

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por: Consultor	Validado por: Responsable de Seguridad de la Información	Aprobado por: Director General
Organización: ESTUDNET S.I.	Organización: SEGURIDAD INTEGRAL SECOEX S.A.	Organización: SEGURIDAD INTEGRAL SECOEX S.A.
		Firma:
Fecha: 13/01/2020	Fecha: 12/11/2024	Fecha: 18/11/2024
<p>Descripción: Política de Seguridad de la Información de conformidad con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y la UNE-ISO/IEC 27001:2023 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información Requisitos</p>		
Control de Versiones		
Versión	Fecha	Descripción del cambio
1.0	31/01/2020	Primera versión
2.0	09/11/2020	Ampliación requisitos mínimos de seguridad

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

3.0	12/11/2024	Se actualiza apartado 3 y las referencias al ENS obsoleto e ISO obsoleta.
-----	------------	---

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

1. Objeto y ámbito de aplicación

El presente documento tiene por objeto establecer la Política de Seguridad de la Información (en adelante, PSI) de SEGURIDAD INTEGRAL SECOEX S.A. (en adelante, SECOEX) y describir las directrices que han de regir la misma.

La PSI de SECOEX, que se integra en el Sistema de Gestión de Seguridad de la Información de SECOEX, será de aplicación para todo el personal de SECOEX y colaboradores.

2. Definiciones

A los efectos previstos en esta PSI, las definiciones y términos han de ser entendidos en el siguiente sentido:

- **AUTENTICIDAD:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **CONFIDENCIALIDAD:** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **DISPONIBILIDAD:** Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- **GESTIÓN DE RIESGOS:** actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- **INFRAESTRUCTURA TECNOLÓGICA:** aquellos recursos, físicos y lógicos, sobre los que se soportan los sistemas de información.
- **INTEGRIDAD:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **MEDIDAS DE SEGURIDAD:** Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

- **RIESGO:** estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:** Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.
- **SISTEMA DE INFORMACIÓN:** conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **TRAZABILIDAD:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

3. Marco normativo

El marco normativo de los servicios de SECOEX es el siguiente:

ESTATAL

- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (BOE núm. 77, de 31 de marzo).
- Ley 5/2014, de 4 de abril, de Seguridad Privada (BOE núm. 83, de 5 de abril).

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada (BOE núm. 8, de 10 de enero de 1995).
- Real Decreto 513/2017, de 22 de mayo, por el que se aprueba el Reglamento de instalaciones de protección contra incendios (BOE 12.06.17)
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. nº 298, de 14/12/1999).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (en adelante RLOPD) (B.O.E. nº 17, de 19/01/2008).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 34/2002, de 11 de junio, 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
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

EUROPEO

- Reglamento General de Protección de Datos (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.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

4. Misión

La misión de SECOEX es prestar a empresas, instituciones y particulares, soluciones globales de seguridad que les permitan vivir y desarrollar sus actividades con total tranquilidad.

5. Principios de seguridad de la información

Sin perjuicio de los principios básicos establecidos en el Esquema Nacional de Seguridad (en adelante, ENS), la PSI de SECOEX, en el ámbito de la Administración electrónica, se desarrollará, de acuerdo con los siguientes principios:

- Principio de seguridad integral: la seguridad de la información se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.
- Principio de confidencialidad: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.
- Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.
- Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los sistemas de información y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

- Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.
- Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.
- Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.
- Principio de detección y respuesta: los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad
- Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.
- Principio de mejora continua: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de SECOEX.
- Principio de seguridad TIC en el ciclo de vida de los sistemas de información: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

6. Valores de seguridad de la información

Además de los principios anteriores, la PSI de SECOEX se sustenta en los siguientes valores:

- La concienciación y la formación del personal adscrito a SECOEX, sobre las amenazas y las medidas de seguridad de la información, como acción de participación y corresponsabilidad.
- El análisis de los riesgos de la seguridad de la información manejada por SECOEX, como principio para la prevención de las amenazas a la confidencialidad, la integridad, la continuidad, la autenticidad y la trazabilidad de la información y de los servicios prestados a las entidades interesadas.
- La gestión, proactiva o correctiva, de los incidentes de seguridad de la información manejada por SECOEX, como principio para la mitigación de sus efectos sobre a la confidencialidad, la integridad, la continuidad, la autenticidad y la trazabilidad de la información y de los servicios prestados a las entidades interesadas.
- El cumplimiento por SECOEX y sus colaboradores, de la legislación aplicable en materia de telecomunicaciones y nuevas tecnologías, con especial incidencia la relativa de protección de datos de carácter personal, como principio de respeto a los derechos fundamentales de protección de la intimidad y privacidad de las entidades a las que se presta servicio.
- La medida y el análisis de los indicadores de eficacia y eficiencia de gestión de la seguridad de la información manejada por SECOEX, como principio para la innovación y la mejora continua, en este ámbito, de los servicios prestados a cualquier entidad interesada.

7. Organización de la seguridad de la información de SECOEX

La estructura organizativa de la gestión de la seguridad de la información de SECOEX está compuesta por las entidades siguientes:

- El Comité de Seguridad de la Información.
- Las personas Responsables de la Información y del Servicio
- La persona Responsable de Seguridad de la Información
- La persona Responsable del Sistema de Información

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

- La persona Responsable de Protección de Datos Personales

8. Comité de Seguridad de la información de SECOEX

El Comité de Seguridad de la Información está compuesto por:

- Presidente: el Director General de SECOEX
- Vocales miembros:
 - Dirección de Seguridad: Responsable de la Información y del Servicio
 - Dirección de Central Receptora de Alarmas: Responsable de la Información y del Servicio
 - Dirección de RRHH/Jurídico: Responsable de la Información y del Servicio y Responsable de Protección de Datos Personales
 - Dirección de Financiero: Responsable de Seguridad de la Información
 - Responsable de Sistemas de Información: Responsable del Sistema de Información

El Comité de Seguridad de la Información supervisará y coordinará todas las actividades relacionadas con la seguridad de la información en SECOEX y ejercerá las siguientes funciones y competencias:

- Actualizar la PSI adaptándola los cambios organizativos, legales, operativos y tecnológicos.
- Establecer e impulsar los criterios y directrices sobre seguridad de la información.
- Establecer las medidas para mejorar y reforzar los sistemas de seguridad y control.
- Difundir la PSI, promoviendo las actividades de concienciación y formación en materia de seguridad para el personal dentro del ámbito de aplicación de la presente PSI.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

- Elaborar las directrices y normas de seguridad generales dentro del ámbito de aplicación de la presente PSI.
- Coordinar las decisiones y actuaciones de los diferentes responsables
- Implantar las medidas para la adecuación al cumplimiento del ENS y del Reglamento General de Protección de Datos.
- Impulsar los planes de mejora de la seguridad de la información de los sistemas de información de SECOEX.
- Priorizar las actuaciones en materia de seguridad de la información cuando los recursos sean limitados.
- Establecer los objetivos de seguridad de la información y proporcionar los recursos, personales y materiales, derivados de los planes y acciones para su ejecución, tomado en consideración las disponibilidades presupuestarias.
- Gestionar que el sistema de gestión de la seguridad de la información de SECOEX logre los resultados establecidos en los objetivos de seguridad de la información, articulando las acciones preventivas y correctivas necesarias.

- Establecer las acciones de concienciación y la formación del personal adscrito a SECOEX y a las partes interesadas, sobre las amenazas y las medidas de seguridad de la información, como principio de participación y corresponsabilidad.
- Analizar los riesgos de la seguridad de la información manejada por SECOEX, como principio para la prevención de las amenazas a la confidencialidad, la integridad, la continuidad, la autenticidad y la trazabilidad de la información y de los servicios prestados a las entidades interesadas.
- Gestionar, proactiva y correctivamente, los incidentes de seguridad de la información manejada por SECOEX, como principio para la mitigación de sus efectos sobre los servicios públicos prestados a las entidades interesadas.

El Comité se deberá reunir con carácter ordinario, al menos, una vez al año, y con carácter extraordinario cuando lo decida su Presidencia.

El Comité podrá recabar del personal técnico la información o asesoramiento pertinente para el ejercicio de sus funciones. En caso

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

necesario este personal podrá ser convocado por el Comité para su asistencia a las reuniones, en calidad de asesores, con voz, pero sin voto.

Así mismo se acuerda la constitución de un grupo de trabajo para el análisis, elaboración y ejecución de trabajos o actividades específicas, dentro del ámbito de sus funciones elevando sus propuestas para la aprobación del Comité.

9. Los Responsables de la Información.

Los Responsables de la Información, establecen las necesidades de seguridad de la información que maneja SECOEX y efectúan las valoraciones del impacto que tendría un incidente que afectara a su seguridad.

Tienen, además, en exclusiva, la potestad de modificar el nivel de seguridad requerido para la misma.

Esta responsabilidad recaerá en el titular de la unidad organizativa que gestione cada proceso en el ámbito del ENS.

Son funciones de los Responsables de la Información, dentro de su ámbito de actuación, las siguientes:

- Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

- Determinar la categoría de los sistemas de información, según lo descrito en el Anexo I del ENS.

Son, asimismo, responsables, junto con los Responsables del Servicio, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control.

10. Los Responsables del Servicio.

Los Responsable del Servicio, son quienes determinan los requisitos de seguridad de los servicios prestados.

Esta responsabilidad recaerá en el titular de la unidad organizativa que gestione cada servicio en el ámbito del ENS.

Asimismo, los Responsables del Servicio son los encargados, junto a los Responsables de la Información, de aceptar los riesgos residuales, resultado del análisis de riesgos, y de realizar su seguimiento y control.

11. El Responsable de Seguridad de la Información de SECOEX

El Responsable de Seguridad de la Información es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Serán funciones del Responsable de Seguridad las siguientes:

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Proponer la normativa correspondiente a las políticas específicas de seguridad.
- Aprobar la normativa correspondiente a los procesos, procedimientos e instrucciones técnicas de seguridad de la información.
- Actualizar, organizar y custodiar la documentación de seguridad y establecer los controles de acceso a la misma.
- Promover las actividades de concienciación y formación en materia de seguridad.
- Coordinar y seguir la adecuación al Esquema Nacional de Seguridad y al Reglamento General de Seguridad de la Información.
- Realizar los análisis de riesgos, seleccionar las salvaguardas a implantar y revisar el proceso de gestión del riesgo, elevando un informe anual al Comité.
- Promover las auditorías periódicas para verificar el cumplimiento de las obligaciones de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a proponer a los Responsables del Servicio y de la Información para que adopten las medidas correctivas o preventivas adecuadas.
- Coordinar el proceso de Gestión de la Seguridad.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período.
- Asesorar en la determinación de la categoría de los sistemas de información, según lo descrito en el Anexo I del ENS.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

- Establecer las medidas de seguridad que deben aplicarse, de acuerdo con lo previsto en el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

Para el ejercicio de sus funciones podrá recabar de personal técnico la información o asesoramiento pertinente y contar con el asesoramiento y apoyo del Comité de Seguridad de la Información.

12. El Responsable del Sistema de Información de SECOEX

El Responsable de Seguridad de los Sistemas de información, es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Serán funciones del Responsable de los Sistemas de Información, las siguientes:

- Desarrollar, operar y mantener los subsistemas de Información durante todo su ciclo de vida, así como aprobar y/o ejecutar los cambios que afecten a la seguridad del modo de operación del sistema.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, siguiendo las indicaciones del Responsable de Seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio, y con el Responsable de Seguridad.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

- 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 de los sistemas de información.
- La gestión de las autorizaciones concedidas a los usuarios las personas usuarias del sistema.
- La aplicación de los procedimientos de seguridad.
- Ejecutar los cambios de configuración del sistema de información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- 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 Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

13. Procedimiento de designación y renovación de responsables

El Administrador de SECOEX designará a los siguientes responsables:

- Información

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

- Servicios
- Seguridad
- Sistemas de información
- Delegado de Protección de Datos Generales

Los nombramientos se revisarán cada 2 años o cuando el puesto quede vacante.

14. Resolución de conflictos

En caso de conflicto entre los diferentes los responsables que componen la estructura organizativa de la PSI, este será resuelto en el seno del Comité de Seguridad de la Información de SECOEX.

En caso de conflicto entre las personas responsables que componen la estructura organizativa de la seguridad de la información en SECOEX y los definidos en la normativa de protección de datos de carácter personal, prevalecerá la decisión que determine la persona responsable del tratamiento, asesorado por el Delegado de Protección de Datos Personales, que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

15. Gestión de riesgos de la seguridad de la información

La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

El Responsable de Seguridad de la Información es el encargado de realizar los preceptivos análisis de riesgos, y de seleccionar las medidas de seguridad o salvaguardas a implantar.

Los Responsables de la Información y de los Servicios son los responsables o propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, y por tanto de aceptar los riesgos residuales calculados en el análisis, y de realizar su seguimiento y control.

El proceso de gestión de riesgos comprende la identificación y categorización de los sistemas y subsistemas de información, el análisis de riesgos y la selección de medidas de seguridad a aplicar, que deberán ser proporcionales y justificadas, revisándose, al menos, anualmente o cuando se produzca un cambio o incidente relevante, por parte el Responsable de Seguridad, que elevará un informe para su aprobación por el Comité de Gestión de la Seguridad de la Información.

16. Protección de datos de carácter personal.

En lo que se refiere a los ficheros con datos de carácter personal, estarán referenciados en el correspondiente Registro de Actividades de Tratamientos, realizándose un análisis de riesgos para establecer las medidas de seguridad.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

Todos los sistemas de información de SECOEX se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.

En caso de conflicto con la normativa de seguridad, prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

17. Desarrollo de documentación de seguridad de la información

La documentación de seguridad de la información será de obligado cumplimiento y se desarrollará en dos niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles son los siguientes:

- Primer nivel normativo: la presente PSI, y las disposiciones generales, directrices y normas de seguridad generales dentro del ámbito de aplicación de la PSI.
- Segundo nivel normativo: constituido por los Procedimientos e Instrucciones Técnicas STIC (Procedimientos STIC), desarrollado en detalle las disposiciones de la PSI en un ámbito determinado, dando así respuesta a qué y cómo actuar para planificar, implantar, registrar, evaluar y mejorar una medida de seguridad.

Los documentos relativos a este segundo nivel normativo los deberá aprobar el Comité de Gestión de la Seguridad de la Información, a propuesta del Responsable de Seguridad.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

El Responsable Seguridad será responsable de registrar, custodiar, actualizar y facilitar el acceso a la documentación de seguridad.

18. Obligaciones del personal

Todo el personal de SECOEX tiene la obligación de conocer y cumplir la normativa de seguridad que desarrolle la presente PSI, siendo responsabilidad del Comité de Seguridad de la información supervisar su observancia y disponer los medios necesarios para la difusión, concienciación y formación de los afectados.

Todo el personal que se incorpore o vaya tener acceso a los sistemas de información o a la información manejada por SECOEX, deberá ser informado de la PSI.

19. Formación y concienciación en seguridad de la información

SECOEX desarrollará las actividades necesarias para la concienciación y formación de su personal, así como a la difusión entre los mismos de la PSI y de su desarrollo normativo.

El Comité de Seguridad de la Información y el Responsable de Seguridad se encargarán de planificar, implantar, registrar, evaluar y mejorar las actividades de formación y concienciación de seguridad de la información.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

20. Auditoría de seguridad de la información

El sistema de gestión de seguridad de la Información y los sistemas de información de SECOEX, serán objeto, al menos, anualmente, de una auditoría, interna o externa, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales que puedan repercutir en el cumplimiento de las medidas de seguridad establecidas.

Los informes de auditoría se elevarán, para su aprobación, al Comité de Seguridad de la Información, identificándose las acciones preventivas o correctivas.

21. Actualización de la PSI

Para la actualización de la presente PSI, el Responsable de Seguridad de la Información elaborará su propuesta, sometiéndola a la revisión del Comité de Seguridad de la Información, para su aprobación por el Administrador de SECOEX.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

DECLARACIÓN

SEGURIDAD INTEGRAL SECOEX S.A. (en adelante, SECOEX), organización dedicada a prestar servicios globales de seguridad a empresas, instituciones y particulares es muy consciente de la importancia de la seguridad de la información, como factor clave para alcanzar la excelencia organizativa, la competitividad en el mercado, la sostenibilidad del negocio y el cumplimiento normativo.

SECOEX, con el fin de garantizar la confidencialidad, la integridad, la autenticidad, la trazabilidad y la disponibilidad de la información que maneja y de los servicios que presta, ha adoptado como marco un Sistema de Gestión de Seguridad de la Información, de acuerdo con:

- El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- La norma UNE-ISO/IEC 27001:2023. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información Requisitos

; que cubre de forma adecuada todos los requisitos necesarios y que se concreta en los objetivos siguientes:

- Establecimiento de un comité de seguridad de la información, con autoridad y competencia.
- Implantación de la organización de la seguridad, designando a los responsables de la seguridad, de los servicios, de la información, de la protección de datos personales y de los sistemas de información.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

- Análisis de los riesgos y las amenazas a la seguridad de la información manejada e implantar las medidas, organizativas, operativas y técnicas, necesarias para su debido tratamiento.
- Aseguramiento de la continuidad del negocio ante incidentes críticos.
- Planificación de los recursos, humanos y tecnológicos, para prestar los servicios a los clientes de acuerdo con los requisitos de seguridad de la información y de conformidad con la legislación vigente.
- Concienciación y formación de todo el personal y colaboradores, en los riesgos y amenazas de la información, la normativa para su prevención y mitigación y la notificación de las incidencias.
- Profesionalidad
- Métodos adecuados para la autorización y control de los accesos.
- Medidas necesarias para la protección de las instalaciones.
- Metodología y control para la adquisición de productos.
- Seguridad por defecto.
- Procedimientos que protejan la integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registros de actividad
- Control de los Incidentes de seguridad
- Medición y análisis los indicadores de seguridad de la información, permitiendo la gestión y mejora de la eficacia de las medidas y controles.
- Implantación de los procesos de auditoría y mejora continua, que garantice el mantenimiento de los controles y medidas de seguridad

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

- Cumplimiento de los requisitos legales, normativos y reglamentarios, con especial énfasis los que garantizan la protección de los datos personales.

La dirección de SECOEX, en coherencia, con lo anterior, está comprometida con el buen funcionamiento del Sistema de Gestión de Seguridad de la Información, asignando los recursos humanos y materiales, razonables y proporcionales, para la consecución de los objetivos anteriores y delegando en el Responsable de Seguridad de la Información la autoridad y las competencias necesarias para su implantación, acreditación, mantenimiento y mejora, para lo que cuenta con el respaldo del equipo directivo y personal de SECOEX.

SEGURIDAD INTEGRAL SECOEX S.A.

Administrador

FIRMA Y FECHA

18 de Noviembre de 2024

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: INTERNO		

DISPOSICIÓN FINAL

La Política de Seguridad de la Información de SECOEX será revisada, al menos, anualmente, para asegurar su continua idoneidad, adecuación y eficacia o actualizada, en el momento que se produzcan cambios significativos en la organización, en los procesos, en las tecnologías, en la legislación, en las amenazas y/o en los riesgos a la seguridad de la información.

Las versiones del presente documento serán elaboradas por el Responsable de Seguridad de la Información y aprobadas por el Comité de Seguridad de la Información de SECOEX, destruyéndose y registrando sus versiones.

Los cambios o mejoras a la Política de Seguridad de la Información, procedentes de los empleados de SECOEX o de cualquier parte interesada, serán recepcionados por el Responsable de Seguridad de la Información que analizará e informará al Comité de Seguridad de la Información sobre su idoneidad, procediéndose a su aceptación, en su caso, y al reconocimiento a las personas que los propongan.

La presente política estará accesible para todas las partes interesadas y será suscrita por todo el personal y colaboradores de SECOEX.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:3.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información		Clasificación: INTERNO	

ACUSE RECIBO

NOMBRE DEL EMPLEADO:

FIRMA

FECHA:

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:2.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: PÚBLICO		

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por: Consultor	Validado por: Responsable de Seguridad de la Información	Aprobado por: Comité de Seguridad de la Información									
Organización: ESTUDNET S.I.	Organización: SEGURIDAD INTEGRAL SECOEX S.A.	Organización: SEGURIDAD INTEGRAL SECOEX S.A.									
		Firma:									
Fecha: 13/01/2020	Fecha: 12/11/2024	Fecha: 18/11/2024									
Descripción: Declaración de la Política de Seguridad de la Información											
Control de Versiones:											
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%;">Versión</th> <th style="width: 20%;">Fecha</th> <th style="width: 60%;">Descripción del cambio</th> </tr> </thead> <tbody> <tr> <td>1.0</td> <td>31/01/2020</td> <td>Primera versión.</td> </tr> <tr> <td>2.0</td> <td>12/11/2024</td> <td></td> </tr> </tbody> </table>	Versión	Fecha	Descripción del cambio	1.0	31/01/2020	Primera versión.	2.0	12/11/2024			
Versión	Fecha	Descripción del cambio									
1.0	31/01/2020	Primera versión.									
2.0	12/11/2024										

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:2.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: PÚBLICO		

SEGURIDAD INTEGRAL SECOEX S.A. (en adelante, SECOEX), organización dedicada a prestar servicios globales de seguridad a empresas, instituciones y particulares es muy consciente de la importancia de la seguridad de la información, como factor clave para alcanzar la excelencia organizativa, la competitividad en el mercado, la sostenibilidad del negocio y el cumplimiento normativo.

SECOEX, con el fin de garantizar la confidencialidad, la integridad, la autenticidad, la trazabilidad y la disponibilidad de la información que maneja y de los servicios que presta, ha adoptado como marco un Sistema de Gestión de Seguridad de la Información, de acuerdo con:

- El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- La norma UNE-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información Requisitos

; que cubre de forma adecuada todos los requisitos necesarios y que se concreta en los objetivos siguientes:

- Establecimiento de un comité de seguridad de la información, con autoridad y competencia.
- Implantación de la organización de la seguridad, designando a los responsables de la seguridad, de los servicios, de la información, de la protección de datos personales y de los sistemas de información.
- Análisis de los riesgos y las amenazas a la seguridad de la información manejada e implantar las medidas, organizativas, operativas y técnicas, necesarias para su debido tratamiento.
- Aseguramiento de la continuidad del negocio ante incidentes críticos.
- Planificación de los recursos, humanos y tecnológicos, para prestar los servicios a los clientes de acuerdo con los requisitos de seguridad de la información y de conformidad con la legislación vigente.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:2.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: PÚBLICO		

- Concienciación y formación de todo el personal y colaboradores, en los riesgos y amenazas de la información, la normativa para su prevención y mitigación y la notificación de las incidencias.
- Medición y análisis los indicadores de seguridad de la información, permitiendo la gestión y mejora de la eficacia de las medidas y controles.
- Implantación de los procesos de auditoría y mejora continua, que garantice el mantenimiento de los controles y medidas de seguridad.
- Cumplimiento de los requisitos legales, normativos y reglamentarios, con especial énfasis los que garantizan la protección de los datos personales.

La dirección de SECOEX, en coherencia, con lo anterior, está comprometida con el buen funcionamiento del Sistema de Gestión de Seguridad de la Información, asignando los recursos humanos y materiales, razonables y proporcionales, para la consecución de los objetivos anteriores y delegando en el Responsable de Seguridad de la Información la autoridad y las competencias necesarias para su implantación, acreditación, mantenimiento y mejora, para lo que cuenta con el respaldo del equipo directivo y personal de SECOEX.

SEGURIDAD INTEGRAL SECOEX S.A.

Consejero Delegado

FIRMA Y FECHA

18 de noviembre de 2024

POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Versión:2.0	Fecha: 18/11/2024	
Sistema de Gestión de Seguridad de la información	Clasificación: PÚBLICO		

DISPOSICIÓN FINAL

La Política de Seguridad de la Información de SECOEX será revisada, al menos, anualmente, para asegurar su continua idoneidad, adecuación y eficacia o actualizada, en el momento que se produzcan cambios significativos en la organización, en los procesos, en las tecnologías, en la legislación, en las amenazas y/o en los riesgos a la seguridad de la información.

Las versiones del presente documento serán elaboradas por el Responsable de Seguridad de la Información y aprobadas por el Comité de Seguridad de la Información de SECOEX, destruyéndose y registrando sus versiones.

Los cambios o mejoras a la Política de Seguridad de la Información, procedentes de los empleados de SECOEX o de cualquier parte interesada, serán recepcionados por el Responsable de Seguridad de la Información que analizará e informará al Comité de Seguridad de la Información sobre su idoneidad, procediéndose a su aceptación, en su caso, y al reconocimiento a las personas que los propongan.

La presente política estará accesible para todas las partes interesadas y será suscrita por todo el personal y colaboradores de SECOEX.