correcta toma de decisiones de la Dirección de **INERZA**. Esto ha motivado a basar la Metodología de Análisis y Gestión de Riesgos del ENS en MAGERIT versión 3.

Para la implementación de la metodología de Análisis y Gestión de Riesgos se ha decidido utilizar una herramienta propia como se establece en el procedimiento interno *"IT Análisis y Gestión del Riesgo"*.

7. 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: Manuales y procedimientos de seguridad.
- Tercer nivel: Informes, registros y evidencias electrónicas.

7.1. Primer nivel: Política de seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de la organización, recogido en el presente documento.

7.2. Segundo nivel: Manuales y procedimientos de seguridad

De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente, desarrollados por **INERZA** en el marco de su *Sistema Integrado de Gestión* en los que se han incluido los aspectos específicos del ENS para cumplir con los requisitos mínimos de seguridad que marca su artículo 11, 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.

7.3. Tercer nivel: Informes, registros y evidencias electrónicas

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

7.4. Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC que publique el Centro Criptológico Nacional (CCN).

8. DESARROLLO Y DOCUMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

Esta Política se desarrolla por medio de las normativas de seguridad específicas, que se encuentran en el procedimiento interno "*P Políticas y normativa interna*".

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo con los requisitos generales del *Sistema Integrado de Gestión* que se recogen en el procedimiento interno "*M Manual del SIG*".

La normativa de seguridad está a disposición de todos los miembros de la organización en el repositorio documental de la misma.

9. PROCESO DE APROBACIÓN Y REVISIÓN

Esta *Política de Seguridad de la Información ENS* es aprobada por el Director General, entra en vigor el día de su aprobación y es revisada junto a la Política de los Sistemas de Gestión de forma periódica o cuando las circunstancias técnicas u organizativas lo requieran.