DocuSign Envelope ID: B5F1BA7B-87C2-4509-B9D3-79AAEC7E9DD1

Política General del Sistema de Gestión de Seguridad de la Información

Fecha de Modificación	Versión Actual	Descripción / Modificaciones
16/05/2019	00	Edición Inicial
06/08/2021	01	Se revisó y se determina que no se realizan cambios durante esta revisión.
11/07/2022	02	Se revisó y se determina que no se realizan cambios durante esta revisión.
24/07/2023	03	Se revisó y se determina que no se realizan cambios durante esta revisión.
02/02/2024	04	Se revisó y se determina que no se realizan cambios durante esta revisión.
14/01/2025	05	Se revisó y se adecuo a la norma ISO/IEC 27001:2022

DocuSigned by: Jorge Temoche DDCC3D6839824B7...	DocuSigned by: JAVIER DRAXL A8A6485F68A94C8...
Revisado:	**Aprobado:**
OFICIAL DE SI	**GERENTE GENERAL**
Fecha: 14/01/2025	**Fecha: 14/01/2025**

DocuSign Envelope ID: B5F1BA7B-87C2-4509-B9D3-79AAEC7E9DD1

INTRODUCCION

BIZLINKS S.A.C., empresa dedicada a brindar servicios PSE y OSE**,** ha decidido implementar un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001 teniendo como alcance "**servicios especializados de facturación electrónica y comprobantes electrónicos PSE y OSE a nivel nacional"** con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información, proteger a ésta de un amplio grupo de vulnerabilidades y amenazas, aplicando una adecuada Gestión de Riesgos, que permita el cumplimiento de los objetivos estratégicos de la Empresa. Esta política tiene como objetivo establecer y adoptar directivas para una adecuada gestión de la Seguridad de la Información en BIZLINKS, debidamente alineada a los estándares y buenas prácticas del sector, permitiendo tomar acción preventiva y proactiva ante potenciales eventos que impacten en la Empresa. La presente política es aplicable a todo el personal, colaboradores de la Empresa y partes interesadas.

Por lo tanto, BIZLINKS mediante su Sistema de Gestión de Seguridad de la Información, considera las siguientes directivas:

- Desarrollar productos y servicios conformes con los requisitos legislativos y aplicables, identificando para ello las legislaciones de aplicación a las líneas de negocio desarrolladas por la organización e incluidas en el alcance del Sistema de Gestión de la Seguridad de la Información.
- Establecimiento y cumplimiento de los requisitos contractuales con las partes interesadas.
- Definir los requisitos de formación en seguridad y proporcionar la formación necesaria en dicha materia a las partes interesadas, mediante el establecimiento de planes de formación.
- Prevención y detección de virus y otro software malicioso, mediante el desarrollo de políticas específicas y el establecimiento de acuerdos contractuales con organizaciones especializadas.
- Gestión de la continuidad del negocio, mediante planes de continuidad conformes a metodologías de reconocido prestigio internacional.
- Establecimiento de las consecuencias de las violaciones de la política de seguridad, las cuales serán reflejadas en los contratos firmados con las partes interesadas, proveedores y subcontratistas.
- Actuar en todo momento dentro de la más estricta ética profesional.
- Impulsar la mejora continua para aumentar la eficacia del sistema de gestión de seguridad de la información.

Esta política es aplicable a todo el personal y colaboradores de BIZLINKS, y está alineada con los estándares y buenas prácticas del sector. A través de este enfoque preventivo y proactivo, buscamos proteger nuestros activos de información y garantizar la confianza de nuestros clientes y socios comerciales.

DocuSign Envelope ID: B5F1BA7B-87C2-4509-B9D3-79AAEC7E9DD1

1. GENERALIDADES

1.1. Objetivos

1.1.1. Crear un marco referencial para gestionar de manera apropiada la seguridad de la información de BIZLINKS.

1.1.2. Establecer las expectativas de la Alta Dirección con respecto al uso que los colaboradores deben hacer de los activos de información de BIZLINKS, así como de las medidas que se deben adoptar para la protección de estos recursos.

1.1.3. Concientizar a todos los colaboradores de BIZLINKS sobre la importancia y la comprensión de sus responsabilidades individuales sobre seguridad de la información.

1.1.4. Especificar las medidas de seguridad de la información que el BIZLINKS debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información, las cuales podrían ocasionar alguna de las siguientes consecuencias:

- Pérdida o mal uso de los activos de información.
- Pérdida de imagen de BIZLINKS frente a sus clientes y terceros.
- Incumplimiento de las normas legales que debe cumplir BIZLINKS.
- Proporcionar a todos los colaboradores de BIZLINKS los lineamientos que faciliten una adecuada toma de decisiones en aspectos relacionados a la seguridad de la información.

2. NORMAS ANULADAS

- **Política de Seguridad Corporativa**

3. BASE LEGAL Y NORMATIVA

- Reglamento de comprobantes de Pago (Resolución de Superintendencia N° 007-99/SUNAT)
- Resoluciones de Superintendencia de SUNAT para facturación electrónica siendo las Regulaciones para PSE (Proveedor de Servicios Electrónicos) y OSE (Operador de Servicios Electrónicos).
- Ley N° 29733 – Ley Protección de Datos Personales.
- Decreto Supremo N° 003-2022-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales.
- ISO/IEC 27001:2022, Sistemas de Gestión de la Seguridad de la Información (SGSI)
- ISO/IEC 27002:2022, Código de prácticas para los controles de seguridad de la información.

DocuSign Envelope ID: B5F1BA7B-87C2-4509-B9D3-79AAEC7E9DD1

4. NIVEL DE APROBACIÓN

Este documento ha sido suscrito en señal de conformidad por el Gerente General, Gerente de Tecnología de la Información, Responsable de Administración y Finanzas y el Oficial de Seguridad de la Información, habiéndose aprobado el 14 de enero de 2025

5. ALCANCE

Lo dispuesto se aplica al contexto de la organización y las necesidades de las partes interesadas pertinentes como todo el personal que labora en BIZLINKS, así como a terceros que, previo contrato de confidencialidad, tengan acceso a la información de la organización para el cumplimiento del servicio contratado.

6. RESPONSABILIDADES

De la Oficialía de Seguridad de la Información

- Asegurar que la Política General de Seguridad de la Información y los Objetivos del SGSI, se establezcan considerando los requisitos de la norma ISO/IEC 27001:2022 sean compatibles con la planificación estratégica de BIZLINKS.

De la Gerencia de Tecnología de la Información

- La Gerencia de Tecnología, trabajar en conjunto con la Oficialía de Seguridad de la Información, la aplicación de controles de Seguridad y Protección a los activos informáticos.

Del Departamento de Talento Humano

- Apoyar en la difusión de la Política General de Seguridad de la Información a todos los colaboradores de BIZLINKS.
- Al plan de capacitación de seguridad de la información, incluirlo dentro del plan general.

7. REFERENCIAS

- Metodología de Gestión de Riesgos de Seguridad de la Información
- Política de Uso Aceptable de Activos
- Política de uso dispositivos móviles

8. GLOSARIO DE TÉRMINOS

- **SGSI (Sistema de Gestión de Seguridad de la Información):** Conjunto de políticas, procedimientos, directrices y recursos asociados, implementado para proteger los activos de información.

- **Política de Seguridad de la Información:** Directriz aprobada por la alta dirección que define el enfoque y compromiso de la organización respecto a la seguridad de la información.

- **Propietario del Activo de Información:** funcionario responsable de la integridad, confidencialidad y disponibilidad de cierta información. Tiene autoridad para especificar, exigir las medidas de seguridad y otorgar niveles de accesos a los activos de información de su responsabilidad.

DocuSign Envelope ID: B5F1BA7B-87C2-4509-B9D3-79AAEC7E9DD1

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

- **Directorio:** Persona o grupo de personas que dirige y controla una organización al más alto nivel. El Directorio (o alta gerencia) tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización. Si el alcance del sistema de gestión cubre solo una parte de una organización.

- **Análisis de Riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [Fuente: Guía ISO 73: 2009] El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.

9. POLÍTICA

Adhesión a la Política

- La presente política, los procedimientos y los estándares que tenga asociados, deben ser cumplidos por todos los colaboradores, proveedores de servicios y terceros sin excepción.
- La Oficialía de Seguridad de la Información debe monitorear el cumplimiento de las políticas, procedimientos y estándares del Sistema de Gestión de Seguridad de la Información a través de los procedimientos de revisión establecidos y el Oficial de Seguridad de la Información debe reportar los resultados al Directorio de BIZLINKS.
- La presente Política debe ser revisada al menos una vez cada doce meses y actualizada según sea necesario para reflejar los cambios en los objetivos de BIZLINKS o los posibles riesgos.

Protección de la Información

- El Directorio y las Gerencias reconocen que la seguridad de la información es importante para BIZLINKS y su protección debe ser impulsada y apoyada por todos los miembros de BIZLINKS.
- La información es un activo valioso que debe ser protegido de manera consistente con los requerimientos legales, normativos y contractuales que sean aplicables en BIZLINKS.
- Toda información generada por los colaboradores o proporcionada por BIZLINKS para el desempeño de sus labores es de propiedad de BIZLINKS, durante y luego de la finalización de la relación laboral, esto incluye información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos.
- Se debe tener presente que no es posible eliminar el riesgo, sólo mitigarlo, por lo tanto, los controles que se definan para proteger los activos de información deben ser determinados en base a un análisis de riesgo a los activos de información, el cual debe ser realizado periódicamente.

Compromiso de la alta Dirección

- Proteger los activos de información frente a amenazas internas o externas, deliberadas o accidentales.
- Cumplir con los requisitos legales, reglamentarios y contractuales aplicables en materia de seguridad de la información.
- Integrar el SGSI en los procesos estratégicos y operativos de la organización.

DocuSign Envelope ID: B5F1BA7B-87C2-4509-B9D3-79AAEC7E9DD1

- Proporcionar los recursos necesarios para establecer, implementar, mantener, asegurando la mejora continua de la eficacia del SGSI.
- Garantizar que la política y los objetivos del SGSI sean compatibles con la dirección estratégica y el contexto de la organización.
- Alinear la seguridad de la información con las necesidades y expectativas de las partes interesadas pertinentes.
- La alta Dirección de BIZLINKS debe destinar los recursos necesarios para asegurar que todos los colaboradores reciban concientización permanente en seguridad de la información, de acuerdo a su función y rol.
- Abordar los riesgos y oportunidades que puedan afectar la seguridad de la información y los resultados del sistema.
- Para aquellos riesgos que no sean aceptables, deberán seleccionarse medidas de mitigación apropiadas, las cuales serán sometidas a la aprobación de la Gerencia General de ser el caso, para asegurar que:
    - Son suficientes para llevar el riesgo a un nivel apropiado.
    - Reciben los recursos y el apoyo necesarios para su implementación.

9.4. Análisis de Riesgos

- El Análisis de Riesgo comprende la identificación de los riesgos a los cuales están expuestos los activos de información de las Gerencias mediante la identificación de las vulnerabilidades y las amenazas que las pueden explotar, la probabilidad de ocurrencia y el impacto potencial sobre los procesos operativos de las Gerencias y Unidades de negocio.
- El análisis de riesgo de BIZLINKS se realizará usando la Metodología de Gestión de Riesgos de Seguridad de la Información, el cual forma parte del Sistema de Gestión de Seguridad de la Información de BIZLINKS.

9.5. Gestión de Riesgos

- La Gestión del Riesgo comprende establecer la estrategia a fin de eliminar, reducir, mitigar, transferir el riesgo e identificando oportunidades estableciendo, según sea el caso, planes de mejora que comprenden políticas, procedimientos y controles en función al riesgo asociado y al activo(s) de información que ha sido evaluado.
- Estos planes de mejora deben tener un enfoque integrador de aspectos relacionados con el personal, los procesos y la tecnología, logrando reducir el riesgo e implementar las mejores prácticas, lo cual permite fortalecer el nivel de protección de la información.

9.6. Clasificación de La Información

- Los Propietarios de Información y/o Custodios de Información clasifican la información que esté bajo su responsabilidad en “Restringida”, “Confidencial”, “Uso Interno” o “General o de Uso Público “de acuerdo con su importancia para el BIZLINKS.

9.7. Uso de Activos de Información

- Todo uso de los activos de información debe ser para propósitos de las operaciones de BIZLINKS de acuerdo con las políticas, estándares, procedimientos y manuales que definan.

DocuSign Envelope ID: B5F1BA7B-87C2-4509-B9D3-79AAEC7E9DD1

9.8. Cumplimiento

- BIZLINKS debe cumplir las disposiciones relacionadas a Seguridad de Información que emitan los Órganos Reguladores, así como sus Políticas Organizacionales.

9.9. Concientización

- EL departamento de Administración y Finanzas, a través del Plan de Capacitación se asegura que los colaboradores son conscientes de:
    - La importancia de la Política General de Seguridad de la Información y sus implicancias.
    - Su contribución a la eficacia del Sistema de Gestión de Seguridad de la Información, incluidos los beneficios de su mejora.
    - Las consecuencias de no cumplir con los requisitos del Sistema de Gestión de Seguridad de la Información, según lo establecido en el Reglamento Interno de Trabajo