POLÍTICA DE SEGURIDAD ENS

REGISTRO DE EDICIONES

Edición	Fecha	Descripción del cambio
1.0	31/05/2016	Redacción inicial.
1.1	01/04/2019	Cambios en la codificación de los documentos
1.2	01/01/2020	Cambios como consecuencia auditoría interna: roles y responsabilidades. Quitar a CV del alcance.
1.3	10/06/2020	Modificación para incluir todos los requisitos ENS según la guía CCN-STIC-805 como consecuencia de NC de auditoría externa 2020.

Contenido

1 MISIÓN Y ALCANCE

Desde su fundación en 1982, Signe se ha especializado en el diseño y desarrollo de soluciones de seguridad documental, produciendo y editando documentos -tanto en soporte papel como digital- protegidos contra posibles falsificaciones y modificaciones fraudulentas.

Como parte de su política estratégica para el desarrollo de sus actividades, Grupo SIGNE, (Signe S.A. y ADOS), ha desarrollado e implantado de un Sistema Integrado de Gestión de Calidad, Medio Ambiente, Seguridad de la Información e Impresión de Seguridad, basado en el análisis, la prevención y la mejora continua.

La misión, visión y valores de la organización están recogidos en la "GSIGNE. POLÍTICA DE LOS SISTEMAS DE GESTIÓN" que está publicada en la web de la organización.

Considerando que parte de las actividades del Grupo se realizan para y/o en nombre de organismos de la Administración Pública, Grupo Signe ha decidido implantar, en el marco de la seguridad de la información, las medidas establecidas en el Esquema Nacional de Seguridad para estas actividades. En concreto, el ENS se aplica a:

"Los sistemas de información que dan soporte a las actividades de emisión de documentos en formato electrónico y certificación electrónica asociada a documentos de seguridad, de acuerdo al documento de determinación de la categoría vigente".

Estas actividades se pueden realizan desde las instalaciones del Grupo ubicadas en:

- Oficinas Tres Cantos: Avda. de la Industria, 18, 28760 Tres Cantos, Madrid.

2 MARCO NORMATIVO

2.1 Identificación

Grupo Signe realiza sus actividades en el marco normativo de la impresión de seguridad y la certificación electrónica. La sistemática utilizada por Grupo Signe para la identificación, análisis y cumplimiento de la legislación y normativa vigentes se recoge en el procedimiento general "GSIGNE-GRAL-PR-09 Cumplimiento legal", que se mantiene debidamente actualizado.

2.2 Datos de carácter personal

En el ámbito de los datos de carácter personal, Grupo Signe 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". Dentro de esta adecuación se han desarrollado las nuevas cláusulas del deber de información, nuevos contratos de ETD, RAT, análisis de riesgos, análisis de necesidad de EIPD, etc.

La información documentada relativa al RGPD se encuentra alojada en el recurso de red "\\sistemas gestión\16 - RGPD".

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

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 (o servicios externos contratados) 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.

3.2 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 9 del ENS.

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

3.3 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).

3.4 Recuperación

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

3.5 Otros principios generales

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- 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 deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- 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 del Grupo Signe están definidos en los documentos “GSIGNE-GRAL-MSG Manual de Sistemas de Gestión”, “GSIGNE-RRHH-MO Manual de Organización” y “GSIGNE-RRHH-PR-01 Funciones y Responsabilidades”.

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. 10).

Grupo Signe articula esta diferenciación en el ámbito del alcance del ENS a través de los roles (CCN-STIC 801 ANEXO B. ESTRUCTURAS POSIBLES DE IMPLANTACIÓN):

- Gobierno:
  - Dirección ejecutiva asesorada por el CSG
- Supervisión:
  - Dirección de SI
- Operación:
  - Departamento de sistemas

4.2 Coordinación, nombramiento y resolución de conflictos

La coordinación se lleva a cabo en el seno del Comité de Dirección. Podrá delegar en el Comité de Sistemas de Gestión.

Tanto los nombramientos como la posible resolución de conflictos correrán a cargo de la Dirección Ejecutiva.

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 RRHH.

La sistemática seguida por Grupo Signe para la detección de necesidades de formación y concienciación y para darles curso se describe en el procedimiento “GSIGNE- RRHH-PR-03 Formación”.

6 GESTIÓN DE RIESGOS

Una correcta identificación y gestión de los riesgos a los que se encuentran sometidos los activos de información, que sustentan los servicios de cara al ciudadano de Signe, es primordial para la correcta toma de decisiones de la Dirección de Signe. 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 la herramienta PILAR como se establece en el procedimiento interno GSIGNE-SI-PR-01 Gestión del riesgo - 01 metodología ENS - 01 Texto.

7 DESARROLLO DE LA POLÍTICA

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: Procedimientos Técnicos de Seguridad.
- Cuarto 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 y aprobado mediante Decreto de la Organización.

7.2 Segundo Nivel: Normativas y Procedimientos de Seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente, desarrollados por Grupo Signe en el marco de su Sistema 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 CCN-STIC 825 ENS - NATIONAL SECURITY FRAMEWORK 27001 CERTIFICATIONS, apartado 5.1. SUMMARY TABLE.

Para facilitar la trazabilidad entre las medidas de seguridad requeridas por el ENS y su implantación en Grupo Signe 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 de Seguridad (CCN-STIC 825) Esquema Nacional de Seguridad – Certificaciones 27001.

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

7.3 Tercer Nivel: Procedimientos Técnicos 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 afectaran a varios sistemas de información será responsabilidad del Responsable de Seguridad el aprobarlos.

7.4 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.

7.5 Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500 y 600.

8 DOCUMENTACIÓN

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo a los requisitos generales del Sistema Integrado de Gestión que se recogen en el procedimiento general "GSIGNE-GRAL-PR-01 Control de la documentación".

Toda la información documentada relativa al Sistema Integrado de Gestión se aloja en el recurso de red "\\sistemas gestion".

Respecto a la calificación de la información, se documenta en el procedimiento "GSIGNE-SI-PR-08 Gestion de activos".

9 PROCESO DE APROBACIÓN Y REVISIÓN

Esta Política de Seguridad de la Información ENS será aprobada por la Dirección Ejecutiva y revisada junto a la Política de los Sistemas de Gestión de forma periódica o cuando circunstancias técnicas u organizativas lo requieran para evitar que quede obsoleta.

Eduardo Quintero Barona

Firmado digitalmente por Eduardo Quintero Barona
Fecha: 2020.06.10 14:19:11 +02'00'

Dirección Ejecutiva de SIGNE, S.A.
10 de junio de 2020.