POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

ESQUEMA NACIONAL DE SEGURIDAD

USO PÚBLICO

PO ENS

Ed. 01

INDICE

22 de marzo de 2022

Elaborado por:
Mª Belén Dorado
Responsable del Sistema

Aprobado por:

Comité de Seguridad

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 22 de marzo de 2022 por Comité de Seguridad.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

PUE DATA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, establecidos según se describe en el documento PG 11 Objetivos e indicadores. Estos sistemas son administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados. Estas medidas se han incluido en el documento controles-declaración de aplicabilidad.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC de PUE DATA están protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se ha establecido una estrategia que se adapta a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos aplican las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, y realizan un seguimiento continuo de los niveles de prestación de servicios, siguen y analizan las vulnerabilidades reportadas, y preparan una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos de PUE DATA se aseguran de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, se identifican e incluyen en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos están preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS y al apartado gestión de incidentes del MN ENS Manual y procedimientos.

3. PREVENCIÓN

Los departamentos evitan, 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 los departamentos implementan las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados en el PG 08 Apreciación de riesgos de seguridad de la información.

Para garantizar el cumplimiento de la política, PUE DATA:

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

4. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los departamentos monitorizan la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios, reevaluando y actualizando periódicamente las medidas de seguridad para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad si fuese necesario.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se han establecido mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5. RESPUESTA

PUE DATA, en el apartado Gestión de incidentes del MN ENS Manual y procedimientos, ha establecido:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designado punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos a través de la dirección de correo electrónico cau@pue.es y el portal cau.pue.es para sus empleados.
- Ha establecido protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, PUE DATA ha desarrollado planes de continuidad de los sistemas TIC como parte de su plan de continuidad de negocio.

7. ALCANCE

Esta política se aplica a todos los sistemas TIC de PUE DATA, S.L., en adelante PUE DATA y a todos los miembros de la organización, sin excepciones.

Los principales servicios que presta la organización son:

Formación presencial, virtual y online. Servicios de consultoría y soporte en proyectos de Big Data.

8. MISIÓN

Ser capaces de ayudar a las empresas y a los profesionales, del presente y del futuro, en el constante reto de conocer y aplicar las tecnologías más novedosas de la mano de las multinacionales y organizaciones referentes en el mundo TIC.

PUE apuesta por el aval que supone la formación oficial y la acreditación de conocimientos como un valor seguro para que nuestros clientes puedan aplicar las soluciones de su interés de forma ágil y eficiente en el objetivo de mejorar su competitividad.

En ese sentido, nuestro lema es “La formación y certificación oficial como garantía de calidad”.

9. MARCO NORMATIVO

- 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)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- 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 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. (Esquema nacional de seguridad)
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. (Esquema nacional de seguridad).
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

10. ORGANIZACIÓN DE LA SEGURIDAD

El Comité de Seguridad de PUE DATA es responsable de la aprobación de cualquier estructura de seguridad que sustenta al sistema y que permite el cumplimiento de los requisitos de seguridad necesarios para manejar la información que soporta.

De forma específica tiene las funciones de:

- Aprobación de la política de seguridad de la información.
- Aprobación de los nombramientos de los responsables.
- Aprobar las necesidades presupuestarias en materia de seguridad.
- Resolver los conflictos que puedan aparecer entre los diferentes responsables.

11. ROLES: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad de PUE DATA ha establecido los siguientes roles y responsabilidades:

- Responsable de la información. El Comité de Dirección de PUE DATA tiene las funciones de responsable de la información, determinando los requisitos de seguridad de los servicios prestados. También asume las responsabilidades de responsable de tratamiento en los términos establecidos en la legislación relativa a protección de datos de carácter personal, y actúa a su vez como responsable último de los servicios prestados por la organización.

- Responsable de Seguridad de la Información. Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Es el responsable de la aprobación de la declaración de aplicabilidad de la organización.
- Responsable del Sistema. Se encarga de:
    - La operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
    - Realizar el análisis y gestión de riesgos en el Sistema.
    - Elaborar y aprobar la documentación de seguridad del Sistema.
- Responsable de protección de datos. Encargado de la gestión del cumplimiento de los requisitos legales establecidos en materia de protección de datos.
- Administrador de sistemas:
    - La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
    - La aplicación de los Procedimientos Operativos de Seguridad.
    - Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
    - Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

Las demás funciones y responsabilidades se encuentran descritas en el documento PG 09 R02 Competencia personas.

12. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por el D. General a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

13. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por D. General y difundida a través de la página web de la organización para que la conozcan todas las partes afectadas.

Esta política, incluye los siguientes compromisos en materia de seguridad de la información:

- La disponibilidad: El acceso a la información con la que trabajan nuestros consultores, formadores, y alumnos se realiza en tiempo real desde cualquier parte del mundo.

- La integridad: Protegemos el código que generamos contra cualquier tipo de alteración, y preservamos nuestros sistemas y material de formación para garantizar que se cumplen los criterios establecidos en las formaciones oficiales.
- La confidencialidad: Únicamente las personas autorizadas acceden al código que desarrollamos para nuestros clientes y a la información facilitada por nuestros alumnos.
- La trazabilidad: Desde la emisión de la oferta a la facturación de los servicios prestados.
- La autenticidad: Contamos con mecanismos de seguridad que permiten identificar el emisor y receptor del código generado por nuestros consultores, y al alumno en las pruebas y exámenes realizados.

Estos compromisos:

- Proporcionan el marco de referencia para establecer y actualizar los objetivos del sistema de gestión.
- Incluyen el cumplimiento de requisitos legales y otros requisitos.
- Tienen en cuenta los resultados de la apreciación y tratamiento de riesgos de seguridad de la información.
- Implican la mejora continua del sistema de gestión.

14. DATOS DE CARÁCTER PERSONAL

El responsable de protección de protección de datos, a través de la dirección de correo electrónico: protecciondedatos@pue.es, da respuesta a las solicitudes de información sobre los datos recogidos por la organización para distintos tratamientos que realiza la organización, desde los datos facilitados para la inscripción en una formación, hasta el tratamiento relacionado con las redes sociales de la organización.

15. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política realizan un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repite:

- regularmente, al menos una vez al año.
- cuando cambie la información manejada.
- cuando cambien los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad ha establecido una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados, y que se ha definido según se establece en el PG 08 Apreciación de riesgos de seguridad de la información.

16. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Además de este documento, la política de seguridad de la información se complementa con las políticas y procedimientos establecidos en los documentos:

- MN ENS Manual y procedimientos.
- Seguridad en la gestión de proyectos.
- PDEVS01 – Procedimiento de codificación de software seguro.

Y en todos los documentos que componen el sistema de gestión de seguridad de la información y que se recogen en el Listado de documentación en vigor de la organización.

17. OBLIGACIONES DEL PERSONAL

Todos los miembros de PUE DATA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados en el momento de su incorporación a través del documento Manual de buenas prácticas.

El responsable del sistema, planifica las formaciones y acciones de concienciación en materia de seguridad TIC al menos una vez al año.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC reciben formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación es 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.

18. TERCERAS PARTES

Cuando PUE DATA preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando PUE DATA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

19. DOCUMENTACIÓN RELACIONADA

- Guía de seguridad CCN-STIC-805. Esquema nacional de seguridad. Política de seguridad de la información.
- CCN-STIC 402. Organización y gestión STIC.

- Apartado 5.2 de la norma UNE-EN ISO/IEC 27001:2017. Sistemas de gestión de seguridad de la información. Requisitos.

20. CONTROL DE EDICIONES

EDICION	MOTIVO DEL CAMBIO	FECHA
1	Primera elaboración del procedimiento.	22/03/2022