Junta de Andalucía

POLÍTICA DE SEGURIDAD ENS

(Extracto de la revisión 2. de fecha 18/07/2023)

INTRODUCCIÓN

Este documento constituye un extracto de la Política de Seguridad de la Información de Verificaciones Industriales de Andalucía, S.A., en adelante VEIASA, en cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

La Política de Seguridad de la Información recoge la postura de VEIASA en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad de la organización en cuanto a la seguridad.

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 de información deben estar protegidos contra amenazas con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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.

La presente Política de Seguridad determina:

- El marco de gestión y organización de la seguridad, definiendo los roles participantes, junto con sus funciones y responsabilidades.
- Los requisitos de seguridad de obligado cumplimiento para el personal interno y externo a VEIASA, en relación al manejo de los activos propiedad de, o custodiados por, VEIASA.
- Los controles de seguridad que será preciso implantar para satisfacer los requisitos de seguridad necesarios para la seguridad de las operaciones.
- Las pautas para el establecimiento de un Sistema de Gestión de la Seguridad de la Información para los procesos de VEIASA.
- Las bases para el aseguramiento del cumplimiento normativo legal vigente, en materia de protección de datos y Seguridad de la Información.

POLÍTICA GENERAL DE SEGURIDAD

El objetivo de la política general de seguridad de VEIASA es el de contrarrestar las amenazas mencionadas anteriormente con los medios suficientes y proporcionados. Para este fin, se establecerá una estructura de seguridad, junto con los mecanismos apropiados para su gestión, y un conjunto de instrumentos de apoyo de forma que se garantice:

- El cumplimiento de los objetivos de su misión y de prestación de servicios.
- El cumplimiento de la legislación y normativa aplicables.

Para ello:

- La previsión y despliegue de medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo la información.
- La aplicación de medidas de respuesta ante incidentes de seguridad, física o lógica, de forma que se minimice el impacto de los mismos, en caso de que ocurrieran.

Como norma general, se tendrá un enfoque de orientación al riesgo a la hora de diseñar las medidas de seguridad necesarias, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo.

Las distintas áreas bajo cuya responsabilidad se encuentran los servicios prestados deben contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad prescritas por el Esquema Nacional de Seguridad

Los requisitos de seguridad de los sistemas, las necesidades de formación de los usuarios, administradores y operadores y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las TIC.

Se deben articular mecanismos de prevención, detección, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.
Los datos personales estarán protegidos de acuerdo a lo establecido en la legislación vigente. A estos datos, en lo que respecta a su protección, se les aplicarán las medidas establecidas para la información en general, en función de su criticidad, que será la correspondiente a las características del dato, ya sea normal o de especial sensibilidad.

ALCANCE

Esta Política de Seguridad es de aplicación a toda la información y servicios de VEIASA. La en todas las fases de su ciclo de vida. .

Todo el personal de VEIASA, entidades u organizaciones externas que accedan, usen, gestionen, operen, desarrollen o mantengan activos o información o propiedad custodiada por VEIASA, están sujetos al obligado cumplimiento con las directrices y normas de esta Política de Seguridad.

ESTRUCTURA DE GESTIÓN Y ORGANIZACIÓN DE LA SEGURIDAD

La seguridad en VEIASA está soportada sobre las estructuras y roles que se describen a continuación:

- **Estructura de especificación**, que es la que se encarga de establecer los requisitos de seguridad asociados a la información y a los servicios prestados. Forman parte de esta estructura el Responsable de la Información y los Responsables de los Servicios, los cuales establecen el nivel de seguridad de la información y de los servicios respectivamente, en base a sus requisitos de confidencialidad, integridad y trazabilidad en el caso de la información, y de disponibilidad y autenticidad en el caso de los servicios.

- **Estructura de supervisión**, que es la que se encarga de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continúo con los objetivos de la organización. Forma parte de esta estructura el Responsable de Seguridad y el Delegado de Protección de Datos.

- **Estructura de operación**, que se encarga de implantar las medidas de seguridad identificada, siendo el Responsable del sistema el rol que desempeña esta función.

VEIASA cuenta con un **Comité de Seguridad Corporativa**, cuya función es la de coordinar las actividades de seguridad integral y velar por el cumplimiento de las directrices marcadas en materia de Seguridad Corporativa de la información.

REQUISITOS DE SEGURIDAD DE OBLIGADO CUMPLIMIENTO

Para la correcta implementación y cumplimiento de la presente Política de Seguridad es necesario aplicar los siguientes requisitos de seguridad de obligado cumplimiento:

➢ LA SEGURIDAD EN LA ORGANIZACIÓN

La seguridad debe comprometer a todos los miembros de la Organización, sin excepción.

➢ ANÁLISIS Y GESTIÓN DE RIESGOS

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos que facilite la selección y priorización de las medidas de protección necesarias para el control del riesgo en los niveles aceptados por la organización..

El análisis se realizará:

- 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 habían sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.
- cuando se vaya a iniciar o a modificar un tratamiento de datos de carácter personal, en línea a lo establecido en el Reglamento General de Protección de Datos

De acuerdo con la escala de riesgos de la metodología Magerit, el nivel de riesgo deberá situarse por debajo de nivel ALTO para considerarse de forma automática como aceptable (el riesgo residual máximo debe ser MEDIO). Valores de riesgo residual mayores a MEDIO deberán ser aceptados explícitamente por el Comité de Seguridad Corporativa, previa justificación de la conveniencia de su aceptación.

Para los valores de riesgo residual que no sean aceptables se deberá elaborar el correspondiente Plan de Tratamiento que permita llevar los valores de riesgo a valores aceptables.

A raíz de los resultados obtenidos en los mencionados análisis de riesgos se determinarán las medidas necesarias para proteger dichos datos.

VEIASA considera la concienciación en seguridad de la información como una herramienta necesaria y conveniente para capacitar al personal en el uso seguro de los equipos y sistemas y la identificación y detección de incidentes, actividades o comportamientos sospechosos. Es por ello que VEIASA realiza acciones de concienciación de forma periódica para alcanzar estos objetivos.
De la misma forma, y para garantizar la correcta capacitación del personal que administra y revisa la seguridad de los sistemas, VEIASA impulsa la formación continua de su personal técnico.

➢ DATOS DE CARÁCTER PERSONAL

VEIASA solo recoge 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, deben adoptarse las medidas de índole técnica y organizativa necesarias para el cumplimiento de la normativa vigente en materia de Protección de Datos.

Los tratamientos de datos realizados por VEIASA como Responsable del Tratamiento, así como los realizados como Encargado del Tratamiento se encuentran recogidos en el Registro de Actividades de Tratamiento.

➢ CONTROL DE ACCESO

El acceso a los sistemas de información estará restringido y limitado a aquellos usuarios o procesos que lo necesiten para el desarrollo de su actividad y estén previamente autorizados.

El acceso a la información seguirá el principio de "necesidad de conocer", de forma que los privilegios otorgados a cada entidad sean los mínimos imprescindibles para el desarrollo de su actividad.

La identificación de los usuarios será tal que se pueda conocer en todo momento quién recibe derechos de accesos y quién ha realizado alguna actividad, por lo que los identificadores deberán ser personales, no compartidos, e intransferibles.

➢ SEGURIDAD POR DEFECTO

Los sistemas y aplicaciones se diseñan y desarrollan bajo el principio de seguridad por defecto, de tal forma que:

- El sistema debe ofrecer la funcionalidad mínima necesaria, y ninguna adicional. Cualquier función que no sea de interés o innecesaria será deshabilitada o no implementada.
- La operación y explotación de los sistemas debe estar limitada a aquellas personas o ubicaciones que se autoricen, quedando prohibidas para el resto.
- El uso del sistema ha de ser seguro, de tal forma que el uso inseguro requiera intención por parte del usuario.

➢ SEGURIDAD POR DISEÑO

La seguridad estará presente desde la concepción de un sistema o aplicación y permanecerá presente durante todo su ciclo de vida.

En la concepción de un nuevo sistema o aplicación, o modificación sustancial de un sistema o aplicación existentes, se contará siempre, y desde el inicio, con la participación del Responsable de Seguridad de la Información.

- **PROTECCIÓN DEL PERÍMETRO**

VEIASA despliega las protecciones necesarias para proteger el perímetro de la red corporativa de VEIASA, de forma que se neutralicen las posibles intrusiones procedentes del exterior, ya sean iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros.

- **REGISTRO DE ACTIVIDAD**

Los sistemas y aplicaciones generarán los registros de actividad necesarios para conocer la actividad en los sistemas, de forma que se pueda determinar en todo momento qué persona actúa, sobre qué datos, con qué operaciones y sus privilegios de acceso.

- **GESTIÓN DE INCIDENTES DE SEGURIDAD**

VEIASA gestiona los incidentes de seguridad mediante procedimientos que aseguran la correcta gestión y respuesta efectiva que permita anular o minimizar el impacto del incidente en la información, los servicios, los clientes y, en general, en la actividad de VEIASA. Estos procedimientos contemplan la comunicación y notificación de los incidentes a los organismos receptores de dicha información, de acuerdo con la legalidad vigente.

- **GESTIÓN DE LA SEGURIDAD Y MEJORA CONTINUA**

VEIASA establece un Sistema de Gestión de la Seguridad que permita conocer en cada momento el estado de la seguridad, mediante la definición y medida de indicadores, y permita tomas las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos.

Se establecerá un proceso de mejora continua mediante el análisis de la situación, la implantación de nuevas medidas de seguridad, la mejora de las existentes y la aportación de mejoras sugeridas por el Comité de Seguridad Corporativa y por toda la Organización en su conjunto.

- **CUMPLIMIENTO**

Se deberá cumplir lo establecido en el Esquema Nacional de Seguridad para la protección de la información y los servicios, y para la protección de la información de carácter personal y la satisfacción de los derechos de los afectados se aplicará la legislación en materia de protección de datos vigente.

Para la determinación de los controles de seguridad aplicables a los sistemas, la información, los locales y el personal, se tomará como base de obligado cumplimiento el catálogo de controles de seguridad incluidos en el Anexo II del ENS.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad se desarrolla en cuatro niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento de desarrollo se fundamente en el nivel superior.

Todo el cuerpo normativo de seguridad, así como esta Política de Seguridad se encontrará a disposición de todo el personal de la organización que necesite conocerla y, en particular, el personal que utilice, opere o administre los sistemas de información y comunicaciones o la información misma albergada en dichos sistemas o los servicios prestados por VEIASA.

COMPROMISO DE LA DIRECCIÓN

La Dirección de VEIASA manifiesta su compromiso formal con el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política.

Dicho apoyo se concretará en:

- proporcionar los recursos necesarios, dentro de las posibilidades presupuestarias;
- asignar roles y responsabilidades a las personas asociadas a los planes de seguridad;
- destinar presupuesto, dentro de las posibilidades;

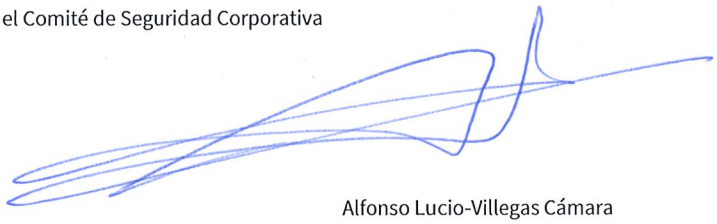
- apoyar la formación de los recursos humanos implicados en los planes de seguridad para que adquieran el nivel de concienciación y las competencias necesarias;
- garantizar el mantenimiento de la documentación asociada a los planes de seguridad;
- facilitar las comunicaciones con otras organizaciones en materia de seguridad de la información;
- promover la mejora continua.

El compromiso con el apoyo a los planes se manifiesta con la aprobación del presente documento.

REVISIÓN Y APROBACIÓN

La presente Política de Seguridad, como cualquier documento del SGI en vigor, se encuentra aprobada según lo establecido en el procedimiento correspondiente a Control de la Documentación.

Esta Política de Seguridad será revisada al menos anualmente por el Comité de Seguridad Corporativa



Alfonso Lucio-Villegas Cámara

Director General de Verificaciones Industriales de Andalucía, S. A.