POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Referencia: [ORG.1] Política de seguridad

Autor: Comité Seguridad

Versión: 06

Clasificación: Pública

Contenido

APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 05 de agosto de 2024 por AREA PROJECT.

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

1. INTRODUCCIÓN

AREA PROJECT depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser 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.

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 deben estar 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 requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar

las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse 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 deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 1 del ENS.

1.1. PREVENCIÓN

Los departamentos deben 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 los departamentos deben implementar 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.

1.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben 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 8 del ENS. Se establecerán 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.

1.3. RESPUESTA

Los departamentos 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).

1.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

2. ALCANCE

Al igual que queda expuesto en el SGSI de la ISO 27001, el alcance del sistema para ENS es: "Los sistemas de información que soportan los procesos de Comercialización, consultoría, instalación y mantenimiento de hardware; sistemas cloud, sistemas informáticos e infraestructuras de telecomunicaciones”

3. MISIÓN

La misión de AREA PROJECT es la de cumplir con las necesidades y expectativas de las partes interesadas involucradas dentro del alcance del sistema protegiendo la información interna y relacionada con la prestación de los servicios digitales al ciudadano y que se materializan en las siguientes prestaciones:

- Comercialización
- Consultoría
- Instalación y mantenimiento de hardware
- Sistemas Cloud
- Sistemas informáticos e infraestructuras de telecomunicaciones

Estas cuestiones se materializan con las aportaciones de personas formadas, certificadas y en permanente actualización de conocimientos, así como en métodos y prácticas.

4. Marco Normativo

La presente política se rige por la siguiente legislación y normativa de referencia:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. (ITS) de Conformidad con el ENS y la de Auditoría del ENS.
- Artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Guías CCN-STIC (800).
    - **CCN-STIC 801** (Guía de seguridad ENS)
    - **CCN-STIC 817** (Criterios de auditoría ENS)
    - **CCN-STIC 820** (Medidas de seguridad en el ENS)
- ISO 27001:2022.
    - **ISO/IEC 27002:2022** (Controles de seguridad)

- **ISO/IEC 27005:2022** (Gestión de riesgos de seguridad de la información)
- **ISO/IEC 27701** (Extensión de privacidad para ISO 27001, alineada con GDPR)

5. ORGANIZACIÓN DE LA SEGURIDAD

5.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

Los Comités, que se constituirán como órganos colegiados, de conformidad con lo señalado en la Ley 40/2015, estarán formados por los miembros de todas las partes implicadas.

En este sentido y con las funciones atribuidas en materia de Seguridad de la Información y seguridad física se crea el Comité de Seguridad de AREA PROJECT.

El Comité de Seguridad estará formado por:

- Responsable de la Información
- Responsable de los Servicios
- Responsable del Sistema de gestión de la seguridad de la información (SGSI)
- Responsable de Seguridad
- Responsable del Sistema

Las funciones del Comité de Seguridad son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Empresa y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.

- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la empresa y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.

- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con el Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de la ISO 27001 de protección de datos que permitan verificar el cumplimiento de las obligaciones de la empresa en materia de seguridad de la Información.

Asimismo, podrán ser delegadas otras funciones por otro órgano de la entidad con competencias en la materia. Las funciones atribuidas al Comité por otro órgano no podrán ser delegadas si bien podrán ser revocadas en cualquier momento.

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

5.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Se establecen en el archivo llamado; **[ART.11] Aprobación integrantes del Comité de Seguridad Area Project,** los roles, funciones y designaciones al respecto del comité de seguridad, de manera más extensa y exhaustiva.

5.3. PROCEDIMIENTOS DE DESIGNACIÓN

La designación de los integrantes del Comité de Seguridad de la Información y de los responsables identificados en esta política se realiza por la Dirección de AREA PROJECT, considerando criterios de aptitud, cualificación y experiencia en materia de seguridad de la información y gestión de riesgos.

Criterios de designación:

- La Dirección seleccionará a los miembros del comité en base a los siguientes criterios:
- Experiencia y formación en seguridad de la información, tecnologías de la información o normativa aplicable.
- Conocimiento de los procesos críticos de la organización y su impacto en la seguridad.
- Capacidad de liderazgo y toma de decisiones en materia de seguridad.
- Competencias en gestión de riesgos, cumplimiento normativo y respuesta a incidentes.

Proceso de nombramiento:

1. La Dirección evalúa a los candidatos y realiza la designación de los miembros del Comité de Seguridad de la Información.
2. La designación de los responsables se formaliza mediante acta oficial del Comité de Seguridad y se comunica a las partes afectadas.
3. La notificación de los nombramientos se realiza a través de la plataforma de AREA PROJECT, quedando registrada en la misma como evidencia de designación.

4. Los miembros del comité y los roles de seguridad serán revisados cada cuatro años, salvo en caso de vacante, cambios organizativos o necesidades específicas de la seguridad de la información.

5.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la **revisión anual** de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por el propio comité de seguridad y difundida para que la conozcan todas las partes afectadas.

6. DATOS DE CARÁCTER PERSONAL

Los sistemas de información de AREA PROJECT solo recogerán datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del 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) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto,

el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

La empresa Conversia (PROFESSIONAL GROUP CONVERSIA, S.L.U.) se encarga de la gestión de la protección de datos de Area Project y designa al Delegado de Protección de Datos de AREA PROJECT. Persona de contacto de Conversia: Vicente Ruiz (vicente.ruiz@conversia.es).

7. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá: 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 TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- El Comité de Seguridad ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad y la normativa ISO 27001:2022. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

- Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por la dirección de AREA PROJECT.

- Cuando AREA PROJECT preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información.

- Dirección a propuesta del Comité de Seguridad aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que AREA PROJECT lleve en materia de Seguridad en relación con otros organismos.

- Cuando AREA PROJECT utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad

existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad. De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en el Real Decreto Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica modificado por el Real Decreto 951/2015 de 23 de octubre, y en consideración a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad de categorías MEDIA o ALTA.

- Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS 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.

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de AREA PROJECT, incluidos en el alcance, 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de AREA PROJECT atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de AREA PROJECT, en particular a los de nueva incorporación.

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

Además, en **FOP - FUNCIONES Y OBLIGACIONES PARA TODO EL PERSONAL**, se definen las funciones y obligaciones del personal.

10. TERCERAS PARTES

Cuando AREA PROJECT 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 la AREA PROJECT 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.

11. POLÍTICAS ESPECÍFICAS

En nuestra organización, hemos desarrollado y mantenemos una serie de políticas específicas para asegurar la protección y gestión efectiva de la información. Estas políticas incluyen, pero no se limitan a:

- Seguridad de la información
- Seguridad del personal
- Gestión de activos de información
- Control de accesos
- Gestión de incidentes de seguridad
- Evaluación de proveedores

- Adquisición, mantenimiento y explotación

Estas políticas son revisadas y actualizadas periódicamente (anualmente) para garantizar su adecuación y eficacia en el contexto de los riesgos y desafíos emergentes en el ámbito de la seguridad de la información.

Los usuarios pueden consultar estas políticas específicas solicitándolas directamente al departamento de seguridad de la información. Para más información los usuarios pueden ponerse en contacto con info@areaproject.com