Política de Seguridad (ENS)

Mayo 2024

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
ITSEC-POL-UNEI- Política de Seguridad (ENS)	1.00	Primera versión.	10/06/2022
ITSEC-POL-UNEI- Política de Seguridad (ENS) v2	2.00	Adaptación Real Decreto 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 Fecha firma electrónica	
ITSEC-POL-UNEI- Política de Seguridad (ENS) v3	3.00	Revisión Consultora	17/01/2023
ITSEC-POL-UNEI- Política de Seguridad (ENS) v4	4.00	Revisión interna	12/04/2023
TSEC-POL-UNEI- Política de Seguridad (ENS) v5	5.00	Revisión interna	30/04/2024
TSEC-POL-UNEI- Política de Seguridad (ENS) v6	6.00	Revisión interna	10/05/2024

CLASIFICACIÓN

INFORMACIÓN PUBLICA

Índice

Introducción

El **Grupo UNEI**, en adelante UNEI, como muestra de compromiso con la seguridad de la información de sus sistemas ha desarrollado la presente Política de Seguridad de la Información, en adelante Política de Seguridad.

El Sistema de Gestión de la Seguridad de la Información implantado en el Grupo UNEI debe dar respuesta a los requisitos establecidos al respecto en la legislación vigente aplicable a la actividad de la entidad y cuyas referencias constan en la "Registro de Legislación aplicable" (Normativa legal aplicable ENS.pdf).

El mantenimiento del marco normativo será responsabilidad del Responsable de CALIDAD que mantendrá el "Registro de Legislación Aplicable", incluyendo las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

La Política de Seguridad es una declaración ética, responsable y de estricto cumplimiento en toda UNEI, la cual es desplegada a través de las diferentes Normativas y Procedimientos con los que se procura que los riesgos sean tratados adecuadamente.

El uso de los Activos de información debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información y los servicios.

UNEI comprende la totalidad del Grupo UNEI, que está compuesta por cuatro sociedades:

- Unei Grupo Social, S.A., con C.I.F. A-41431891
- Unei Iniciativa Social, S.L.U., con CIF B-41610825. Nº Calificación CEE 66/93-SE.
- G.E.S. JAÉN, S.L., con CIF B-23313158. Nº Calificación CEE 73-JA.
- Recursos a Domicilio, A.I.E., con CIF G-91367243.

El objetivo de la Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información frente a amenazas, internas o externas, deliberadas o accidentales que puedan afectar a los sistemas de información necesarios para la prestación de los servicios, a información de nuestros clientes o la información propia considerada como confidencial.

Alcance

El alcance son los sistemas que dan soporte a los Servicio de instalación, renovación digital, mantenimiento y otras actuaciones de los terminales y dispositivos domiciliarios, móviles y detectores de gas y de humo.

La Política de seguridad de la información constituye el establecimiento de un marco organizativo y tecnológico en UNEI. Será de aplicación a toda la organización, así como a los organismos o terceras partes que utilicen los sistemas de información y/o dependientes de UNEI.

Debe ser conocida y cumplida por todo el personal de UNEI, independientemente del puesto, cargo y responsabilidad dentro del mismo, ya sea personal propio o subcontratado.

Toda persona cuya actividad pueda, directa o indirectamente, verse afectada por los requisitos del Sistema de Gestión Integral, está obligada al cumplimiento estricto de la Política de Seguridad.

Asimismo, es aplicable y de obligado cumplimiento para las personas que, aunque no presten servicio directamente en UNEI, tengan acceso a la información o a los sistemas que gestionen dicha información

Misión

La misión de UNEI es aportar a la sociedad soluciones empresariales innovadoras, sostenibles y eficientes, contribuyendo al desarrollo social y laboral de las personas con discapacidad, especialmente derivada de problemas de salud mental.

Para ello UNEI mantiene y garantiza unos adecuados niveles de seguridad y protección frente a amenazas para la información que gestiona, que es el activo fundamental para cumplir sus objetivos, y garantizar, así mismo, la protección y seguridad de los servicios que presta manejando dicha información.

Visión

La visión de UNEI es contribuir a transformar el mundo en un lugar emocionalmente saludable, más empático y humano.

Y los valores fundamentales de UNEI son la diversidad y la integración, la honestidad y la lealtad y la valentía y la decisión. En suma, UNEI es energía e ilusión, empleo e innovación, eficiencia e integración para integrar profesional y socialmente a un colectivo de talento competitivo, eficaz y extraordinario.

Organización de la Seguridad de la Información

La seguridad de los sistemas de información deberá comprometer a todos los miembros de UNEI.

La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 del ENS y según se detalla en la sección 3.1 del anexo II del ENS, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento.

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la seguridad de la información y de la protección de Datos de UNEI está compuesta por los siguientes agentes:

a) Comité de Dirección
b) El Comité de Gestión de la Seguridad de la Información.
c) El Responsable de Seguridad.
d) Responsables de la Información y de los Servicios.
e) Responsables del Sistema de Información.
f) Delegado de Protección de Datos.

Comité de Dirección

Es el responsable de aprobar la política de seguridad.

Comité de Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Gestión de la Seguridad de la Información, en adelante el Comité de Seguridad, dentro del ámbito de la presente Política de Seguridad. Estará formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en UNEI y que velará por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad.

Son funciones del Comité de Seguridad las siguientes:

a) Identificar los objetivos de UNEI en el ámbito de la Seguridad de la Información.

b) Elaborar la Política de Seguridad, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento.

c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en UNEI.

d) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnicos y de control, los sistemas y servicios de UNEI.

e) Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y es un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

f) Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a lo exigido en el ENS.

g) Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información.

h) Valorar el grado de conformidad de los procedimientos implantados en UNEI con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.

i) Supervisar las normativas y procedimientos de seguridad que se definan para dar cumplimiento y desarrollo a la Política de Seguridad.

j) Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

k) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.

l) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de UNEI en materia de Seguridad.

m) Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.

n) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de UNEI.

o) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en UNEI.

El Comité de Seguridad estará compuesto por los siguientes miembros:

- Presidente: CIO.
- Secretario: Delegado Protección de Datos (DPO).
- Vocales: Varía según puntos a tratar.

El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez al año, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

Responsable de Seguridad

Es el responsable de que los servicios y sistemas de información de UNEI se mantengan con el mayor grado de seguridad atendiendo a los principios de:

a) Confidencialidad: la información asociada a los servicios electrónicos solo debe poder ser conocida por las personas autorizadas para ello.
b) Integridad: la información asociada a los servicios electrónicos no debe ser alterada por personas no autorizadas.
c) Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios permanecerán disponibles.

Son funciones del Responsable de Seguridad:

a) Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
b) Asesorar en materia de seguridad a los integrantes de UNEI que así lo requieran.
c) Coordinar la interacción con otros organismos especializados en materia de seguridad de la información.
d) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
e) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
f) Asesorar, en colaboración con el Responsable del Sistema, los Responsables de los Servicios y de la Información en la realización de los análisis y gestión de riesgos, elevando el informe resultado al Comité de Seguridad.
g) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
h) Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
i) Aprobar la categorización de los sistemas.

Respecto a la documentación, son funciones del Responsable de Seguridad:

a) Aprobar y proponer al Comité de Seguridad la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
b) Supervisar la documentación de tercer nivel (Instrucciones técnicas) de obligado cumplimiento.
c) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Respecto a la protección de datos de carácter personal, son funciones del Responsable de Seguridad:

a) Garantizar la seguridad de los datos, implantando y haciendo cumplir las medidas, procedimientos, instrucciones y normativas establecidas en el Sistema de Gestión de UNEI.
b) Colaborar con el responsable del tratamiento en la difusión del Manual Política de Privacidad y de sus anexos.
c) Mantener un listado actualizado del personal autorizado a acceder a los sistemas de información
d) Realizar los controles periódicos establecidos para verificar el cumplimiento del Manual jurídico y de sus anexos.
e) Analizar los informes de auditoría y proponer al responsable del tratamiento las medidas correctoras oportunas.
f) Cumplir con el procedimiento de ejercicio de derechos de los interesados según las solicitudes recibidas.

g) Autorizar permisos de acceso a los usuarios sobre los recursos, (automatizados y no automatizados) que se encuentran bajo su responsabilidad y que sean estrictamente necesarios para el desarrollo de las funciones del trabajador.
h) Realizar un inventario y un registro de entrada y salida de soportes.
i) Autorizar la salida de soportes con datos personales que se encuentren bajo su responsabilidad.
j) Autorizar la generación de copias o reproducción de documentos.
k) Mantener un listado de personal autorizado a la información en soporte papel.
l) Revisar los permisos y perfiles de acceso de la información que se encuentra bajo su gestión.
m) Autorizar la recuperación de datos tratados.
n) Habilitar y mantener un registro de incidencias para la información que esté bajo su responsabilidad. Este registro deberá estar disponible para cualquier revisión o auditoría.

En aquellos sistemas de información que, por su complejidad, distribución, separación física de elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones del responsable de Seguridad, el responsable de Seguridad podrá designar cuantos Responsables de Seguridad Delegados considere necesarios, incluyendo los Responsables de Seguridad relativos a la RGPD. Los responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él.

El responsable de Seguridad será nombrado y cesado por el Comité de Seguridad.

Responsables de la Información y de los Servicios

Esta responsabilidad recaerá en el titular de la organización que lo podrá delegar en la dirección de los diferentes departamentos, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione.

Son los responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS.

Son los responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

Son los encargados, contando con la participación y asesoramiento del responsable de Seguridad y del Responsable del Sistema de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

Son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Los responsables de información y de los servicios son establecidos en el Plan Director de Seguridad, el cual contiene la planificación de actuaciones destinadas a subsanar las insuficiencias detectadas, para el cumplimiento del Esquema Nacional de Seguridad.

Responsable del Sistema de Información

Personal designado cuyas responsabilidades son:

a) Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
c) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
d) Elaborar procedimientos técnicos de seguridad de los sistemas de información.
e) Elaborar planes de continuidad de los sistemas de información.

Podrá acordar la suspensión del manejo de determinada información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser acordada con el Responsable de la Información y servicio afectados y el Responsable de Seguridad antes de ser ejecutada.

En aquellos sistemas que, por su complejidad, distribución, separación física de elementos o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Responsable de Sistemas, se podrán designar cuantos Responsables de Sistemas Delegado se consideren oportunos. La designación y delegación de funciones en los Responsables de Sistemas Delegados corresponde al Responsable del Sistema, sin perjuicio de que la responsabilidad final siga recayendo sobre el Responsable del Sistema. Los Responsable de Sistemas Delegados se harán cargo en su ámbito de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de Información correspondiente, así como también tendrá dependencia funcional directa con el Responsable del Sistema que es a quién reporta.

Los responsables del Sistema de Información son establecidos en el Plan Director de Seguridad, el cual contiene la planificación de actuaciones destinadas a subsanar las insuficiencias detectadas, para el cumplimiento del Esquema Nacional de Seguridad. Por regla general será el departamento de Informática, pudiendo delegar en los responsables de cada uno de los sistemas afectados.

Delegado de Protección de Datos

El Delegado de Protección de Datos será único para todos los órganos y organismos de UNEI se informará de su nombramiento y cese a la Agencia Española de Protección de Datos.

Son funciones del Delegado de Protección de Datos:

- Informar y asesorar a UNEI y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del Reglamento General de Protección de Datos en UNEI.

- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la Autoridad de control
- Actuar como punto de contacto de la Autoridad de Control

Además, asesorará y supervisará en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación Organización – encargado de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de UNEI y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditorías de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento
- Análisis de riesgo de los tratamientos realizados
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal de UNEI en materia de protección de datos.

Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de protección de datos y seguridad de la información corresponderá, en última instancia,

al Comité de Dirección, asistida por el Comité de Seguridad de la Información y, cuando proceda, por el Delegado de Protección de Datos.

Obligaciones del Personal

Todo el personal, interno y externo, de UNEI tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, el Código Ético e incluso el Manual de Gestión, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Legislación y normativa de referencia

El marco normativo de las actividades del Grupo UNEI en el ámbito de esta Política de Seguridad está integrado por las normas que se registran en el documento: "Normativa legal aplicable" en la que se incluye la legislación, normas y/o guías aplicables a la entidad.

El mantenimiento de la "Normativa Legal Aplicable" será responsabilidad del Responsable de CALIDAD, quien revisará y mantendrá actualizado dicho documento.

Documentos técnicos de desarrollo de la Política de Privacidad y Seguridad de la Información.

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: Instrucciones Técnicas de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de UNEI, recogido en el presente documento y aprobado por el Comité de Dirección.

Segundo Nivel: Normativas y Procedimientos de Seguridad

De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente.

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

Tercer Nivel: Instrucciones Técnicas 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.

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 delegados en su ámbito.

Principios y directrices

Se entenderá la Seguridad como un proceso integral constituido por todos los elementos técnicos, humanos y materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son la **prevención,** la **detección,** la **respuesta** y la **recuperación**, 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:

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 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.

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 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 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.

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).

Recuperación

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

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 autorizadas, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario (Mínimo privilegio).
- La Seguridad de la Información es **responsabilidad de todos**. Todas las personas que tiene acceso a la información de UNEI 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, así como 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.

Asesoramiento Especializado en Materia de Seguridad

Asesoramiento especializado

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en UNEI con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

Cooperación entre organismos y con Administraciones Públicas

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, UNEI mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad.

Revisión independiente de la Seguridad de la Información

El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en UNEI reflejan adecuadamente sus disposiciones.

Protección de Datos de Carácter Personal

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal de UNEI y a todas las actividades de acuerdo al principio de seguridad integral recogido en el art. 5 del ENS. A estos efectos, UNEI, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Análisis y gestión de riesgos

UNEI asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigente bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad (MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas).

Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, los Responsables de los Sistemas de Información realizarán, con periodicidad al menos anual, análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario.

Se realizará un análisis de riesgos:

- Regularmente, una vez al año.
- cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- cuando ocurra un incidente de seguridad grave.
- cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y éste al Comité de Seguridad.

Estas conclusiones, entre las que se incluirán los residuales y el riesgo objetivo, deberán ser aceptados y aprobados por el Comité de Seguridad.

Revisión y Auditorias

UNEI llevará a cabo de forma periódica, y al menos cada dos años, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos y sistemas de información.

En todo caso realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Las auditorías serán supervisadas por el Responsable de Seguridad de la Información y por el delegado de protección de datos.

Calificación de la información

Grupo UNEI establece un sistema de clasificación de seguridad de la información que genera y gestiona, en función de su ámbito de difusión previsto y de las consecuencias que pudiera tener para la entidad y para otras partes interesadas un eventual acceso no autorizado a la misma.

El sistema se estructura en los siguientes niveles de menor a mayor criticidad:

- Información Pública

  Toda aquella información que, individual o conjuntamente con información de terceros, está destinada a su divulgación pública, sin perjuicio de que antes de la divulgación le corresponda otro nivel de clasificación.

- Uso Interno

  Aquella información cuya vocación sea estar a disposición de toda la organización a través de los cauces habituales de comunicación disponibles, tales como sistemas de gestión documental o sistemas de compartición de ficheros y cualesquiera otros medios de difusión interna existentes. La información no es, en principio, accesible a terceras partes ajenas UNEI, salvo que necesiten acceder a ella para la realización de las funciones que tienen encomendadas. La difusión de esta información fuera del ámbito de UNEI no conlleva impacto relevante alguno.

- Información Confidencial

  Aquella información, propia o de terceros, destinada a ser utilizada en un ámbito concreto o proyecto de UNEI y cuya revelación no autorizada podría causar un impacto moderado en la actividad de la organización o en la de un tercero. La información que, de acuerdo a los criterios establecidos por el ENS, esté categorizada como de nivel Bajo, será incluida en esta categoría.

Los criterios y desarrollo de la calificación de la información serán desarrollados a través de procedimiento específico.

Tratamiento de la Información

Aprobación

La documentación que es susceptible de necesidad de aprobación contará con una sección dentro del documento definida a tal fin donde quede contenida la firma del aprobador.

La versión aprobada será almacenada en la estructura de carpetas y el Responsable del Sistema de Información velará por la seguridad de sus metadatos a fin de prevenir modificaciones no autorizadas.

Revisión de la documentación

La documentación que es susceptible de necesidad de aprobación tendrá definidos los plazos y métodos de revisión y actualización de documentos.

Las versiones siguientes a la documentación inicial identificarán los cambios y el estado de la versión vigente de los documentos.

Los documentos se mantendrán accesibles, identificables y legibles de acuerdo a su calificación para los miembros autorizados que así lo requieran.

Para la documentación de origen externo, como resultados de auditorías externas, se llevará a cabo el control de su distribución.

Prevenir el uso de documentos obsoletos y aplicarles una identificación adecuada en el caso de que se mantengan por razones de utilidad para la Organización.

La documentación informal de los sistemas cuando vaya a servir de evidencia documental del cumplimiento de los controles se restructurará de conformidad con lo descrito en la política de seguridad, de este modo la documentación contará con la aprobación del responsable del sistema y será sometida al mismo trato que el resto de documentación del ENS.

El Responsable de Seguridad, junto con los Responsables de la información y de los servicios velarán por el cumplimiento de la política de seguridad.

Categorías de seguridad.

La categoría de seguridad del sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I del ENS.

- Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

El responsable de cada información seguirá los criterios determinados anteriormente para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo con lo descrito anteriormente.

En base a los criterios anteriores y realizada la valoración de los activos de información del Grupo UNEI, la categorización de sus sistemas es de nivel MEDIO.

Publicación de la política de seguridad

El presente Documento se incluirá dentro del Sistema de Gestión de la calidad de UNEI.

Entrada en vigor

La Política de Seguridad que se aprueba en este documento será aplicable a partir del día siguiente al de su firma.

28931076C RAFAEL ANGEL CIA (R: A41431891)

Firmado digitalmente por 28931076C RAFAEL ANGEL CIA (R: A41431891)
Fecha: 2024.06.04 09:29:37 +02'00'

El Director General - Rafael Cía González