Política de Seguridad de Enusa

ENUSA Industrias Avanzadas, S. A., S. M. E.

Sistemas de Información

Contenido

I. Objetivo

El Manual y Política de Seguridad de la Información queda establecido como el documento de alto nivel que formaliza las diferentes directrices de actuación en materia de seguridad adoptadas por ENUSA, y que serán desarrolladas en mayor detalle en la correspondiente normativa de seguridad elaborada a tales efectos.

Bajo esta premisa, por tanto, el Manual y Política de Seguridad de la Información contempla los siguientes objetivos principales:

- Dar cumplimiento a la normativa legal de aplicación en el ámbito de la seguridad de la información.
- Contribuir a cumplir con la misión y objetivos estratégicos establecidos por ENUSA.
- Alinear la seguridad de la información con los requerimientos demandados por el negocio mediante la formalización y ejecución del proceso de análisis y evaluación de los riesgos a los que se encuentran expuestos los distintos activos de información, alcanzando la definición de una estrategia para la mitigación de los riesgos relacionados con el entorno de la seguridad de la información.
- Garantizar la protección adecuada de los distintos activos de información en función del grado de sensibilidad y criticidad alcanzado por los mismos (valor de seguridad de los activos de información según las distintas dimensiones consideradas: confidencialidad, integridad y disponibilidad).
- Facilitar el dimensionamiento de los recursos necesarios para la correcta implantación de las medidas de seguridad de índole técnica y organizativa recogidas en la normativa de seguridad documentada a tales efectos.
- Fomentar el uso de buenas prácticas en materia de seguridad de la información, así como crear una cultura de seguridad en el contexto de la estructura organizativa de ENUSA.
- Impulsar la definición, implantación y mantenimiento de un Plan de Continuidad de Negocio.
- Establecer los mecanismos de revisión, monitorización, auditoría y mejora continua con el objeto de mantener los niveles de seguridad oportunos demandados por el modelo de negocio de ENUSA.

II. Alcance

El Manual y Política de Seguridad de la Información contempla en su alcance la totalidad de los activos de información existentes en ENUSA y que actúan como infraestructura de soporte para la posible ejecución de los procesos de negocio de los centros de trabajo de Madrid, Juzbado y Saelices.

Este Manual y Política de Seguridad de la Información aplica a todo el personal que desarrolle su actividad en ENUSA, estando obligado a cumplir todas las disposiciones, aquí recogidas, que le afecten.

III. Marco Normativo

La formalización de la Política de Seguridad de la Información, así como la normativa de seguridad que se derive de la misma, tendrá en consideración e integrará la siguiente normativa legal aplicable:

- 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 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- 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, modificado por Real Decreto 951/2015, de 23 de octubre.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto RD 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Guía de seguridad 10.9: Garantía de calidad de las aplicaciones informáticas relacionadas con la seguridad de las instalaciones nucleares.
- UNE-73-404: "Garantía de la calidad de los sistemas informáticos aplicados a las instalaciones nucleares".
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

IV.Cumplimiento de artículos del Esquema Nacional de Seguridad

ENUSA, para lograr el cumplimiento de los artículos 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, que recogen los principios básicos y de los 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.

Seguridad como un proceso integral y seguridad por defecto

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad a ENUSA, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a 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.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Reevaluación periódica e integridad y actualización del sistema

ENUSA ha implementado controles y evaluaciones regulares de la seguridad 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.

Gestión de personal y profesionalidad

Se establecerá un programa de concienciación continua en ENUSA para atender a todos los empleados, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Gestión de la seguridad basada en los riesgos y análisis y gestión de riesgos

Todos los tratamientos de datos personales así como los procesos cuyo índice de criticidad sea superior al valor umbral definido en la matriz de criticidad de ENUSA, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos cada una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad, prevención, detección, reacción y recuperación

Los principios fundamentales que deben contemplarse a la hora de garantizar las dimensiones de la seguridad de la información son la prevención, detección, reacción y recuperación, de manera que las potenciales amenazas existentes no se materialicen o, en

caso de materializarse, no afecten gravemente a la información precisa para la ejecución de los procesos de negocio de ENUSA, manteniéndose en unos niveles aceptables con relación al impacto causado.

ENUSA debe prevenir y evitar, en la medida de lo posible, que la información de negocio se vea perjudicada por incidentes de seguridad. Para ello, se deben implementar las medidas de seguridad que queden identificadas tras la ejecución del proceso de análisis y evaluación de los riesgos. Estos controles, así como los roles y responsabilidades formalizados en materia de seguridad, están claramente definidos y documentados.

Dado que los sistemas de información pueden degradarse rápidamente debido a incidentes de seguridad que pueden ir desde una simple desaceleración 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.

Esta monitorización es especialmente relevante cuando se establecen líneas de defensa en los términos considerados por las buenas prácticas de referencia en materia de seguridad de la información.

En el supuesto de que la degradación sea atribuida directamente a incidentes de seguridad, deberán establecerse los mecanismos oportunos de reporte que lleguen al Responsable de Seguridad para su análisis e investigación de las causas.

ENUSA establecerá mecanismos para responder eficazmente a los incidentes de seguridad.

Para garantizar la disponibilidad de los servicios, ENUSA dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa y prevención ante otros sistemas interconectados

ENUSA ha implementado 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.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada y organización e implantación del proceso de seguridad

ENUSA 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 en el apartado de "Organización y Responsabilidades" del presente documento.

Autorización y control de los accesos

ENUSA ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones

ENUSA ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos, ENUSA tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito y continuidad de la actividad

ENUSA ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de ENUSA. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad

ENUSA ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

V. Estructura

La normativa de seguridad establecida por ENUSA se estructura en los siguientes niveles relacionados jerárquicamente:

a) Nivel I: Política de Seguridad de la Información

b) Nivel II: Estándares de Seguridad de la Información

c) Nivel III: Procedimientos de Seguridad de la Información

d) Nivel IV: Instrucciones específicas de Seguridad de la Información

Esta estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en el entorno operativo de ENUSA sin necesidad de revisar su estrategia de seguridad.

El personal de ENUSA tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todos los estándares y procedimientos de seguridad que puedan afectar a sus funciones.

La normativa de seguridad estará disponible en la intranet de ENUSA.

5.1. Nivel I: Política de Seguridad de la Información

Recogida en el presente documento, ha sido aprobada formalmente por el Comité de Seguridad de la Información, y detalla las directrices de actuación de ENUSA en materia de seguridad de la información con el objeto de contribuir al cumplimiento de la misión formalizada por la Dirección.

5.2. Nivel II: Estándares de Seguridad de la Información

El segundo nivel desarrolla la Política de Seguridad de la Información mediante la identificación de los objetivos de seguridad considerados para los distintos dominios de seguridad:

- Seguridad relativa a los recursos humanos
- Gestión de activos de información
- Control de accesos
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones

- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Relación con proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- Cumplimiento

Los objetivos de seguridad y, por ende, las medidas de seguridad que deben ser implantadas sobre los distintos activos de información para garantizar las dimensiones de seguridad de la información en los distintos procesos de ENUSA, se encuentran, de igual forma, clasificados en tres niveles de seguridad, según las exigencias consideradas en cada caso (valores de seguridad alcanzados para los activos de información que actúan como soporte para la ejecución de los procesos de negocio).

Los estándares de seguridad deberán ser aprobados por la Dirección con carácter previo a su formalización y divulgación.

5.3. Nivel III: Procedimientos de Seguridad de la Información

El tercer nivel está constituido por procedimientos técnicos y organizativos de actuación que recogerán el conjunto de actividades y tareas que deben ser ejecutadas con el objeto de dar cumplimiento a los objetivos de seguridad formalizados a través de los distintos estándares de seguridad documentados, según el valor de seguridad alcanzado por el activo de información.

Estas pautas de actuación serán de aplicación específica según los distintos dominios de seguridad considerados y detallados en el nivel de estándares de seguridad (Nivel II).

Los procedimientos de seguridad deberán ser aprobados por el Responsable de Seguridad con carácter previo a su formalización y divulgación.

5.4. Nivel IV: Instrucciones específicas de Seguridad de la Información

Las instrucciones específicas de trabajo serán documentadas con el objeto de personalizar la aplicación de un procedimiento para un activo de información concreto y, por tanto, presentará el detalle de las actividades y tareas a ejecutar en el contexto de dicho activo de

información para dar cumplimiento a lo establecido en el procedimiento de seguridad del cual deriva dicha instrucción.

Las instrucciones específicas de seguridad de la información aun cuando forman parte de la normativa de seguridad de ENUSA, serán documentadas según el consenso alcanzado por el Responsable de Seguridad y la organización de Sistemas de Información en función de la complejidad de entendimiento en lo relativo a la aplicación de lo establecido en el procedimiento para un activo de información concreto.

Las instrucciones específicas de seguridad de la información serán aprobadas internamente por la organización de Sistemas de Información tras el consenso alcanzado con el Responsable de Seguridad.

VI. Organización y Responsabilidades

La organización de la seguridad en ENUSA queda establecida mediante la identificación y definición de las diferentes funciones y responsabilidades consideradas en esta materia.

6.1. Comité de Seguridad de la Información

Actúa como máximo órgano de control y supervisión en materia de seguridad de la información.

6.1.1. Composición

El Comité de Seguridad de la Información está conformado por los siguientes miembros permanentes:

- Director Técnico de Sistemas y Transformación Digital (en calidad de Presidente)
- Delegado de Protección de Datos (DPD)
- Responsable de Gestión de la Seguridad de Juzbado
- Responsable de Gestión de Calidad
- Responsable de Transformación Digital y Mejora Continua
- Responsable de Sistemas de Información (en calidad de Secretario)
- Responsable de Seguridad de la Información
- Responsable de Explotación
- Representante de la Dirección de Auditoría Interna
- Responsable de Coordinación Económica y Proyectos

Representante de Relaciones Industriales, responsable de Organización y Desarrollo y representante de Asesoría Jurídica que no formarán parte permanente del CSI pero que podrán ser consultados en materias de su competencia.

6.1.2. Funciones

- Aprobar formalmente la Política de Seguridad de la Información y la normativa de seguridad (estándares, procedimientos e instrucciones) que se deriven de la misma.
- En caso de cambios que originen una nueva versión de la Política de Seguridad de la Información, aprobar formalmente dicha nueva versión.

• Aprobar las iniciativas que estime oportunas para mejorar la seguridad de la información.

• Monitorizar los incidentes de seguridad de mayor relevancia notificados por el Responsable de Seguridad de la Información.

• Ejecutar el proceso de asignación de responsabilidades para la estructura organizativa establecida en materia de seguridad.

6.1.3. Resolución de conflictos

6.2. El Comité de Seguridad de la Información se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad. Asignación de Responsabilidades.

La asignación de responsabilidades en materia de seguridad se encuentra debidamente alineada con las competencias funcionales formalizadas en el contexto de la estructura organizativa de ENUSA.

Director Técnico de Sistemas y Transformación Digital

• Presidir las reuniones del Comité de Seguridad de la Información.

• Aprobar el análisis y evaluación de los riesgos identificados en el contexto de la seguridad de la información.

• Exponer al Comité de Dirección las necesidades y propuestas identificadas en materia de seguridad como estrategia para la mitigación de los riesgos.

Representante de Relaciones Industriales

• Asesorar en materia de relaciones laborales y su interrelación con las responsabilidades de los empleados en materia de seguridad de la información.

• Comunicar la baja de empleados al Responsable de Seguridad de la Información.

Delegado de Protección de Datos

• Asesorar en el ámbito de los requerimientos legales relacionados con el entorno de protección de datos y seguridad de la información.

• Asesorar en el ámbito de los requerimientos contractuales que deben ser formalizados en la relación con terceros y específicos del entorno de protección de datos y seguridad de la información.

• Comunicar cualquier brecha de seguridad que se produzca en el entorno de la protección de datos.

Responsable de Organización y Desarrollo

• Planificar los seminarios de formación y concienciación de empleados en materia de seguridad de la información.

• Comunicar las altas de empleados y cambios de organización al Responsable de Seguridad de la Información.

Responsable de Gestión de la Seguridad

• Integrar la seguridad de la información en el contexto de la seguridad general.

Dirección de Auditoría Interna

• Planificar las auditorías necesarias en materia de seguridad de la información y protección de datos de carácter personal, junto con el Delegado de Protección de Datos.

Responsable de Transformación Digital y Mejora Continua

• Colaborar en la ejecución del análisis y evaluación de riesgos y en la emisión de la documentación relacionada con la seguridad de la información.

Responsable de Sistemas de Información

• Proponer mejoras tecnológicas hardware y software en materia de seguridad.

• Aprobar las instrucciones de trabajo relacionadas con la seguridad de la información.

• Coordinar la actualización del análisis y evaluación de riesgos.

• Licenciar y auditar los productos instalados según lo acordado con el suministrador.

Responsable de Seguridad de la Información

• Desarrollar inicialmente la Política de Seguridad de la Información para su aprobación formal en el Comité de Seguridad de la Información.

• Formalizar y divulgar la normativa de seguridad que emana de la Política de Seguridad de la Información.

• Monitorizar el correcto cumplimiento de los objetivos de seguridad recogidos en los estándares de seguridad.

• Verificar la implantación de las medidas de seguridad consideradas mediante la ejecución de análisis de riesgos periódicos.

• Realizar el seguimiento de las incidencias de seguridad de la información, coordinando la respuesta oportuna junto con el Delegado de Protección de Datos, en caso de que las incidencias afecten a datos de carácter personal.

• Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información con el detalle de los incidentes más relevantes y el nivel de respuesta actual.

• Promover la planificación de auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

• Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.

• Establecer puntos de enlace con especialistas externos que le permitan la identificación de tendencias, normas y métodos de seguridad pertinentes.

• Coordinar la definición, implantación y mantenimiento de un Plan de Continuidad de Negocio para los distintos procesos considerados críticos.

• Firmar en calidad de emisor el análisis y evaluación de riesgos.

Responsable de Explotación

• Desarrollar, operar y mantener la infraestructura tecnológica y de comunicaciones durante todo su ciclo de vida, garantizando el correcto funcionamiento.

• Implementar las mejoras tecnológicas aprobadas.

• Crear y actualizar los documentos de instalación, configuración, contingencia y copia de seguridad de cada uno de los activos hardware informáticos.

• Gestionar el control de accesos de los usuarios y administradores.

• Firmar en calidad de verificador el análisis y evaluación de riesgos.

Responsables de organizaciones propietarias de la información

• Definir los criterios de clasificación de la información según las distintas dimensiones de seguridad consideradas, valorando el impacto que podría provocar la presencia de determinados incidentes de seguridad.

• Participar junto con el Responsable de Seguridad en los preceptivos análisis de riesgos, identificando los niveles de riesgo residual aceptables.

• Notificar al Responsable de Seguridad de la Información y al Delegado de Protección de Datos si la información tratada contiene datos de carácter personal.

• Notificar al Responsable de Seguridad de la Información los roles de acceso a la información.

• Solicitar el archivo de la información de un proyecto. Se solicitará mediante una incidencia de archivo de información en la aplicación correspondiente. En la petición de archivo se indicarán los años a mantener la información. Una vez cumplido el periodo de archivo de información, los soportes que la contengan serán destruidos físicamente.

Usuarios

• Conocer y cumplir la Política de Seguridad, así como la normativa de seguridad que se deriva de la misma y que sea de aplicación en el desempeño de sus funciones.

• Colaborar en la notificación al Responsable de Seguridad de la Información de toda incidencia que se detecte relativa a la seguridad de la información, y al Delegado de Protección de Datos en caso de que la incidencia afecte a datos de carácter personal.

• Utilizar los servicios informáticos para el propósito establecido.

• Obtener el certificado electrónico para su uso en las aplicaciones donde se encuentre instalada la firma electrónica.

• Gestionar la seguridad informática en aquellos servicios donde la administración quede delegada en el propietario del servicio (servidores de ficheros, carpetas públicas de correo, etc.).

• Quienes intervengan en cualquier fase de tratamiento de los datos de carácter personal están obligados a guardar secreto de todos los datos a los que accedan o tengan acceso, así como a tratar los mismos de tal manera que se garantice la seguridad de dichos datos de carácter personal, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Obligaciones que subsistirán aún después de finalizar sus relaciones con ENUSA.

• Los usuarios responsables de la contratación de servicios con terceros están obligados a obtener de éstos la conformidad con relación a las cláusulas de confidencialidad oportunas.

6.3. Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de los roles de seguridad ENS:

Funciones del Responsable de la Información y de los Servicios

• Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta al Responsable de Seguridad de la Información, y/o Comité de Seguridad de la Información

• Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad

El rol de responsable de Seguridad lo ejerce el Responsable de Seguridad de la Información que tiene estas funciones asociadas al ENS:

• Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.

• Promover la formación y concienciación en materia de seguridad de la información.

• Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.

• Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.

• Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.

• Gestionar las revisiones externas o internas del sistema.

• Gestionar los procesos de certificación.

• Elevar al Comité de Seguridad de la Información la aprobación de cambios y otros requisitos del sistema.

Funciones del responsable del Sistema

El rol de responsable del Sistema los ejerce el responsable de Sistemas de Información que tiene estas funciones asociadas al ENS:

• Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

• Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

• Elaborar los procedimientos operativos necesarios.

• Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

• Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

• Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.

• Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

• Llevar a cabo las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

VII. Personal

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, así como el cumplimiento de la legalidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos y también de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental formar e informar al personal desde su ingreso en la empresa y de forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y protección de datos personales así como cualesquiera asuntos de confidencialidad.

Por ello y con el fin de alcanzar este objetivo, ENUSA establece criterios y requisitos relacionados con la seguridad de la información en los Puestos de Trabajo, en la Contratación del Personal, en los Procedimientos de altas y bajas de usuarios de aplicaciones informáticas y en la Concienciación y Formación del personal.

7.1. Requisitos del Puesto de Trabajo

En función del puesto de trabajo que desempeñe el personal, los requisitos exigidos serán acordes con las funciones y responsabilidades que se hayan asignado.

7.1.1. Todo el Personal

Todos los empleados de ENUSA deberán:

• Conocer, comprender y comprometerse a cumplir las directrices y normas relativas a la seguridad de la información según se establecen en los diferentes documentos del SGSI.

• Conocer, comprender y comprometerse a cumplir las directrices y normas en materia de protección de datos de carácter personal.

• Guardar estricta Confidencialidad con la información que manejan y a la que tienen acceso.

• Aceptar y cumplir las condiciones de uso de Sistemas de Información.

• Colaborar en la comunicación de las debilidades detectadas en materia de seguridad, así como de los incidentes ocurridos con el objeto de minimizar sus efectos y prevenir su incidencia.

7.1.2. Personal de Sistemas de Información

Las responsabilidades en materia de Seguridad de la Información se desarrollan en cada uno de los procedimientos e instrucciones de Sistemas de Información específicos, siendo de obligado cumplimiento.

7.2. Contratación de Personal

ENUSA tiene establecidos, en sus procesos de selección de personal, los mecanismos adecuados para garantizar la idoneidad de los solicitantes en cuanto a su compromiso con el cumplimiento de sus funciones y responsabilidades dentro de la empresa.

El proceso y las pautas a seguir en la selección y contratación del personal, se encuentran definidos en el Procedimiento de Operación de ENUSA correspondiente.

7.3. Acceso a los Sistemas de Información

El alta de un usuario en los Sistemas de Información vendrá definida por el responsable directo quién, teniendo en cuenta las funciones y responsabilidades de su puesto de trabajo, definirá las aplicaciones a las que tendrá acceso y con qué perfil (usuario, administrador…) debe ser dado de alta. Igualmente la baja será responsabilidad de quien haya solicitado el alta, que lo comunicará a Sistemas de Información para que proceda.

El proceso a seguir, así como las herramientas y las actividades a realizar, se desarrolla en una instrucción de Sistemas de Información.

7.4. Concienciación, Formación y Competencia del Personal

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, ENUSA asegura, mediante los procedimientos adecuados, que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI está suficientemente capacitado.

Con el fin de alcanzar este objetivo:

• En el Manual de Formación de Sistemas de Información, se definen y determinan las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.

• Dichas necesidades se satisfacen por medio de la formación adecuada, regulado por el Procedimiento de Operación de ENUSA aplicable.

• Para evidenciar dichas competencias, se mantienen los registros de estudios, formación, habilidades, experiencia y cualificación que sean necesarios.

Además, ENUSA pondrá los medios para que todo el personal esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI. Por este motivo y con el fin de asegurar la implantación y correcto funcionamiento del SGSI, establece un plan de formación para todo el personal, destinado a su sensibilización con los requisitos y riesgos asociados a la Seguridad de la Información.

Este plan de formación consiste en que anualmente y mediante los mecanismos que se consideren adecuados en cada momento (charlas, presentaciones, intranet…), se informará/formará a todo el personal con el fin de concienciarle sobre la importancia de las responsabilidades de cada uno en la Seguridad de la Información. Esta formación quedará debidamente documentada mediante los registros oportunos.

VIII. Terceras Partes

Cuando ENUSA requiera de la participación de terceras partes para la prestación de un servicio, les hará participes de la normativa de seguridad que sea de consideración en el contexto de dicha colaboración, quedando éstos sujetos a las obligaciones establecidas en dicha normativa.

Se formalizarán los procedimientos específicos de reporte y resolución de incidencias que pudieran presentarse durante la prestación del servicio.

Cuando algún aspecto de la normativa de seguridad no pueda ser satisfecho por una tercera parte, se requerirá la autorización del Responsable de Seguridad de la Información previa identificación de los riesgos en que se incurre y la forma de tratarlos, no siendo posible la formalización de la contratación con carácter previo a la obtención de dicha autorización.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

IX. Revisión

La política de seguridad de la Información será revisada anualmente por el Responsable de Seguridad o cuando exista un cambio significativo (enfoque de la gestión de la seguridad, circunstancias del negocio, cambios legales, cambios en el ambiente técnico, recomendaciones realizadas por autoridades de control, tendencias relacionadas con amenazas y vulnerabilidades) que obligue a ello.

En el caso de que se obtenga una nueva versión de la Política de Seguridad de la Información, será precisa la aprobación formal del Comité de Seguridad de la Información con carácter previo a su divulgación.

Sistemas de Información

Edificio ENUSA
Santiago Rusiñol 12, pl. baja
28040 Madrid
Telf.: 913474200
comunicacion-interna@enusa.es