DocumentForm editar

Titulo	Política de seguridad de la información
AreaDocumental	Compliance (NOR)
TipoDocumental	Política General (PG)
Codigo	NOR-PG-Seguridad_de_la_informacion
EmpresaCertificada	European Agency of Digital Trust
NormasCertificadas	ISO27001
ResponsableDocumental	Dirección General
ClasificacionDeSeguridad	Publico (P)
RevisionPeriodica	Revision Trienal

Información de compliance

Seguridad de la Información

Como proveedor de servicios de confianza, cualquier brecha en la seguridad de la información (incluida la pérdida o el robo) puede provocar la inmediata pérdida de confianza de todos los stakeholders del mercado y, por tanto, la inviabilidad de nuestra agencia. Es decir, la seguridad de la información es la máxima prioridad de EAD Trust.

La política de seguridad de la información acompaña a la Política de Calidad y a la de Gestión de Servicios, además de estar supeditada a la Política de Gestión del Cambio.

Alcance

Esta política es de aplicación a todo el personal, que tendrá que garantizar que todos los procedimientos, servicios y activos de la empresa con capacidad para almacenar o procesar datos cumplen estas políticas.

Debido a la importancia de la seguridad de la información en la operativa de la empresa y a la dificultad de asimilar distintos documentos de políticas, en el 2020 se decidió unificar la mayoría de las políticas temáticas bajo este documento. Las políticas de Recursos Humanos, Protección de datos personales, uso de controles criptográficos, accesos y seguridad física, se mantienen separadas debido a su complejidad e importancia en operativas críticas (ISO27002 5.1.1).

Política General de Seguridad de la Información

Esta política proporciona referencia, orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativa pertinentes y, en particular, con relación al Esquema Nacional de Seguridad establecido por el Real Decreto 311/2022, de 3 de mayo, así como normas de estándares ISO que crean un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización (ISO27002 5.1) (ISO27002 6.1).

En este sentido, la empresa se compromete a mantener actualizado a todo su personal en materia de Seguridad y velar por el cumplimiento de los requisitos establecidos en la legislación vigente en materia de Seguridad de la Información. Asimismo, se invertirá en la mejora continua del sistema siguiendo las mejores prácticas vigentes (ISO27001 5.2).

En caso de que se realizara algún cambio en la política de seguridad de la información, EAD Trust se comunicará a los clientes, partes de confianza, organismos de evaluación, supervisión u otros organismos reguladores, la información requerida. Para ello se seguirá lo establecido en la CAL-GUIA-Comunicacion.

Definición y documentación de Seguridad de la Información

EAD Trust define la **seguridad de la información** como *el conjunto de sistemas tecnológicos y de medidas preventivas y reactivas que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos*.

El sistema de gestión documental adoptado para la aprobación de otras políticas y procedimientos que describen las tareas cuya ejecución se requieren para la adopación de las referidas medidas, se establece en la guía para la gestión de la documentación EADTRUST Guía sobre la codificación de la documentación.

Principios

Principio de confianza

Los pilares de la confianza son la hipótesis de una conducta futura y su cumplimiento. Por lo tanto, EAD Trust, su personal y cada uno de los servicios, sistemas, activos y procedimientos actuará de manera que la expectativa del servicio prestado y el resultado sean lo mismo o al menos lo más parecidos posible.

Este principio debe estar presente, con mayor atención, en la documentación del sistema integrado de gestión de la información y en las contrataciones con clientes y proveedores.

Principio de clasificación

Toda la información utilizada en la empresa podrá tener asignada una clasificación de seguridad. En caso de que no tenga una clasificación explícitamente designada, deberá considerarse que la clasificación es UsoInterno. La información se protegerá de acuerdo a los riesgos asociados a su clasificación de seguridad.

Principio de separación de roles

Existe separación de roles cuando es necesaria e insoslayable la presencia de dos o más personas para llevar a cabo una operativa acogida a este principio.

Todos los **servicios críticos** se servirán del principio de separación de roles (también llamado *de 4 ojos*) para maximizar la seguridad de las actividades gestión de servicios de confianza.

Principio de mínimo acceso

Sólamente se otorgarán los mínimos permisos de seguridad necesarios para cumplir las responsabilidades de cada rol y poder realizar las tareas encomendadas. Los privilegios se mantendrán durante el menor tiempo posible una vez no sean necesarios.

Principio de cumplimiento

EAD Trust y su personal velarán por el cumplimiento de los reglamentos y leyes vigentes, integrando estos requisitos con las políticas, procedimientos y sistemas correspodientes, y practicándolos en su trabajo.

Principio de necesidad de conocer

Los usuarios recibirán acceso a aquellos sistemas necesarios para poder llevar a cabo sus funciones y responsabilidades.

Responsabilidades

La responsabilidad directa de la definición, puesta en marcha, seguimiento y actualización del SGSI recaerá en el Responsable de Seguridad de la Información, excepción hecha de los aspectos relacionados con el cumplimiento de la CAL-PE-Politica_ de_ Privacidad_ y_ Protección_ de_ Datos_ Personales de EADTrust, el Reglamento General de Protección de Datos (conocido, abreviadamente, como REGLAMENTO (UE) 2016/679 RGPD) y la Ley 3/2018, de 5 de diciembre de 2018 de proteccion de datos personales y garantía de derechos digitales (conocida, abreviadamente como LOPDGDD), que serán responsabilidad del Responsable de LOPD.

El Responsable de Seguridad de la Información, se verá apoyado por un Comité de Seguridad de la Información, constituido por el Responsable de la Información, el Responsable del Sistema, el Responsable de los Servicios, el Responsable de Verificación de Cumplimiento y el Responsable de Compliance de EAD Trust, adoptándose al respecto de sus funciones los criterios de Guías del CCN (Guía de Segurdad CCN-STIC-801).

Objetivos

Información e información de autenticación

La **información** deberá:

- Clasificarse de acuerdo a los niveles de secreto (ISO27002 8.1)
- Protegerse en función de su clasificación de seguridad (ISO27002 8.1)
- Ser protegida en las redes y recursos de tratamiento de la información (ISO27002 13.2)
- Evitarse su pérdida mediante copias de seguridad (ISO27002 12.3)
- Gestionarse con especial cuidado cuando se encuentre en soportes extraibles (ISO27002 8.3.1).
- Destruirse antes de su enajenación (ETSI-EN-319-401 REQ-7.4-10)

En particular, la **información de autenticación** tendrá la clasificación de "Reservado" y deberá:

- ser controlada a través de un proceso formal de gestión (ISO27002 9.2.4) y
- ser alvaguardada por cada usuario, como responsable de la misma (ISO27002 9.3)
- siguiendo las prácticas de la organización (ISO27002 9.3.1) y
- usando un sistema de gestión de contraseñas interactivo (ISO27002 9.4.3).

Seguridad de la Información

La **seguridad de información** deberá:

- Ser tratada dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto (ISO27002 6.1.5).
- Mantenida durante las transferencias con entidades externas (ISO27002 13.2).
- Garantizada en el ciclo de vida del desarrollo de software de acuerdo a las restricciones propias de la clasificación de la seguridad procesada (ISO27002 14.2).
- Asegurarse con proveedores externos medante SLA (ISO27002 15.2)
- Revisarse para garantizar que se implementa y opera de acuerdo a las políticas y procedimientos de la organización (ISO27002 18.2, ETSI-EN-319-401 REQ-6.3-07).
- Formar parte de continuidad de negocio (ISO27002 17.1)

Activos, personal, personal de confianza y eventos de seguridad

Para ello, los **activos** deberán ser:

- Identificados y sus responsabilidades de protección deberán ser adecuadamente definidas (ISO27002 8.2)
- Verificados respecto a la integridad del software en explotación (ISO27002 12.1)
- Custodiados contra la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización (ISO27002 11.2) asegurando la disponibilidad de los activos críticos

(ISO27002 17.2).
- Protegidos contra el malware (ISO27002 12.2)
- Resguardados contra modificaciones de software no autorizadas (ISO27002 12.5)
- Defendidos contra la explotación de vulnerabilidades técnicas (ISO27002 12.6, ETSI-EN-319-401 REQ-7.7-09, ETSI-EN-319-401 REQ-6.3-10 L))
- Borrados antes de destinarlos a otro uso (ETSI-EN-319-401 REQ-7.4-10)

Todo el **personal** deberá: CAL-PE-Politica_de_tratamiento_de_informacion_de_caracter_restringido

- Comportarse lealmente, contribuyendo a los objetivos definidos en las pollíticas de la empresa.
- Oponiéndose y negando su apoyo a cualquier filtración o brecha de seguridad, incluyendo cualquier información clasificada como de UsoInterno o más secreta.

En particular el **personal de confianza** será:

- Designado por un proceso documentado
- Autorizado explicitamente a acceder a zonas seguras y de alta seguridad
- Asignado a seguir incidentes de seguridad (ETSI-EN-319-401 REQ-7.9-06)
- Vigilante de los principios de *menor privilegio* y *separación de roles* (ETSI-EN-319-401 REQ-7.4-10)

Y los **eventos y vulnerabilidades de seguridad** deberán ser:

- Registrados (ISO27002 12.4, ETSI-EN-319-401 REQ-7.9-03)
- Procesados y gestionados de manera coherente y eficaz (ISO27002 16.1), siendo analizados en menos de 48h (ETSI-EN-319-401 REQ-7.9-10)
- Escalados mediante alarmas (ETSI-EN-319-401 REQ-7.9-03).
- Comunicados de acuerdo a los requisitos vigentes (ISO27002 16.1)

Política de datos

Recogida de datos

Compliance: ETSI-EN-319-411-1 REG-6.2.2-23

EAD Trust siempre recogerá la menor cantidad de datos y evidencias necesarias para llevar a cabo sus servicios, manteniendo la privacidad de los datos que marquen las leyes vigentes ETSI-EN-319-411-1 REG-6.4.5-05.

Datos de prueba

Compliance: ISO27002 14.3

El uso de datos reales para pruebas esta sujeto a las restricciones de seguridad de la fuente original de los datos. En general, se desaconseja el uso de datos personales reales para pruebas en cualquier entorno.

No está autorizado el uso de datos reales personales, financieros o médicos en entornos de test o desarrollo y se requiere aprobación expresa de la dirección para utilizarlos en entornos de preproducción durante las pruebas finales a un despliegue.

Cuando se utilicen datos reales para pruebas siempre se utilizarán copias de los mismos. El tiempo de vida de estas copias será efímero y el proceso deberá garantizar su destrucción una vez terminadas las pruebas.

Política de dispositivos móviles y *bring your own device*

Compliance: ISO27002 6.2.1, CAL-PE-Politica_de_informatica_y_comunicaciones_moviles

No se permite el uso de dispositivos móviles personales para actividades de trabajo o teletrabajo ni el almacenamiento de datos corporativos con nivel de clasificación superior a Público en cualquier dispositivo personal, ya sea total o parcialmente.

Excepcionalmente y bajo autorización, podrá permitirse el acceso a herramientas de comunicación como el correo electrónico desde estos dispositivos.

Política de escritorio despejado y pantalla limpia

Compliance: ISO27002 11.2.9, ETSI-EN-319-401 REQ-7.4-10

La información con clasificación de seguridad DifusionLimitada o más secreta deberá estar guardada cuando no se necesite, independientemente de su soporte (en papel o cualquier almacenamiento electrónico). Además, cuando se imprima este tipo de información, se deberá retirar este tipo de información de la impresora inmediatamente.

Los ordenadores y terminales deben quedarse apagados o protegidos mediante un mecanismo de bloqueo de pantalla y teclado controlado mediante una contraseña, dispositivo hardware o mecanismo similar de autenticación de usuario cuando estén desatendidos y deben estar protegidos mediante claves de bloqueo, contraseñas u otros controles cuando no están en uso;

Política de uso de sistemas

Integrar: CAL-PE-Politica_de_buen_uso_de_los_sistemas_corporativos_de_gestion_de_informacion

Información de compliance

Los requisitos ISO20000-1 7.5.4, ISO27001 5.2, ETSI-EN-319-401 REQ-6.3-03 y ETSI-EN-319-421 REQ 7.2 establecen la necesidad de documentar una política de Seguridad de la Información.

El documento esta clasificado para su revisión cada tres años ISO27002 5.1.2.

Los cambios deben aprobarse por el Consejo de Administración. ISO20000-1 8.7.3.1