sando

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Gestión Documental

Referencia	PSI-SGSI-001
Título de la *Norma*	Política de Seguridad de la Información
Categoría	Política
Fecha de aprobación	29-11-2024
Órgano de aprobación	Consejo de Administración
Versión aprobada	V1.1

INDICE

1. Introducción

En un entorno empresarial cada vez más interconectado y digitalizado, Grupo SANDO se erige como una entidad decididamente comprometida con la protección y salvaguarda de la información. De esta forma, reconocemos que la información no solo es un recurso fundamental para nuestras operaciones, sino que también constituye un activo crítico que sustenta la confianza de nuestros clientes, empleados y socios comerciales.

La presente Política de Seguridad de la Información (en adelante, "PSI") ha sido desarrollada con el objetivo de establecer directrices y principios claros que guíen al Grupo SANDO en la protección de la confidencialidad, integridad y disponibilidad de toda la información que gestionamos. Estas directrices son el marco en el que se estructuran las prácticas de seguridad de la información, permitiendo que Grupo SANDO mantenga un entorno seguro y resiliente frente a las diversas amenazas que podrían comprometer nuestros sistemas y datos.

Asimismo, el compromiso de Grupo SANDO no se limita a implementar medidas de seguridad; también abarca el cumplimiento riguroso de las leyes y regulaciones aplicables en materia de seguridad de la información. El Grupo SANDO se esfuerza por adherirse a las mejores prácticas del mercado, considerando tanto los estándares nacionales como internacionales. En particular, la PSI está alineada con los requisitos del Estándar Internacional ISO/IEC 27001:2022, que se reconoce como una referencia fundamental en la gestión de la seguridad de la información.

Entendemos que la protección de la información debe ser un esfuerzo continuo, y es por ello por lo que se han establecido principios básicos y líneas de actuación que el Grupo SANDO se compromete a aplicar de manera consistente.

Ciertamente, la presente PSI no solo es un documento regulador, sino que representa un compromiso organizacional integral que involucra a todos los miembros de nuestra comunidad corporativa. Cada empleado y colaborador tiene un papel fundamental en la implementación de estas directrices, lo que refuerza la responsabilidad compartida en la protección de nuestros activos informáticos.

De todo lo anterior se concluye que, a través de esta PSI, el Grupo SANDO reafirma su dedicación a la seguridad de la información, buscando no solo proteger sus activos, sino también promover un entorno de confianza y seguridad en todas nuestras interacciones comerciales.

2. Objetivos

El objetivo fundamental de la PSI del Grupo SANDO es proporcionar una declaración clara y formal de nuestras intenciones en materia de seguridad, abarcando tanto la ciberseguridad como la seguridad física.

Luego, el presente documento establece los principios y conceptos básicos que servirán de guía para el desarrollo y la implementación de otros documentos que integran el Cuerpo Normativo de Seguridad del Grupo SANDO. En este sentido, dado que la PSI es el documento de más alto nivel del Cuerpo Normativo de Seguridad, se erige como

el marco de referencia fundamental que orientará todas las acciones relacionadas con la protección de la información y la seguridad organizacional, así como todas las políticas y normas subsecuentes del Grupo SANDO.

La presente PSI tiene como objetivos clave los siguientes:

- **Cumplimiento normativo**: Asegurar el cumplimiento riguroso de las leyes, regulaciones y estándares aplicables en materia de seguridad de la información. Este objetivo implica no solo la identificación de las normativas relevantes, sino también la implementación de medidas que garanticen su observancia de manera continua y sistemática.

- **Salvaguarda de la información**: Proteger la información del Grupo SANDO contra accesos no autorizados, divulgaciones indebidas, alteraciones y destrucciones no intencionadas. Este objetivo se logra a través de la implementación de controles técnicos y organizativos que mitiguen los riesgos asociados a la gestión de la información.

- **Confidencialidad, integridad y disponibilidad**: Asegurar que la confidencialidad, integridad y disponibilidad de la información sean mantenidas en todo momento. Esto requiere un enfoque integral que contemple la gestión adecuada de la información a lo largo de su ciclo de vida.

- **Disponibilidad y rendimiento de sistemas**: Garantizar que los sistemas de información y los servicios críticos estén disponibles y funcionen de manera óptima. Esto incluye la realización de evaluaciones periódicas y pruebas de rendimiento para identificar y corregir posibles fallos en los sistemas.

- **Minimización de riesgos**: Trabajar activamente para minimizar los riesgos asociados a la seguridad de la información. Esto se complementa con la promoción de una cultura de seguridad organizacional, que se logrará a través de la concienciación, formación y capacitación continua de todos los empleados del Grupo SANDO.

- **Definición de roles y responsabilidades**: Establecer claramente los roles necesarios y definir las responsabilidades asociadas a la gestión de la seguridad de la información. Este objetivo es esencial para asegurar que cada miembro de la organización entienda su papel en la protección de los activos de información.

La PSI del Grupo SANDO, en su esencia, no solo establece un marco de protección, sino que también refuerza el compromiso de la organización con la seguridad y la integridad de sus operaciones. Al adherirnos a estos objetivos, el Grupo SANDO se posiciona para enfrentar los desafíos del entorno actual, garantizando una gestión eficaz de la seguridad de la información que sustenta su éxito a largo plazo.

3. Alcance

La presente Política de Seguridad de la Información es de obligatorio cumplimiento para todos los usuarios de las entidades que conforman el Grupo SANDO que tengan acceso

a los activos de información de la organización. Esto incluye, pero no se limita a, las oficinas centrales, los centros de producción y los empleados que realicen su labor en modalidad remota.

Para los efectos de esta PSI, se considerarán usuarios a todos los profesionales que integran la Sociedad, lo cual abarca a todo el personal directivo, técnico, administrativo, productivo y de servicios. Esta categorización es aplicable sin distinción del tipo de contrato laboral que cada individuo ostente, ya sea este de carácter fijo, temporal o cualquier otra modalidad que regule la relación laboral.

Adicionalmente, se extiende la consideración de usuarios a terceros, lo que incluye a clientes, proveedores, subcontratistas y demás entidades o individuos que colaboren con Grupo SANDO. Este grupo de usuarios abarca a todos aquellos que, por cualquier razón, tengan acceso a los mecanismos y recursos informáticos y tecnológicos de la Sociedad, ya sea de forma directa o indirecta.

La inclusión de estos diversos grupos como usuarios de la Política subraya la importancia de una cultura de seguridad integral que abarque no solo a los empleados del Grupo SANDO, sino también a aquellos que interactúan con la organización en el marco de relaciones comerciales o de prestación de servicios.

En consecuencia, todos los usuarios mencionados están obligados a cumplir con las directrices establecidas en esta Política, así como con cualquier normativa complementaria que se derive de la misma.

4. Ámbito de aplicación

La presente Política de Seguridad de la Información tiene un ámbito de aplicación global y es de cumplimiento obligatorio en todas las entidades que forman parte del Grupo SANDO. Este cumplimiento se establece sin menoscabo de las particularidades que pudieran derivarse de la legislación vigente aplicable en cada una de las sociedades integrantes del grupo.

A los efectos de esta Política, se entenderá por Grupo SANDO a aquellas sociedades en las que la entidad posea, de forma directa o indirecta, la mayoría de las acciones, participaciones o derechos de voto. Asimismo, se considerará parte del Grupo a aquellas sociedades en las que Grupo SANDO haya designado o tenga la facultad de designar a la mayoría de los miembros de su Órgano de Administración, garantizando así un control efectivo sobre dichas entidades. Esta definición se aplica independientemente del tratamiento que se dé a la información, de los individuos que tengan acceso a la misma, del medio de almacenamiento utilizado o de su ubicación, abarcando tanto información física como electrónica.

La Política se extiende a todas las fuentes de información gestionadas por las sociedades del Grupo SANDO, enfatizando la importancia de proteger tanto los activos de información en formato digital como los documentos y datos físicos. Esta integración es esencial para asegurar una gestión uniforme y coherente de la seguridad de la información a lo largo de todas las entidades del Grupo.

Adicionalmente, la presente Política de Seguridad de la Información estará disponible para su consulta en la página web oficial de Grupo SANDO, en el enlace

www.sando.com. Asimismo, se garantiza que todos los empleados del Grupo SANDO tendrán acceso a este documento a través de un repositorio compartido designado específicamente para tal fin. Este acceso asegura que todos los miembros de la organización estén debidamente informados sobre las políticas y directrices que regulan la seguridad de la información, promoviendo así una cultura de seguridad que involucre a toda la organización.

5. Principios

Con el fin de llevar a cabo las actividades y tareas relacionadas con la seguridad de la información, Grupo SANDO reconoce la necesidad de que los siguientes principios sean fundamentales y prevalentes en todas sus operaciones:

- **Alineación con la estrategia de negocio**: Todas las iniciativas y acciones relacionadas con la seguridad de la información deben estar alineadas con la estrategia general de negocio de Grupo SANDO. Esto garantiza que la gestión de la seguridad no solo proteja los activos informáticos, sino que también respalde los objetivos comerciales y el crecimiento sostenible de la organización.

- **Cumplimiento normativo**: Es imperativo que todas las tareas y actividades vinculadas a la seguridad de la información se realicen en estricta conformidad con los reglamentos, legislación y contratos aplicables. Este compromiso legal asegura que Grupo SANDO actúe dentro de un marco regulatorio claro y establecido, minimizando riesgos legales y reputacionales.

- **Análisis de riesgos**: Se llevará a cabo un análisis riguroso de los riesgos y amenazas actuales y proyectados que puedan afectar a la seguridad de la información, de acuerdo con lo establecido en las políticas corporativas. Este análisis es esencial para identificar vulnerabilidades y establecer controles proactivos.

- **Respeto a los principios corporativos**: Todas las actividades relacionadas con la seguridad de la información deben respetar los principios corporativos de Grupo SANDO, los cuales guían la conducta y las decisiones en el ámbito de la seguridad. Estos principios crean un marco ético y operativo que sustenta nuestra política de seguridad.

- **Compromiso con los requisitos de seguridad**: Grupo SANDO se compromete a satisfacer todos los requisitos aplicables relacionados con la seguridad de la información. Este compromiso es crucial para mantener la confianza de nuestros clientes y partes interesadas.

- **Mejora continua**: La organización se compromete a implementar un enfoque de mejora continua en el sistema de gestión de seguridad de la información. Esto implica la revisión periódica de políticas y procedimientos, así como la adaptación a nuevas amenazas y tecnologías emergentes.

- **Asignación de responsabilidades**: Se asignarán responsabilidades y funciones diferenciadas para la gestión de la seguridad de la información. Esta asignación clara de roles es fundamental para garantizar que todas las áreas de

la organización comprendan sus responsabilidades y trabajen de manera cohesiva para proteger los activos de información.

- **Protección de dimensiones básicas de seguridad**: Grupo SANDO se compromete a proteger las dimensiones esenciales de la seguridad de la información, que incluyen la confidencialidad, integridad y disponibilidad de los datos y sistemas en todas sus operaciones. Estas dimensiones son pilares fundamentales de nuestra estrategia de seguridad.

- **Consideración de otras dimensiones de seguridad**: Además de las dimensiones básicas, se tendrán en cuenta otras dimensiones críticas de seguridad, tales como la trazabilidad, autenticidad y no repudio, que son igualmente esenciales para asegurar la confianza y la transparencia en nuestras operaciones.

- **Concienciación del personal**: Es fundamental que todo el personal de Grupo SANDO conozca la existencia de esta PSI, así como de los documentos que componen el resto del Cuerpo Normativo de Seguridad, en la medida que estos sean aplicables a sus funciones y actividades diarias. La concienciación y formación del personal son componentes clave para la efectividad de nuestra política.

En consonancia con nuestro compromiso hacia la seguridad de la información, la presente política se fundamenta en las mejores prácticas de seguridad establecidas en el Estándar Internacional ISO/IEC 27001:2022. Esta norma proporciona un marco robusto para la gestión de la seguridad de la información, orientando la identificación y evaluación de riesgos de seguridad, así como la implementación de controles adecuados para mitigar tales riesgos.

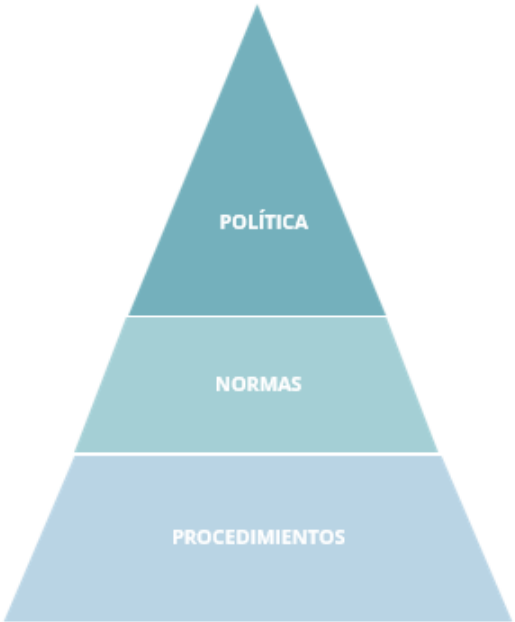
Adicionalmente, Grupo SANDO se compromete a cumplir rigurosamente con las leyes y regulaciones pertinentes en materia de protección de datos, en particular el Reglamento General de Protección de Datos (RGPD) de la Unión Europea y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD). Estos marcos legales establecen principios fundamentales para el tratamiento de datos personales, incluyendo su recolección, procesamiento, almacenamiento y transferencia. Nuestros procedimientos internos están alineados con estos requisitos legales, asegurando que los datos personales sean tratados de manera legal, justa y transparente, así como implementando medidas de seguridad adecuadas para proteger la privacidad de todos los individuos involucrados.

6. Cuerpo Normativo de Seguridad (CNS)

Para cumplir con los objetivos listados en el apartado anterior se desarrollan documentos más específicos enmarcados en diferentes niveles de acuerdo con el nivel de detalle y concreción que corresponda en cada caso.

De forma general, el Cuerpo Normativo de Seguridad se compone de una estructura piramidal mediante diferentes niveles, según el grado de detalle que se describe en cada uno. A continuación, se describen los niveles del CNS:

- **Nivel 1 - Política de Seguridad de la Información,** de ella dependen la totalidad de los documentos que componen el Cuerpo Normativo de Seguridad. Se trata de un documento de declaración de intenciones que formaliza y presenta la totalidad del CNS a alto nivel.
- **Nivel 2 – Normativas de Seguridad**, son documentos que describen de forma específica los controles concretos que el personal y el Grupo SANDO debe disponer para asegurar la protección de los activos de la organización. Cada Normativa ha sido definida basándose en los dominios y temáticas de seguridad habituales, así como en las regulaciones aplicables al Grupo SANDO.
- **Nivel 3 –** El tercer nivel del CNS se compone de Procedimientos, Guías, Directivas, Anexos y Otros documentos.
    - **Procedimientos**, son documentos que definen el cómo se realizan los diferentes procesos en el Grupo SANDO con funciones y tareas bien definidas.
    - **Guías**, ofrecen información muy detallada sobre un proceso o tarea, para un producto, una tecnología o un entorno concreto.
    - **Planes,** son documentos que detallan como se lleva a cabo la gestión de seguridad en ambientes específicos en los que la información de la compañía podría verse afectada.
    - **Anexos**, complementan información que pueda ser del alcance de más de un documento.
    - **Otros** documentos de diferente índole aplicables en materia de seguridad.



La Política de Seguridad de la Información se engloba dentro del primer nivel del CNS del Grupo SANDO.

7. Desarrollo de la Política de Seguridad de la Información

El desarrollo de la Política de Seguridad de la Información es fundamental para establecer un marco robusto que garantice la confidencialidad, integridad y disponibilidad de la información en el Grupo SANDO. Esta política se basa en la identificación y gestión de riesgos, la integración de medidas de seguridad en todas las etapas del ciclo de vida de los sistemas de información, y la promoción de una cultura de seguridad en toda la organización. A través de normas específicas y procedimientos claramente definidos, se busca mitigar amenazas y vulnerabilidades, asegurando así un entorno seguro para el manejo de datos críticos y la continuidad del negocio.

7.1 Gobierno de ciberseguridad

La Política de Seguridad de la Información de Grupo SANDO se fundamenta en una estructura organizativa sólida y un modelo de gobierno claro, que establece roles y responsabilidades para la gestión efectiva de la seguridad.

El gobierno de la seguridad es administrado por un Comité de Seguridad, compuesto por miembros clave de la Alta Dirección. Este Comité actúa como la principal autoridad en materia de ciberseguridad, con la responsabilidad de aprobar el Cuerpo Normativo de Seguridad y supervisar su implementación. Se reúne semestralmente para evaluar las prácticas de seguridad y asegurar la alineación con los objetivos organizacionales.

Adicionalmente, el Delegado de Protección de Datos (DPO) juega un papel crítico en el cumplimiento del Reglamento General de Protección de Datos (GDPR), asegurando que la organización se adhiera a las normativas de protección de datos.

A su vez, se supervisa el cumplimiento de los controles de seguridad establecidos, evaluando continuamente los riesgos y proponiendo medidas correctivas cuando sea necesario. Además, todos los empleados del Grupo SANDO deben ser informados sobre sus responsabilidades en relación con la seguridad de la información y comprometerse a cumplir las normas establecidas.

Finalmente, el Grupo SANDO se compromete a proporcionar formación continua en ciberseguridad a su personal, asegurando que todos estén debidamente capacitados y concienciados sobre la importancia de proteger la información a lo largo de su relación contractual con la organización.

7.2 Ciberseguridad relativa a los recursos humanos

La gestión de la ciberseguridad en relación con los recursos humanos en Grupo SANDO se desarrolla mediante un enfoque integral que abarca el ciclo de vida completo del empleado. Este enfoque garantiza que cada trabajador esté debidamente calificado

para su puesto y que comprenda a cabalidad sus responsabilidades en materia de seguridad de la información.

Los contratos laborales deben reflejar las políticas de seguridad de la organización, incluyendo acuerdos de confidencialidad que deben ser firmados por todos los empleados que tengan acceso a información sensible. Estos acuerdos se revisarán de manera periódica y deberán especificar aspectos cruciales como la información protegida, la duración del acuerdo y las acciones a seguir en caso de incumplimiento.

Durante el transcurso de la relación laboral, es esencial que cada miembro del personal esté al tanto de sus responsabilidades en materia de ciberseguridad. Las políticas y procedimientos de seguridad son comunicados de manera clara y se establece un plan de formación continua para garantizar la concienciación sobre la importancia de la seguridad de la información.

Además, se ha implementado un proceso disciplinario formal para abordar cualquier infracción de seguridad. Este proceso asegura un trato justo hacia los empleados implicados, garantizando que las respuestas sean proporcionales a la gravedad de la infracción, así como la posibilidad de adoptar medidas disuasorias.

Finalmente, al concluir la relación laboral, se comunican las responsabilidades que permanecen vigentes, tales como la confidencialidad de la información y la protección de la propiedad intelectual. Se establece un procedimiento para la devolución de activos, asegurando que todos los bienes, tanto físicos como electrónicos, sean retornados. Asimismo, se controla la transferencia de conocimientos críticos para salvaguardar la información de la organización.

En conjunto, estas directrices aseguran que la seguridad de la información se convierta en una responsabilidad compartida en todas las etapas del ciclo laboral, reforzando así la cultura de ciberseguridad dentro de Grupo SANDO.

7.3 Gestión de riesgo y terceras partes

La gestión del riesgo en Grupo SANDO es un elemento esencial para la salvaguarda de la ciberseguridad, y se implementa a través de un enfoque estructurado que abarca todo el ciclo de vida del riesgo.

El Comité de Seguridad es el encargado de supervisar y aprobar las normativas de gestión de riesgos, las cuales incluyen un análisis anual de riesgos. Este análisis se actualizará ante cualquier cambio significativo en la organización o su entorno.

Es fundamental llevar a cabo la identificación y clasificación de todos los activos, así como realizar una identificación de amenazas conforme a estándares internacionales. Las amenazas deberán ser clasificadas según su impacto y probabilidad, y este proceso se revisará de manera periódica para asegurar su vigencia y relevancia.

La gestión del riesgo implica clasificar estos riesgos según niveles previamente establecidos, definiendo un umbral de riesgo y designando un responsable para cada uno. Las decisiones sobre la mitigación, aceptación, evitación o transferencia de riesgos se fundamentarán en los resultados del análisis realizado, y cualquier excepción a estas decisiones deberá ser documentada y autorizada por el Comité de Seguridad.

La relación con proveedores y terceras partes también es objeto de una gestión minuciosa, que incluye una evaluación exhaustiva de los riesgos asociados a la

externalización de información crítica. Todos los contratos deberán contener requisitos específicos de seguridad que aseguren la confidencialidad, integridad y disponibilidad de la información.

Asimismo, se definirán acuerdos de nivel de servicio que establezcan niveles mínimos de calidad, acompañados de medidas para sancionar cualquier incumplimiento. La supervisión continua de los proveedores se realizará para garantizar el cumplimiento de los acuerdos de seguridad establecidos, y cualquier cambio en los servicios ofrecidos será evaluado en función de su criticidad.

Finalmente, al concluir un servicio, se garantizará la devolución y eliminación segura de la información y los activos involucrados. En el caso de los proveedores de servicios en la nube, se establecerán requisitos adicionales de seguridad, que incluirán evaluaciones de riesgo y controles específicos destinados a proteger la información.

En conclusión, las políticas y procedimientos descritos aseguran que la gestión de riesgos y la relación con terceras partes en Grupo SANDO se manejen de manera integral, con el objetivo de minimizar riesgos y asegurar la continuidad y seguridad de la información.

7.4 Cumplimiento, regulación y auditoría

La política de cumplimiento normativo de Grupo SANDO establece un marco riguroso destinado a garantizar el respeto de todas las regulaciones, leyes y requisitos contractuales relacionados con la seguridad de la información. Este compromiso se manifiesta en la obligación del Grupo SANDO de cumplir con todos los estatutos relevantes y leyes aplicables a la seguridad de la información, asegurando que la documentación correspondiente sobre la normativa vigente se mantenga actualizada.

En este sentido, se llevarán a cabo revisiones periódicas de esta normativa, y se establecerán procesos para documentar el ámbito de aplicación y las medidas requeridas. Así, ante la aparición de nuevas regulaciones o modificaciones, se priorizarán las adecuaciones necesarias en función de los plazos establecidos.

En cuanto a los derechos de propiedad intelectual, Grupo SANDO se compromete a incluir en sus contratos cláusulas que garanticen el respeto a dichos derechos, estableciendo procedimientos que abarquen desde la recopilación y tratamiento de información de identificación personal (PII) hasta las medidas de seguridad y eliminación de dicha información.

Los sistemas de información de Grupo SANDO estarán sujetos a revisiones independientes periódicas con el fin de asegurar el cumplimiento de las normativas de seguridad. Estas auditorías serán realizadas por organizaciones externas que se comprometerán a mantener la confidencialidad de los resultados. Los informes generados por estas auditorías identificarán posibles deficiencias y propondrán acciones correctivas pertinentes.

Asimismo, la planificación anticipada de revisiones del cumplimiento normativo es fundamental para minimizar riesgos. Las auditorías se realizarán con un alcance definido, garantizando un acceso restringido a datos y un control riguroso de los procedimientos. La independencia del auditor será esencial en este proceso, y en caso de detectar cualquier incumplimiento, se identificarán las causas, se evaluarán las acciones correctivas necesarias y se verificará su efectividad.

En resumen, estas directrices garantizan que Grupo SANDO mantenga un enfoque proactivo y efectivo en el cumplimiento normativo y la auditoría, lo que fortalece la seguridad de la información en toda la organización.

7.5 Gestión de activos y de información

El Grupo SANDO establece procedimientos rigurosos destinados a garantizar la protección de la propiedad intelectual de sus activos.

En primer lugar, el Grupo se compromete a definir el uso compatible de software y otros activos, asegurando que su adquisición provenga exclusivamente de fuentes confiables. Para este fin, se mantendrán registros adecuados que protejan la propiedad intelectual, garantizando el cumplimiento de las licencias y condiciones de uso establecidas.

Asimismo, la organización se asegurará de que los recursos sean suficientes y se ajusten a la capacidad actual. Esto se logrará mediante la contratación de personal adicional, la adquisición de infraestructura moderna y la optimización de procesos y sistemas existentes.

Todos los activos de información deberán estar debidamente inventariados y clasificados según su criticidad e importancia. Cada activo contará con un identificador único, un responsable asignado y un historial de propiedad. Para ello, se designará a un responsable del inventario que tendrá la tarea de mantenerlo actualizado, con revisiones anuales programadas que aseguren su precisión.

Además, el Grupo SANDO implementará un procedimiento de uso aceptable de la información, que incluirá directrices sobre el acceso y manejo de datos, así como la formación periódica del personal en ciberseguridad. Se prohibirá estrictamente el acceso no autorizado y la manipulación de dispositivos, garantizando que solo los administradores autorizados tengan la capacidad de instalar software en los equipos corporativos.

Finalmente, todos los dispositivos corporativos estarán configurados para asegurar su seguridad a fin de proteger la información sensible almacenada en ellos.

Estos procedimientos son fundamentales para salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información del Grupo SANDO, garantizando así una gestión eficaz de la seguridad a lo largo del ciclo de vida de dichos activos.

7.6 Control de accesos a Sistemas

El Grupo SANDO implementará controles de acceso, tanto lógicos como físicos, definidos por los propietarios de los activos. Estos propietarios serán responsables de conceder los permisos de acceso necesarios, asegurando una adecuada segregación de funciones en los procesos de solicitud, autorización y administración. Se adoptará el principio de mínimo privilegio, limitando el acceso a lo estrictamente necesario, y se mantendrán registros de eventos significativos relacionados con la gestión de identidades. Además, se llevarán a cabo revisiones periódicas de los permisos concedidos y se aplicarán las normativas pertinentes para asegurar su cumplimiento.

El ciclo de vida de las cuentas de usuario será regulado formalmente para garantizar la correcta asignación y revocación de permisos. Cada usuario contará con un identificador único, y los permisos de acceso de aquellos que dejen la entidad serán eliminados de manera oportuna. La provisión de acceso será responsabilidad de los propietarios de los sistemas, quienes llevarán a cabo revisiones periódicas para asegurar que los permisos otorgados sean apropiados.

En lo que respecta al control de acceso a sistemas y aplicaciones, los usuarios solo podrán acceder a aquellos sistemas y aplicaciones que les hayan sido autorizados. Se establecerán requisitos específicos de autenticación y autorización, controlando la información accesible en función del perfil del usuario. Además, se implementarán técnicas de enmascaramiento de datos confidenciales con el objetivo de limitar la exposición de información sensible.

Para garantizar procedimientos seguros de inicio de sesión, el Grupo SANDO adoptará medidas que minimicen los accesos no autorizados, evitando la divulgación de información del sistema durante el proceso de inicio de sesión. Se registrarán tanto los accesos correctos como los fallidos, y se bloquearán las sesiones inactivas, restringiendo además los tiempos de conexión en aplicaciones de alto riesgo.

En conjunto, esta política asegura un enfoque sistemático y riguroso en la gestión de accesos y la protección de la información, cumpliendo con las normativas aplicables y promoviendo una cultura de seguridad en la organización.

7.7 Seguridad física del entorno y Sistemas

El Grupo SANDO establece un perímetro de seguridad claro y robusto en sus instalaciones donde se procesa información. Este perímetro debe ser uniforme y adaptado a los riesgos asociados a los activos. Las áreas destinadas al procesamiento de información estarán debidamente cerradas y equipadas con mecanismos de control de acceso diseñados para prevenir intrusiones. Además, se implementarán sistemas de detección de intrusos y se asegurará la correcta protección de ventanas y puertas, en especial en plantas bajas.

La seguridad física abarca todas las instalaciones de la organización y debe cumplir con las normativas de salud y seguridad pertinentes. Se deberán establecer medidas efectivas para proteger los activos contra cortes de energía y otras interrupciones que puedan comprometer su funcionamiento. Las salas de almacenamiento se mantendrán siempre cerradas y se fomentará una política de "mesas limpias" que evite la exposición de información sensible.

El control de visitas es igualmente crucial, por lo que el acceso a áreas seguras estará restringido y cuidadosamente controlado. Se registrarán las entradas y salidas de los visitantes, quienes recibirán instrucciones sobre seguridad y procedimientos de emergencia. Todo el personal deberá portar su identificación visible en todo momento, y el acceso de personal externo a áreas sensibles requerirá autorización previa y supervisión durante su permanencia.

En lo que respecta a la seguridad en los Centros de Procesamiento de Datos (CPDs), estas instalaciones estarán físicamente aisladas de otras áreas. Se llevará a cabo un registro de control de acceso y se instalarán sistemas destinados a monitorear amenazas ambientales y accesos no autorizados. Asimismo, no se permitirá la introducción de alimentos o bebidas en estas áreas, con el fin de preservar la seguridad de la información.

La seguridad física será diseñada para prevenir daños ocasionados por acciones humanas y desastres naturales. Las áreas seguras no deberán almacenar mercancías, y se implementarán equipos de extinción de incendios adecuados para hacer frente a cualquier eventualidad.

Finalmente, todos los equipos del Grupo SANDO deberán estar protegidos contra robos y daños. Los dispositivos que manejen información sensible contarán con medidas de seguridad adicionales, como mecanismos de autenticación y filtros de confidencialidad. Además, se controlarán las condiciones ambientales para prevenir situaciones adversas que puedan afectar el funcionamiento de dichos dispositivos.

En conjunto, esta política asegura un entorno físico seguro que protege los activos de información del Grupo SANDO frente a amenazas externas, garantizando así la continuidad de sus operaciones.

7.8 Protección de la Información

El Grupo SANDO implementará controles criptográficos con el objetivo de garantizar la confidencialidad, integridad, autenticidad y no repudio de la información sensible, tanto en reposo como en tránsito. La aplicación de la criptografía se llevará a cabo de acuerdo con la clasificación de la información establecida en la normativa interna, asegurando que toda información considerada confidencial esté cifrada. En este contexto, los propietarios de activos serán responsables de la correcta implementación de estos controles.

Asimismo, se establecerá un mecanismo de copia de seguridad para las claves críticas, así como un proceso de recuperación que garantice el acceso a los datos cifrados en caso de pérdida. La transmisión de claves deberá llevarse a cabo de forma segura, manteniendo registros de acceso y autorizaciones que permitan realizar auditorías. No se permitirá la distribución de claves privadas asimétricas, con el fin de evitar compromisos en la seguridad.

La gestión de comunicaciones cifradas será igualmente fundamental. Los datos en reposo deberán ser cifrados adecuadamente, utilizando métodos como el cifrado de disco completo o el cifrado a nivel de archivo. En relación con los datos en tránsito, se implementará cifrado a través de certificados y se seguirán protocolos seguros que garanticen la protección de las credenciales de autenticación.

En conclusión, esta política establece un marco robusto para la protección de la información del Grupo SANDO, asegurando la integridad y seguridad de los datos en todos los niveles de su gestión.

7.9 Protección de Endpoints y Servidores

El Grupo SANDO se compromete a garantizar que todo el personal esté debidamente informado sobre la clasificación de la información manejada en los endpoints. Para ello, se llevará un registro seguro de estos dispositivos, protegiéndolo contra el acceso no autorizado. La instalación de software en los endpoints será restringida, permitiéndose la desactivación o bloqueo remoto de dispositivos cuando sea necesario. El uso de dispositivos extraíbles estará sujeto a control riguroso, y se proporcionará capacitación a los usuarios sobre sus responsabilidades en relación con la seguridad de los

dispositivos finales. Además, se implementará un programa de mantenimiento que será supervisado exclusivamente por personal autorizado.

En lo que respecta a la protección contra software malicioso, el Grupo SANDO establecerá reglas específicas para prevenir el uso de malware en endpoints y servidores. Se reducirán las vulnerabilidades mediante el cumplimiento de normativas de gestión de vulnerabilidades, y se instalará software de detección y reparación de malware, que se mantendrá actualizado en todo momento. Se llevarán a cabo escaneos periódicos en dispositivos y medios de almacenamiento con el fin de detectar posibles amenazas.

El Grupo SANDO también implementará configuraciones de bastionado en todos los endpoints y servidores que contengan datos sensibles. La efectividad de estas configuraciones será supervisada semestralmente, asegurando el cumplimiento de las normas de seguridad. Tanto los sistemas operativos como las aplicaciones serán configurados con ajustes de seguridad recomendados, y se aplicarán parches y actualizaciones críticas de manera regular para salvaguardar la integridad de los sistemas.

Asimismo, se adoptarán medidas de cifrado en los dispositivos para proteger la información almacenada, en cumplimiento con los requisitos establecidos en la normativa vigente. En cuanto a los servidores gestionados por terceros, el Grupo SANDO garantizará que se cumplan los requisitos de gestión de riesgos en la adquisición y uso de información en estos servidores, asegurando la protección adecuada de los datos.

En conclusión, esta política establece un marco integral para la protección de endpoints y servidores, asegurando la confidencialidad y seguridad de la información en todos los niveles de la organización.

7.10 Protección de Redes

El Grupo SANDO se compromete a garantizar que todos los sistemas de comunicaciones estén debidamente actualizados con los parches de seguridad pertinentes, documentando cualquier incompatibilidad que pudiera surgir. La gestión de las configuraciones de los firewalls deberá cumplir con los estándares de seguridad referente a la protección de endpoints y servidores. Cada red contará con una clasificación de información definida, y toda la documentación relacionada deberá mantenerse actualizada. Asimismo, se restringirá el uso de software que tenga la capacidad de eludir los controles de seguridad establecidos.

El Grupo SANDO implementará una arquitectura de red que incluya zonas desmilitarizadas (DMZs) y segmentación de redes con el objetivo de proteger sistemas críticos. Todos los procesos y controles estarán alineados con la criticidad de las aplicaciones y los requisitos de acceso, asegurando así la confidencialidad e integridad de la información en redes públicas, así como la correcta autenticación de los usuarios.

En resumen, esta política establece un marco robusto para la protección de las redes, asegurando la integridad, confidencialidad y disponibilidad de la información en toda la organización.

7.11 Seguridad en el Ciclo de vida de Desarrollo y Aplicaciones

El Grupo SANDO se compromete a asegurar la integración de medidas de seguridad en todas las fases del ciclo de desarrollo de aplicaciones, abarcando desde el diseño hasta el mantenimiento.

En la etapa inicial, se identificarán y evaluarán los riesgos de seguridad, manteniendo una comunicación adecuada para proteger la información involucrada. Se establecerán responsabilidades y requisitos de seguridad específicos en función del tipo de proyecto, y se asegurará que los entornos de desarrollo, prueba y producción se encuentren separados y protegidos conforme al nivel de riesgo.

Para garantizar el cumplimiento de los requisitos de seguridad desde la fase de especificación, se implementará una metodología estructurada en el desarrollo de software. Antes de la producción, se llevarán a cabo pruebas de seguridad que incluirán escaneos de código y pruebas de penetración. El código fuente se almacenará en repositorios seguros, y se adoptarán principios de codificación segura con el fin de prevenir vulnerabilidades que puedan comprometer la seguridad de la información.

El Grupo SANDO documentará formalmente cualquier cambio significativo en los sistemas, evaluando su impacto y comunicándolo a las partes interesadas correspondientes. Se mantendrá un registro de todos los cambios realizados, asegurando que existan mecanismos de reversión que mitiguen posibles efectos adversos en la seguridad de la información.

En lo que respecta a la gestión de datos de prueba, la información utilizada en este contexto deberá ser seleccionada y protegida de manera adecuada. Se prohibirá el uso de datos reales sin anonimizar, garantizando que las medidas de seguridad se apliquen tanto en los entornos de prueba como en los de producción.

Antes de desplegar nuevas aplicaciones que manejen datos confidenciales, se llevarán a cabo pruebas exhaustivas de seguridad. El Grupo SANDO exigirá que los proveedores de aplicaciones realicen pruebas técnicas en entornos de preproducción, estableciendo además procesos de monitorización que cumplan con los requisitos de seguridad pertinentes.

Finalmente, el personal del Departamento de Sistemas recibirá formación en prácticas de desarrollo seguro y en la implementación de medidas de seguridad a lo largo del ciclo de vida de desarrollo de aplicaciones. Esto garantizará la prevención y gestión adecuada de vulnerabilidades que pudieran surgir en dicho proceso.

Esta normativa establece un marco robusto para asegurar la seguridad a lo largo de todo el ciclo de desarrollo de aplicaciones, contribuyendo de esta manera a la integridad y confidencialidad de la información gestionada por el Grupo SANDO.

7.12 Gestión de Vulnerabilidades y Parcheado

La gestión de vulnerabilidades en el Grupo SANDO tiene como propósito identificar de manera centralizada las debilidades que afectan a todos los activos informáticos, así como establecer acciones de mitigación que fortalezcan la seguridad de la organización. Para lograr una gestión efectiva, se asignarán roles claros en la identificación y mitigación de vulnerabilidades en todos los activos que contengan información.

La detección de vulnerabilidades se llevará a cabo a los activos de información identificados en el inventario de activos. Se utilizarán herramientas especializadas para realizar escaneos de vulnerabilidades, los cuales se programarán anualmente, aunque se podrán realizar escaneos adicionales en función de las necesidades detectadas. Las vulnerabilidades identificadas se registrarán y clasificarán según su criticidad, utilizando métricas específicas que permitan priorizar su tratamiento de acuerdo con el nivel de criticidad asignado.

El propietario del activo afectado será responsable de remediar la vulnerabilidad o de delegar dicha tarea, estableciendo tiempos máximos para su resolución. En el caso de que la remediación no sea posible, se implementarán medidas mitigatorias que minimicen el impacto de la vulnerabilidad. Además, será posible aceptar la vulnerabilidad si el riesgo asociado se encuentra por debajo del umbral aceptable definido por el Grupo SANDO.

Una vez implementadas las acciones de remediación, se realizarán escaneos adicionales para verificar la correcta resolución de la vulnerabilidad, completando así la fase de remediación. Se establecerán métricas y controles para monitorear la gestión de vulnerabilidades, lo que permitirá evaluar la eficiencia del proceso y propiciar la mejora continua.

En lo que respecta a la gestión de parches de seguridad, la instalación de parches resulta fundamental para mitigar riesgos. En caso de que no se disponga de parches, se implementarán controles adicionales, tales como la desactivación de servicios vulnerables y la mejora de la supervisión. El Grupo SANDO establecerá un calendario de gestión de parches que detalle las semanas destinadas a la instalación de estos en entornos de prueba y producción, garantizando así un proceso ordenado y controlado.

Esta política garantiza un enfoque estructurado para la identificación y mitigación de vulnerabilidades, así como para la gestión de parches, contribuyendo de manera significativa a la seguridad integral de la información en el Grupo SANDO.

7.13 Monitorización de Sistemas y Gestión de Amenazas e Incidentes

El Grupo SANDO establecerá responsabilidades claras para la planificación y gestión de incidentes de seguridad, con el objetivo de garantizar respuestas rápidas y efectivas ante tales eventos. Para ello, se implementarán tareas de monitorización y respuesta que abarcarán la detección, análisis, contención, erradicación y recuperación de incidentes. Además, se asegurará un registro detallado de todas las actividades realizadas, protegiendo dicha información de accesos no autorizados.

Para la gestión de la monitorización, se implementarán herramientas que proporcionen visibilidad sobre la actividad de los sistemas. Todos los eventos relevantes serán registrados y analizados, y los registros (logs) estarán protegidos contra accesos no autorizados. El Grupo SANDO garantizará que todos los sistemas críticos estén sincronizados con una fuente de tiempo confiable, lo que asegurará la precisión de los registros.

La inteligencia sobre amenazas será un componente fundamental para comprender el panorama de seguridad del Grupo SANDO. Se establecerán objetivos claros y se utilizarán fuentes de información confiables. Se implementarán medidas de seguridad clasificadas en inteligencia estratégica, táctica y operacional, que permitirán una respuesta adecuada ante posibles ataques.

En lo que respecta a la gestión de incidentes de seguridad, el Grupo SANDO definirá un protocolo estructurado que incluirá las fases de preparación, detección, análisis, contención, erradicación, recuperación y evaluación post-incidente. Se identificarán los recursos críticos, y se llevarán a cabo revisiones periódicas de los procedimientos establecidos para mantener su efectividad.

Esta política integral garantizará una gestión eficiente de la monitorización, detección y respuesta ante incidentes de seguridad, fortaleciendo la capacidad del Grupo SANDO para proteger su información y responder adecuadamente a amenazas cibernéticas.

7.14 Auditorías Técnicas

El Grupo SANDO llevará a cabo la planificación de auditorías técnicas con el objetivo de minimizar las interrupciones en los sistemas de información operativos. Esta planificación incluirá la definición del alcance de las pruebas y la identificación de activos, priorizando aquellos catalogados como críticos. El equipo encargado de las auditorías deberá poseer las competencias y el apoyo necesario para realizar las auditorías, las cuales se ejecutarán anualmente siguiendo una metodología interna establecida. Esta metodología abarcará la definición de datos, un calendario detallado de actividades, criterios de evaluación y las acciones que deberán llevarse a cabo.

El Grupo SANDO generará informes de auditoría detallados que incluirán hallazgos y recomendaciones en materia de seguridad. Con base en estos hallazgos, se desarrollarán planes de acción que permitan abordar las cuestiones identificadas, asignando responsabilidades y plazos claros para su remediación. El estado de estos planes de acción deberá ser actualizado regularmente, justificando cualquier modificación en los plazos establecidos.

Este enfoque estructurado para las auditorías técnicas garantiza que el Grupo SANDO mantenga altos estándares de seguridad en sus sistemas de información, identificando y mitigando vulnerabilidades de manera proactiva.

7.15 Gestión de la Continuidad de Negocio

Se debe desarrollar, implementar y mantener un Plan de Continuidad de Negocio (BCP) que asegure la capacidad de respuesta ante incidentes de ciberseguridad y emergencias, así como la recuperación eficaz de las operaciones. Este plan es fundamental para proteger los intereses económicos y la reputación de la organización.

El BCP debe ser revisado anualmente y aprobado por el Comité de Seguridad, asegurando que se contemple la identificación de activos críticos, roles y responsabilidades, y los recursos necesarios para la recuperación de actividades prioritarias. Asimismo, se debe realizar un Análisis de Impacto en el Negocio (BIA) que evalúe los impactos de posibles interrupciones y defina los objetivos de recuperación (RTO, RPO, MTPD y MTO).

El Grupo SANDO debe realizar pruebas anuales del BCP y del BIA mediante simulaciones y ejercicios prácticos, lo que permitirá identificar fallos y garantizar que el personal esté capacitado para cumplir sus funciones en caso de una crisis. Además, se requiere que se establezcan criterios claros para la gestión de incidentes y que se implementen controles de seguridad de la información que respalden la continuidad del negocio.

Por último, es imperativo que el Grupo SANDO garantice que las terceras partes críticas cumplan con los requisitos establecidos en esta normativa, asegurando así una colaboración efectiva en la gestión de la continuidad del negocio.

8. Revisión

La PSI entró en vigor en la fecha de su aprobación por el Consejo de Administración de Grupo Empresarial SANDO, S.A., momento en el cual quedó derogada la versión anterior. Esta continuidad en la revisión y actualización es esencial para asegurar la relevancia y efectividad de las disposiciones establecidas.

El Director de Sistemas de la Información es el encargado de ejercer las facultades de interpretación necesarias para la correcta aplicación de esta PSI. Además, corresponde a este Director coordinar las revisiones pertinentes en función de los cambios organizativos, legales o de negocio que puedan surgir en el transcurso del tiempo. Este enfoque proactivo permite que la Política se mantenga adecuada a las circunstancias y necesidades actuales de la organización.

Grupo SANDO llevará a cabo revisiones periódicas de la PSI para asegurar su cumplimiento y efectividad, las cuales no solo evaluarán la alineación con las directrices internas, sino que también considerarán la evolución de la tecnología, las amenazas emergentes y los requisitos legales que la organización debe cumplir. En este mismo sentido, las modificaciones pertinentes se realizarán conforme sea necesario para abordar cualquier cambio significativo en el entorno operativo o regulatorio. En este contexto, el Comité de Seguridad, designado para tal efecto, revisará dichas modificaciones, garantizando que la PSI se mantenga vigente y eficaz en su propósito de proteger los activos de información de la organización.

Finalmente, la PSI será revisada y aprobada anualmente por el Consejo de Administración, asegurando así un compromiso continuo con la seguridad y la protección de la información dentro del Grupo SANDO. Este proceso formal de revisión es fundamental para la integridad de la gestión de la seguridad de la información y refuerza el compromiso de la organización con la mejora continua en este ámbito crítico.

9. Referencias

Esta Política de Seguridad se ha llevado a cabo teniendo en cuenta los siguientes estándares internacionales y guías de ciberseguridad:

- ISO/IEC 27001:2022

10. Entrada en vigor

La presente Política fue aprobada por el Consejo de Administración de grupo SANDO en su reunión de fecha 29 de noviembre de 2024, entrando en vigor desde el momento de su aprobación.