POLÍTICA DE SEGURIDAD DE ENUSA
ENUSA Industrias Avanzadas, S. A., S. M. E.

Indice

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).
- 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.

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.

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.
- 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”.

Principios

Los principios fundamentales que deben contemplarse a la hora de garantizar las dimensiones de la seguridad de la información son la prevención, detección, respuesta 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.

Prevención

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, deben estar claramente definidos y documentados.

Detección

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.

Respuesta

Se deben establecer mecanismos para responder eficazmente a los incidentes de seguridad.

Recuperación

Para garantizar la disponibilidad de los procesos críticos, se deben desarrollar planes de contingencia de los sistemas de información y comunicaciones como parte del plan general de continuidad de negocio y actividades de recuperación de la organización.

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.

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.

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.

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.

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.

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.

Comité de Seguridad de la Información

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

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 Organización y Desarrollo
- Responsable de Gestión de la Seguridad de Juzbado
- Responsable de Gestión de Calidad
- Responsable de 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, Cumplimiento y RSC
- Responsable de Coordinación Económica y Proyectos

Representante de Relaciones Industriales que no formará parte permanente del CSI pero podrá ser consultado en materias de su competencia.

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.

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, Cumplimiento y RSC

- 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 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Edificio ENUSA
Santiago Rusiñol 12
28040 Madrid
Telf.: 913474200
comunicacion@enusa.es