Digital Bank
Servicios Transaccionales

Política de Privacidad Protección y Transferencia de Datos

Versión 0

Tabla de Contenido

1. Información del Documento

Nombre del Documento: Política de Privacidad, Protección y Transferencia de Datos
Creado por: Auditoría Interna
Responsable del Documento: Gerencia de Ciberseguridad & Compliance
Aprobado por: Alta Dirección
Fecha de Aprobación: Septiembre 2022

CONTROL DE VERSIONES

Versión	Fecha de Vigencia	Responsable	Comentario
0	09-2022	Ciberseguridad & Compliance	Primera Versión Oficial

(*) 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

La presente política tiene por propósito definir las normas que regirán la privacidad y protección de los datos cuando se identifique IIP (información identificada personal) en los procesos definidos dentro del alcance del SGSI, partiendo de las premisas de evitar su pérdida, divulgación, y manteniendo su confiabilidad y su disponibilidad. Aunque los datos en general pertenecen a los clientes, el uso por parte de **Digital Bank Servicios Transaccionales** debe asegurar a los clientes que su información es tratada con la máxima privacidad y confidencialidad y para el uso exclusivo para lo que fue designada al momento de participar en los procesos antes mencionados.

3. Alcance

La presente Política norma el uso de la información al interior de **Digital Bank Servicios Transaccionales**, considerando tanto la información impresa como la almacenada en medios digitales, incluidos datos sobre:

- Colaboradores actuales, pasados y potenciales.
- Contratistas.
- Clientes.
- Otras partes interesadas.

4. Referencia Normativa

Norma ISO/IEC 27001.” Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos”

Controles Anexo A:

- A.5 Políticas de seguridad de la información.
- A.6 Organización de la seguridad de la información.
- A.7 Seguridad ligada a los recursos humanos.
- A.8 Administración de activos.
- A.9 Control de acceso.
- A.10 Criptografía.
- A.11 Seguridad física y del ambiente.
- A.12 Seguridad de las operaciones.
- A.13 Seguridad de las comunicaciones.
- A.14 Adquisición, desarrollo y mantenimiento del sistema
- A.15 Gestión de los Proveedores.

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 elcomité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía para las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago débito y crédito.

5. Responsables

Rol	Responsabilidad
Gerencia de Ciberseguridad & Compliance	Es el responsable de mantener debidamente actualizada esta Política de Privacidad, Protección y Transferencia de Datos.
Gerente Infraestructura	Administración total de la Infraestructura de Servidores, de Data Center, y de los sistemas de apoyo (EAA, Cámaras de TV, etc.). Es el responsable de contratar los servicios de destrucción de información crítica impresa.

6. Descripción de la Política

6.1 Protección de Datos personales

Digital Bank Servicios Transaccionales Indica que al identificarse IIP (información identificada personal) en el proceso del Servicio dentro del alcance del SGSI se debe seguir los siguientes lineamientos:

01: El uso de Medios de Almacenamiento Extraíbles está prohibido, para ello todas las estaciones de trabajo tendrán bloqueados los puertos USB, como así mismo los grabadores de CD-ROM y/o DVD. Las excepciones deben ser solicitadas por la Gerencia de Ciberseguridad & Compliance, la cual evaluará los antecedentes para la aprobación o indicará el medio en el que se disponibilizará la información requerida para mantener resguardada su privacidad y confidencialidad.

02: Las transferencias de archivos hacia y desde **Digital Bank Servicios Transaccionales** hacia otras compañías, deberán ser autorizadas explícitamente por el Gerente de Ciberseguridad & Compliance a través de la generación de un ticket, donde se deben incorporar las justificaciones, destinos y fines para la transferencia de esta información, este requerimiento será evaluado por el CSI y la Gerencia de Ciberseguridad & Compliance y de acuerdo al fin y uso que se les dará a la información se otorgará el permiso para la transferencia de la manera que el área considere más segura.

03: Las transferencias de archivos con otras instituciones será encriptada (SFTP Seguro) y se pueden realizar solamente desde estaciones de trabajo o servidores previamente autorizados.

04: Se habilitará un servicio de Alta Disponibilidad para Bases de Datos y Repositorios Operacionales.

05: Todo documento impreso, calificado como crítico, deberá ser eliminado en el recinto donde éste se genera, mediante uso de picadoras de papel exclusivas para el servicio.

06: Cuando se den de baja Servidores, PC´s o Notebooks, donde se tenga conocimiento de haber procesado IIP, esta información será dada de baja de acuerdo con lo establecido en el procedimiento de borrado seguro PR-SI-01. ADMINISTRACIÓN DE ACTIVOS y el PR-SI-19 ALMACENAMIENTO, MANEJO, ELIMINACIÓN Y DESTRUCCIÓN MEDIOS DATO PAN.

07: Toda la información que administra **Digital Bank Servicios Transaccionales** será considerada confidencial, por lo tanto, no puede ser divulgada fuera de sus ambientes e instalaciones.

09: Los Gerentes y Subgerentes de Áreas serán responsables de clasificar la información usada en su ámbito de trabajo, en cuanto a su criticidad (Información Crítica y No Crítica) y privacidad (que contenga o no IIP)y comunicar esto a la Gerencia de Ciberseguridad & Compliance para que se incluya en los procesos de respaldos y se le entregue el tratamiento de acuerdo a lo establecido en el PR-SI-01. ADMINISTRACIÓN DE ACTIVOS

10: La información que contenga IIP o dato de tarjeta PAN estarán disponibles solo en las áreas determinadas para estos fines, se enviarán a los clientes vía SFTP (FTP Seguro), y luego serán eliminadas de acuerdo con lo instruido en el punto 06.

11: Los datos cuando se identifique IIP (información identificada personal) serán resguardados en sistema de almacenamiento controlado por Gestión de Personas, y dispuesto a conocimiento solo a solicitud por escrito y en casos justificados, como, por ejemplo, la necesidad de acreditación del personal ante un cliente por materias de salud laboral, o información relevante para procesos con autoridades, como por ejemplo ante un comparendo ante la inspección del trabajo.

12: Toda transmisión y Protección de los datos se mantendrá asegurados bajo una estrategia de gestión de riesgos como base para esto, considerando los medios necesarios para establecer los controles de Ciberseguridad suficiente de acuerdo con nuestro modelo de negocio.

13: Además de los escenarios donde se identifique el IIP, cuando sea exigido por el cliente y los datos deban contar con total confidencialidad, se aplicará encriptación de la información de acuerdo con lo establecido en la PCC, Política de controles Criptográficos.

14: Se administrarán los Activos de Información realizando un inventario de esto y clasificando la información que estos almacenan según el Procedimiento de Administración de Activos.

15: El Tiempo de Retención de la Información será a lo más de 3 años por política interna, o de acuerdo con lo establecido por requisito contractual según lo que el cliente requiera y especifique en contrato de servicio. Una vez cumplido este plazo, se eliminará a través de lo especificado en el Procedimiento de Administración de Activos.

16: Todos los requerimientos legales de los cuales la organización debe considerar para él tratamiento de los datos, será Identificado y evaluado en el PR-06 Procedimiento de Identificación y Evaluación de requerimientos legales.

6.2 Utilización de los datos personales.

Tal como lo dicta la ley, los datos personales podrán ser tratados solo cuando la ley y otras disposiciones legales lo autorice, o en cuando el titular lo consienta expresamente.
Los titulares deben ser informados debidamente del propósito del almacenamiento de sus datos personales y si posibles comunicaciones para los procesos operacionales y comerciales de **Digital Bank Servicios Transaccionales**

Las autorizaciones deben ser por escrito, y pueden ser revocadas por el titular de forma retroactiva mediante un aviso escrito al área de Gestión de Personas.

Los siguientes datos personales no requieren autorización en el tratamiento de datos:

- Que provengan de fuentes de datos accesibles al público,
- Sean de carácter económico,
- Sean de carácter financiero, bancario o comercial
- Profesión o actividad,
- Títulos educativos,
- Dirección o fecha de nacimiento
- Sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Digital Bank Servicios Transaccionales debe asegurarse de que cumple con todo lo indicado por ley tanto en el tratamiento que realiza actualmente como en el marco de la introducción de nuevos métodos de tratamiento como los nuevos sistemas informáticos. El funcionamiento de un sistema de gestión de la seguridad de la información (SGSI) que se ajusta a la norma internacional ISO / IEC 27001:2017 es una parte clave de ese compromiso.

6.3 Derechos de la persona

Digital Bank Servicios Transaccionales fomenta los derechos de las personas respecto a sus datos. Estos consisten en:

- El derecho a ser informado.
- El derecho de acceso.
- El derecho de rectificación.
- El derecho de supresión.
- El derecho a restringir el procesamiento.
- El derecho a oponerse.
- Derechos en relación con la toma de decisiones automatizada y la elaboración de perfiles.

6.4 Consentimiento del Interesado

A menos que sea necesario por un motivo permitido, se debe obtener el consentimiento explícito de un interesado para recopilar y procesar sus datos. Será el área de Gestión de Personas quien debe mantener en los expedientes de los trabajadores dichos consentimientos, los que deberán ser actualizados al menos cada 24 meses.

6.5 Privacidad por diseño

Los datos serán resguardados en sistema de almacenamiento controlado por Gestión de Personas, y dispuesto a conocimiento solo a solicitud por escrito y en casos justificados, como por ejemplo, la necesidad de acreditación del personal ante un cliente por materias de salud laboral, o información relevante para procesos con autoridades, como por ejemplo ante un comparendo ante la inspección del trabajo.

Rodrigo Heredia
Dirección
Digital Bank Servicios Transaccionales

Digital Bank
Servicios Transaccionales

Política de Privacidad, Protección y Transferencia de Datos
Septiembre 2022 Versión 0
Información Pública