POLÍTICA DE SEGURIDAD ENS

(Revisión 1, 17/03/2022)

1. INTRODUCCIÓN

Este documento constituye la Política de Seguridad de la Información de Verificaciones Industriales de Andalucía, S.A., en adelante VEIASA, en cumplimiento del artículo 11 (Requisitos mínimos de Seguridad) 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 y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

En este sentido, el mencionado artículo 11 establece que "*Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.*"

La estructura de este documento sigue las pautas establecidas por la guía CCN-STIC-805 para la redacción de la Política de Seguridad en el ámbito del 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.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la normativa vigente aplicable en materia de protección de datos personales, 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.

Se entiende por disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad lo siguiente:

- **Disponibilidad**: La disponibilidad es la característica, cualidad o condición de un servicio de encontrarse a disposición de quienes necesitan acceder a él, ya sean personas, procesos o aplicaciones.

- **Integridad:** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

- **Confidencialidad:** es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado por VEIASA a acceder a dicha información.

- **Autenticidad:** es la característica que se asocia a un servicio cuando quien lo utiliza es quien dice ser,

y no alguien que lo suplante.

- **Trazabilidad:** es la característica que se asocia a un servicio cuando se puede conocer quién lo utilizó, cuándo, para qué y de qué forma.

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.

2. MARCO NORMATIVO

La normativa a la que se encuentra sometida VEIASA, relacionada con la Política de Seguridad que se recoge en el presente documento sería la siguiente, además de toda la normativa de desarrollo que se publique al respecto:

- Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.
- 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
- 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.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- 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.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- 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.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se

aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

- Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

- Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

3. POLÍTICA GENERAL DE SEGURIDAD

Uno de los objetivos (o "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:

- se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo la información.
- se diseñarán 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 deberán 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 para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de los servicios y de la información.

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:

- En cuanto a la prevención, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello, VEIASA implementará las medidas de seguridad establecidas en el Anexo II del ENS, así como medidas adicionales que pudieran ser identificadas en el proceso de análisis de riesgos.

- Se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por los usuarios, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.

- En cuanto a la recuperación, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

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. Se utilizará el análisis de riesgos para determinar la fortaleza de las medidas de protección a aplicar.

Se elaborará una Política de Privacidad donde se refleje la postura de la Organización con respecto al tratamiento de datos personales.

Por otra parte, cualquier norma interna que trate algún aspecto particular de la seguridad de la información de VEIASA debe emanar de esta política, tal como se indica en el epígrafe 7. Desarrollo de la Política de Seguridad del presente documento.

4. ALCANCE

Esta Política de Seguridad es de aplicación a toda la información y servicios de VEIASA, con independencia del atributo que les afecte (Confidencialidad, Disponibilidad, Integridad, Autenticidad o Trazabilidad), la forma en la que se presente, el lugar en el que se encuentre, y el personal que la procese. La política es aplicable, igualmente, en todas fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción).

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.

El Comité de Dirección de VEIASA es el responsable último de la presente Política de Seguridad Corporativa e impulsor de su cumplimiento. Para facilitar y asegurar la correcta implantación de la política de seguridad, proporcionará los medios técnicos y humanos que se consideren adecuados en cada momento.

5. 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.

- **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.

- **Estructura de operación**, que se encarga de implantar las medidas de seguridad identificadas.

5.1 ESTRUCTURA DE ESPECIFICACIÓN

Esta estructura es la encargada de determinar los requisitos de seguridad que serán de aplicación *a la información y* a los servicios prestados por VEIASA y a garantizar el cumplimiento normativo asociado que le es de aplicación, en concreto el Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad.

Forman parte de esta estructura:

- el Responsable de la Información
- el Responsable del Servicio.

5.1.1 Responsable de la Información

La figura del responsable de la Información establecerá el nivel de seguridad que la información requiere, en base a sus exigencias en cuanto a confidencialidad e integridad y trazabilidad, considerando el impacto que tendría en los clientes y en la propia Organización la falta de alguno de esos aspectos.

El Responsable de la Información, que podrá ser una persona o un órgano colegiado, será nombrado por el Comité de Dirección.

5.1.2 Responsable del Servicio

El Responsable del Servicio establecerá los requisitos de seguridad de los servicios prestados por VEIASA, en base a sus exigencias en cuanto a disponibilidad, autenticidad y trazabilidad, considerando el impacto que tendría en los clientes y en la propia organización un incidente que afectara a alguno de esos aspectos.

El Responsable del Servicio, que podrá ser una persona o un órgano colegiado, será nombrado por el Comité de Dirección.

5.2 ESTRUCTURA DE SUPERVISIÓN

La estructura de supervisión de la seguridad se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.

En la supervisión global de todas las actividades relativas a la seguridad de la información se encuentra el Responsable de Seguridad de la Información.

En la supervisión global de las actividades relativas a la seguridad física se encuentra el Responsable de Seguridad Física.

En la supervisión global de las actividades relacionadas con el tratamiento de datos personales se encuentra el Delegado de Protección de Datos.

Para la coordinación global e integral de la seguridad se encuentra el Comité de Seguridad Corporativa.

Las funciones y responsabilidades de cada una de las figuras se describen a continuación:

5.2.1 Responsable de Seguridad de la Información

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de seguridad de la información en la Organización.

Este Responsable forma parte del Comité de Seguridad Corporativa, tomando el papel de Secretario del Comité y, por tanto, es el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad de la información.

Sus responsabilidades comprenden:

- Convocar las reuniones del Comité de Seguridad Corporativa
- Asesorar al Comité de Seguridad Corporativa
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de la Organización.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de las normas y procedimientos establecidos.
- Conseguir que se elabore el presupuesto anual de seguridad TI de la Organización.
- Definir un modelo de gestión de la seguridad alineado con la estrategia de la Organización en materia de seguridad. A este modelo de gestión se le llamará SGSI, independientemente de que esté basado en las normas internacionales que recomiendan cómo hacerlo, o se trate de un modelo diferente.
- Supervisar la implantación práctica de la estrategia de seguridad de la información de la Organización.
- Seguir el desarrollo de las acciones identificadas en los planes de gestión del riesgo y cumplimiento.
- Supervisar las situaciones excepcionales (o incidentes) de ciberseguridad producidas en la o rganización.
- Promover la realización de análisis de riesgos de seguridad de la información de forma periódica.
- Solicitar a la Dirección de RRHH la realización de programas de formación y sensibilización en materia de seguridad de la información y seguimiento de los mismos.
- Analizar los indicadores de seguridad para medir la eficacia y eficiencia de las medidas implantadas.
- Analizar los incidentes de seguridad de la información reflejados en los registros de estos y verificar que se han establecido los planes para su resolución.
- Mantener actualizada la documentación asociada a la gestión de la seguridad de la información: normativas, procedimientos y registros.
- Autorizar por escrito la ejecución de procedimientos de recuperación de datos en los casos en que se requiera.
- Colaborar con las Auditorías externas/internas en materia de seguridad de la información, revisarlas y encargar a los responsables de los sistemas la implantación de las correcciones que se deriven.
- Establecer la Declaración de Aplicabilidad de medidas de seguridad seleccionadas del catálogo recogido en el Anexo II del ENS.

El Responsable de Seguridad de la Información será nombrado por el Comité de Seguridad *Corporativa*.

5.2.1.1. Función Diferenciada

En virtud del artículo 10 del ENS y del artículo 5.j de la Política de Seguridad de las Tecnologías de la Información y Comunicaciones en la Administración de la Junta de Andalucía, la función del Responsable de Seguridad estará diferenciada de otras funciones asociadas a la prestación de los servicios, por lo que dicho rol no podrá recaer en el Responsable del Sistema o en sus colaboradores para la prestación de servicios.

En este sentido, se establece que el Responsable de Seguridad de la Información deberá ejercer su labor sin estar condicionado por su ubicación en el esquema organizativo de VEIASA y deberá reportar directamente al Comité de Seguridad *Corporativa*, independientemente de que se adscriba a cualquier área de la Organización.

5.2.2 Responsable de Seguridad Física

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de seguridad física en la Organización.

Este Responsable forma parte del Comité de Seguridad Corporativa, siendo el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad física de los locales y las infraestructuras.

Sus responsabilidades comprenden:

- Identificación de necesidades de seguridad física.
- Conseguir la elaboración de un presupuesto anual de inversiones y actuaciones en seguridad física.
- Supervisar la instalación y el mantenimiento posterior de los elementos y servicios destinados a la seguridad física.
- Analizar los incidentes de seguridad física que se puedan haber producido y establecer actuaciones para dar respuesta a los mismos.
- Participar en el Comité de Seguridad Corporativa.

5.2.3 **Delegado de Protección de Datos**

Es la persona encargada de asesorar a la Dirección en materia de protección de datos personales y de verificar que se cumple la legislación aplicable en dicha materia en todo momento.

Sus funciones comprenden:

- Informar y asesorar a la Dirección y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento General de Protección de Datos y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas corporativas en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participe en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.
- Cooperar con la Agencia Española de Protección de Datos
- Actuar como punto de contacto de la AEPD para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

5.2.4 **Comité de Seguridad Corporativa**

Ver Manual de Responsabilidades y Funciones.

5.3 ESTRUCTURA DE OPERACIÓN

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.

Se describen a continuación las funciones y responsabilidades de las figuras asociadas a la estructura de operación.

5.3.1 **Responsable del Sistema**

Es la persona encargada de la operación del Sistema de Información de la organización, siguiendo las directrices del Responsable de Seguridad de la Información en materia de seguridad.

Sus funciones y responsabilidades son:

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Organización.
- Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticación, control de acceso, auditoría y registro.
- Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada (perfil inicial de seguridad. Bastionado).
- Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.
- Verificar el funcionamiento de mecanismos de Control de Acceso que eviten que un usuario acceda a datos o recursos con derechos distintos de los autorizados, sin que en ningún caso se puedan desactivar.
- Seguir los foros de vulnerabilidades y elaboración del calendario de aplicación de parches para los sistemas de información, en función de los que surjan y el impacto que tengan en la seguridad (los parches mismos los aplicarán los administradores de sistemas).
- Implantar las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.
- Proporcionar datos para la alimentación de indicadores de seguridad de la información.
- Supervisar los procedimientos de copia de seguridad.
- Realizar auditorías técnicas periódicas de la infraestructura, sistemas y aplicaciones.
- En los sistemas de categoría alta, acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescrita, a la vista del dictamen de auditoría.

En materia de seguridad, el Responsable del Sistema deberá seguir las directrices del Responsable de Seguridad de la Información.

5.4 Resolución de conflictos

Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura de gestión y organización de la seguridad definida en el presente documento serán resueltos por el superior jerárquico común. En su defecto, prevalecerá la decisión del Comité de Seguridad Corporativa.

En los conflictos entre las personas responsables que componen la estructura de gestión y organización de la seguridad definida en el presente documento, y las personas responsables definidas en la normativa de protección de datos de carácter personal, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

6. 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:

6.1 LA SEGURIDAD EN LA ORGANIZACIÓN

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

6.2 ANÁLISIS Y GESTIÓN DE RIESGOS

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

Como metodología base para la realización de los análisis de riesgos se utilizará MAGERIT, siendo esta metodología la más recomendable para el sector público nacional.

Se utilizarán, como punto de partida, el catálogo de amenazas de seguridad previsto en la metodología. 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 hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

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.

El análisis de riesgos se realizará igualmente 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. En estos casos se contemplarán en el alcance del análisis todos aquellos activos que intervengan en el tratamiento, considerando tanto activos relacionados con los sistemas de información, como humanos, locales o terceros.

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

6.3 FORMACIÓN Y CONCIENCIACIÓN

El personal que acceda, use, gestione, opere, desarrolle o mantenga activos o información propiedad de VEIASA deberá asistir a una sesión de concienciación en materia de seguridad, al menos, una vez cada dos años. Se establecerá un plan de concienciación para impartir dichas sesiones.

Las personas con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados en las 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

Con carácter bienal se realizará una acción de formación y concienciación en materia de seguridad. El objetivo de la acción formativa y de concienciación es doble:

- mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, riesgos, medidas de protección, configuración segura de sistemas, desarrollo seguro, etc.
- concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

El primer objetivo se asocia a Formación y el segundo a Concienciación.

Las áreas responsables determinarán el formato de la acción de Formación y Concienciación, así como sus contenidos.

6.4 DATOS DE CARÁCTER PERSONAL

VEIASA solo recogerá 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 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 recorridos en el Registro de Actividades de Tratamiento.

6.5 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.

6.6 PROTECCIÓN DE LOS SISTEMAS

Los sistemas de información deberán estar ubicados en zonas protegidas, con acceso restringido, habilitado únicamente al personal autorizado.

6.7 SEGURIDAD POR DEFECTO

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

- El sistema ofrecerá 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 estará 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.

6.8 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.

6.9 ACTUALIZACIÓN DE LOS SISTEMAS

Se deberán seguir en todo momento las informaciones acerca de las vulnerabilidades que afectan a los sistemas de información.

Se seguirán las recomendaciones de los fabricantes de equipos y software en cuanto a actualizaciones de seguridad, que deberán ser analizadas en cuanto a su idoneidad y conveniencia, y aplicadas en caso positivo con la menor dilación.

6.10 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

Se deberán proteger los entornos que contienen información y en tránsito en entornos inseguros. En este sentido se deberán proteger convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles (lápices de memoria, discos duros extraíbles, etc.)

6.11 PROTECCIÓN DEL PERÍMETRO

Se desplegarán 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 sea iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros.

6.12 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.

6.13 GESTIÓN DE INCIDENTES DE SEGURIDAD

VEIASA definirá e implantará procedimientos de gestión de incidentes de seguridad que aseguren 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.

El procedimiento de gestión y respuesta a incidentes de seguridad contemplará la comunicación y notificación de los incidentes a los organismos receptores de dicha información, de acuerdo con la legalidad vigente.

6.14 CONTINUIDAD DE NEGOCIO

Para asegurar la disponibilidad de los servicios y sistemas de información, VEIASA diseñará e implantará Planes de Continuidad de Servicio que eviten las interrupciones de las actividades de la organización y garanticen, ante una contingencia, la reanudación de los servicios y sistemas de información a los niveles adecuados de operatividad.

6.15 GESTIÓN DE LA SEGURIDAD Y MEJORA CONTINUA

Se deberá establecer 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.

6.16 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.

7. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad se desarrollará 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.

Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como a la normativa aplicable en materia de protección de datos de carácter personal.

Los niveles de desarrollo son los siguientes:

1. **Primer nivel**: Política de seguridad ENS, constituida por el presente documento. Es de obligado cumplimiento en toda la organización. Será aprobado por la persona titular de la Dirección General.

2. **Segundo nivel**: Normativa de Seguridad. Describe de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores. Son de obligado cumplimiento en toda la organización. Será aprobado por la persona titular de la Dirección General.

3. **Tercer nivel**: Procedimientos de Seguridad de la Información. Describen las acciones a realizar de procesos concretos relacionados con la seguridad de una manera más específica. Son dependientes de las normas de seguridad y especifican aspectos concretos de las mismas. Será aprobados por la persona titular de la Dirección de Transformación Económica y Digital.

4. **Cuarto nivel**: Guías y documentación técnica. En este último nivel se encuentra toda la documentación técnica o especializada que se considere necesaria para completar y facilitar la implementación y el desarrollo de las medidas de seguridad. Será aprobado por la persona titular de la Dirección Técnica y de Operaciones.

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.

8. 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.

9. 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 que, en caso de cambios, podrá proponer al Comité de Dirección su aprobación.

80119832E FRANCISCO JOSE DELGADO (R: A41398645)

Firmado digitalmente por 80119832E FRANCISCO JOSE DELGADO (R: A41398645)
Fecha: 2022.04.28 10:00:51 +02'00'

Francisco José Delgado Aguilera
Director General de Verificaciones Industriales de Andalucía, S.A.