Digital Bank
Servicios Transaccionales

Serviex.com

# Política de Seguridad
# De la información

Versión 10

# Tabla de Contenido


**1.** Información del Documento..... **2**
**2.** Objetivos Generales de la seguridad de la información..... **3**
**3.** Alcance..... **4**
**4.** Referencia Normativa..... **4**
**5.** Responsables..... **4**
**6.** Descripción de la Política..... **5**
**6.1** Distribución y Capacitación..... **5**
**6.2** Actualización del Marco Normativo..... **5**
**6.3** Estructura de la Política de Seguridad de la Información..... **6**
**6.4** Propiedades de seguridad de la información de los activos..... **6**
**6.5** Faltas a la Política de Seguridad de la Información..... **7**

# 1. Información del Documento

| |
|---|
| **Nombre del Documento:** PSI - Política de Seguridad de la Información |
| **Creado por:** Auditoría Interna |
| **Responsable del Documento:** Gerencia de Ciberseguridad & Compliance |
| **Aprobado por:** Alta Dirección |
| **Fecha de Aprobación:** Septiembre 2023 |

## CONTROL DE VERSIONES

| Versión | Fecha de Vigencia | Responsable | Comentario |
|---|---|---|---|
| 8 | 02-2022 | Ciberseguridad & Compliance | Revisión anual |
| 9 | 09-2022 | Ciberseguridad & Compliance | Cambios de formato e inclusión de la Continuidad operativa. |
| 10 | 09-2023 | Ciberseguridad & Compliance | Revisión de manera anual.<br>Sin modificaciones. |
| | | | |
| | | | |

(*) La presente versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

# 2.- Objetivos Generales de la seguridad de la información

El presente documento tiene por propósito, definir la Política de Seguridad de la Información de **Serviex S.A (Digital Bank Servicios Transaccionales)**, la cual plantea el cumplimiento de los siguientes objetivos estratégicos de seguridad de la información y ciberseguridad:

1. Asegurar la Confidencialidad, Integridad y Disponibilidad de la Información a través procesos que se realizan, al interior y durante el intercambio de información tomando como base el framework normativo de la ISO 27001 como estándar base y la norma PCI-DSS.

2. Mejorar la metodología para control de acceso a los activos declarado como críticos y de la información que contenga (IIP) clasificada como privada, de usuarios y empresas, en el proceso de almacenamiento en servidores, directorios compartidos, áreas comunes o web services.

3. Cumplimiento de los requisitos legales, reglamentarios y las obligaciones contractuales, con clientes y proveedores de seguridad de la información de la actividad empresarial.

4. Gestión de Oportunidades y Acciones de mejora, el cual crea un compromiso dentro de la Organización para la mejora continua del Sistema de Gestión de Seguridad de la Información y así resguardar nuestros activos en cuanto sus propiedades definidas dentro del Sistema de acuerdo a la criticidad con la que se clasifican dentro de nuestros procesos que se amparan bajo el alcance.

5. Establecimiento y mantenimiento de una estrategia de gestión de riesgos como base de análisis para la creación, mantenimiento y mejora continua del SGSI.

6. Desarrollo e implementación de una serie de controles y su revisión para hacer frente a los posibles eventos o incidencias que puedan afectar a la seguridad de la información.

7. Mantenimiento de competitividad, rentabilidad e imagen social.

8. Establecer Planes de Continuidad de Negocio basado en la evaluación de impactos y amenazas sobre la base del marco del alcance, que genere análisis de contexto, acciones de mejora a los procesos de negocio, apuntando a la mejora continua del SGSI.

9. Asegurar la privacidad y protección de la IIP (información identificada personal), como se exige en la legislación y regulaciones relacionadas. Desarrollando e implementando la Política que indica cómo la organización se preocupa de la privacidad y protección de la IIP. Debiendo esta ser comunicada a todas las personas involucradas en su procesamiento.

# 3.- Alcance

**Serviex S.A (Digital Bank Servicios Transaccionales)**como Organización dedicada la entrega de servicios ha implementado un Sistema de Gestión de Seguridad de Información que afecta a todo el Personal de la Empresa que participa en el desarrollo de su actividad principal que es:

**"Los sistemas de información que soportan los procesos de Desarrollo y Operatividad de Portales Transaccionales de acuerdo con la declaración de aplicabilidad vigente de la Norma ISO 27.001" y "Administración de mandatos PAC, PAT y PAN" para la certificación "PCI-DSS"**

# 4.- Referencia Normativa

Norma ISO/IEC 27001:2017 ." Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos".
**Requisito normativo: 5.2 Política.**

**PCI DSS** Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) o PCI-DSS desarrollado por el comité denominado PCI-SSC (Payment Card Industry Security Standards Council) como una guía para las organizaciones que procesan, almacenan y/o transmiten datos de tarjeta habientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago débito y crédito.
**Requisito PCI: Req. 12**

# 5.- Responsabilidades

Todos los empleados, empresas que coexisten en el ecosistema digital y proveedores críticos de **Serviex S.A (Digital Bank Servicios Transaccionales)** son responsables del cumplimiento de estas políticas. Como así mismo deben saber que se podrá supervisar violaciones a las políticas mediante controles automáticos registrados en logs, o cualquier otro medio disponible para dichos efectos, en base a los cuales se pueden tomar medidas disciplinarias. Las Jefaturas son responsables de asegurar que sus empleados o proveedores críticos que trabajan en su área cumplan con estas políticas.

Adicionalmente **Serviex S.A (Digital Bank Servicios Transaccionales)** cuenta con una estructura organizacional que soporta la seguridad al interior de la organización, consistente en un "Área de Ciberseguridad & Compliance" y Comité de Seguridad, estos roles, sus responsabilidades y autoridades quedan definidas en el PR-SI-17 Asignación de Roles y Responsabilidades y el MSI_Manual de Seguridad de la Información.

# 6.- Descripción de la Política

## 6.1.- Distribución y Capacitación

Las políticas serán aprobadas por la Alta dirección y divulgadas por la Gerencia de Ciberseguridad & Compliance. La difusión de estas será responsabilidad del Sistema de Gestión de Seguridad de la Información y todas las Jefaturas de la organización.

El presente documento y los documentos asociados están a disposición de los colaboradores y proveedores críticos a través de los medios de comunicación establecidos en el Plan de Comunicación que se encuentra en el MSI-Manual de Seguridad de la información en el apartado 7.4.Comunicaciones, vía correo electrónico, y divulgada en la Página web de la organización paraconocimiento de las Partes Interesadas.

Todos los empleados internos y cuando sea relevante los externos, al momento de ingresar a la organización y de acuerdo a lo programado en el Plan de Capacitación y Conciencia anual, deberán recibir una capacitación adecuada a las funciones que tengan asignadas, la que debe incluir requisitos de seguridad, responsabilidades legales y controles del negocio, implicancias de no cumplimiento y ventajas de Sistema de Gestión de Seguridad de la Información, como también entrenamiento en el uso correcto de aplicaciones para el procesamiento de la información.

Esta capacitación debe ser actualizada regularmente.

El responsable de verificar que los empleados han sido capacitados en forma adecuada y que se han efectuado las actualizaciones correspondientes, es el Área de Gestión de Personas.

## 6.2.- Actualización del Marco Normativo

El documento de Política de Seguridad de la Información y sus documentos complementarios deben ser revisados y actualizados periódicamente (a lo menos 1 vez al año) o cuando ocurra un cambio significativo dentro de la Organización.

La Gerencia de Ciberseguridad & Compliance es responsable de la actualización de la gestión documental, políticas, procedimientos y estándares. El proceso de mantención deberá asegurar que la revisión se efectúe acorde a cambios en el perfil de riesgo original, incidentes de seguridad significativa, nuevas vulnerabilidades o cambios en la infraestructura organizacional o técnica.

Las consideraciones de que medir son:

• Efectividad de las políticas, procedimientos, instructivos y planes, demostrada por la naturaleza, número e impacto de los incidentes de seguridad registrados.

• El costo e impacto de los controles en la eficiencia de la empresa.

• Efectos de los cambios de tecnología en la plataforma de la empresa.

Cualquier modificación efectuada al marco normativo, Políticas de Seguridad de **Serviex S.A (Digital Bank Servicios Transaccionales)**, deberá mantener el formato de los documentos generados y la correcta administración de sus versiones.

## 6.3.- Estructura de la Política de Seguridad de la Información

La documentación de la Política de Seguridad de la Información de **Serviex S.A (Digital Bank Servicios Transaccionales)**, contempla los siguientes documentos:

• Políticas Generales de Seguridad de la Información, considera Políticas de Seguridad en las cuales se definen las normas correspondientes a cada una de ellas para cumplimiento de controles específicos del Anexo A.

• Procedimientos, son los documentos que se desprenden de cada una de las políticas y que contienen la estructura o paso a paso de las gestiones a realizar para cumplirlos controles del Anexo A de la Norma.

• Instructivos y Planes, acuerdos documentados que contienen especificaciones técnicas o criterios precisos que son utilizados consistentemente, como reglas, guías o definiciones.

## 6.4.- Propiedades de seguridad de la información de los activos

Será responsabilidad del Área de Ciberseguridad & Compliance y el Comité de Seguridad de la Información velar por el cumplimiento - por parte de todo el personal empleado temporal o permanentemente, proveedores críticos y no críticos de **Serviex S.A (Digital Bank Servicios Transaccionales)**, - en cuanto a:

**Integridad**
Garantizar la implementación de procesos y controles para el manejo correcto de la información, resguardando que ésta se encuentre libre de errores y/o irregularidades de cualquier índole y quecorresponda a la realidad.

**Confidencialidad**
Garantizar la implementación de procesos y controles para que toda la información y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran perjudicarla.

**Disponibilidad**
Garantizar la implementación de procesos y controles para la restricción de acceso a la información, toda vez que lo requieran de acuerdo a la clasificación de la misma; para lo cuál se debe garantizar que la información y la capacidad de procesamiento, sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatoria o dañe las instalaciones, medios de almacenamiento y/o equipamiento de procesamiento.

**Privacidad**
Garantizar que la información, cuando sea identificada como personal (IIP), será tratada con los estándares necesarios para su protección y se alineen estos al marco legal y regulatorio de acuerdocon las leyes nacionales e internacionales donde se esté almacenando y transmitiendo dicha información.

**Sistema de Gestión de Seguridad de la Información**
**Serviex S.A (Digital Bank Servicios Transaccionales)**, cuenta con un SGSI que asegura, basándonos en el enfoque de procesos, que los dueños de estos procesos promoverán, de manera natural y abordando la mejora continua del sistema. Las políticas de seguridad de la información son una herramienta que ayudarán a documentar, estructurar, guiar y garantizar el correcto funcionamiento del SGSI

## **6.5.-** Faltas a la Política de Seguridad de la Información

La Seguridad de la información, en todos sus ámbitos, debe ser considerada como un ítem dentro de la evaluación de desempeño del personal, así será posible incentivar, a través de este medio, el cumplimiento del marco normativo.

El incumplimiento de las obligaciones y prohibiciones mencionadas en este documento y otros documentos complementarios otorga el derecho a la institución para aplicar medidas disciplinarias al infractor, las que podrán ir desde amonestaciones verbales, escritas hasta llegar a la desvinculación, dependiendo de la gravedad del incumplimiento, esto según la PPD Política de Procesos Disciplinarios.

Será responsabilidad del trabajador que detecte un incumplimiento de las obligaciones o prohibiciones indicadas en este documento, darlo a conocer en forma inmediata a su j efaturadirecta, de manera que se gestione un Incidente de Seguridad de acuerdo con el **PR-SI-07 Gestión de Incidentes de Seguridad.**
Es fundamental realizar, a lo largo del tiempo, un seguimiento y control de las medidas implementadas, estableciendo incentivos y sanciones al personal, según corresponda.

**Rodrigo Heredia**
Director
**Digital Bank Servicios Transaccionales**

Digital Bank
Servicios Transaccionales

Serviex.com