Manual de Procedimientos

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

HOMBRE-APY-177

Fecha: 20/05/2025
Versión: 2.5

Uso interno

Contenido

MANUAL DE SEGURIDAD DE LA INFORMACIÓN
HOMBRE-APY-342

1. OBJETIVO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Esta Política de Seguridad de la Información y Ciberseguridad es una declaración de las responsabilidades y conductas aceptadas para mantener un entorno seguro en Banco de Occidente. Esta Política establece los lineamientos y lineamientos relacionados con el manejo seguro de la información.

1.1.1. Principios

Con el fin de cumplir con sus objetivos de negocio, Banco de Occidente ha establecido los siguientes principios que sustentan la Política de Seguridad de la Información y Ciberseguridad como fundamentales:

- La información es uno de los activos más importantes del Banco de Occidente y, por lo tanto, se espera que sea utilizada de acuerdo con los requerimientos del negocio.
- Se debe mantener la confidencialidad de la información empresarial y de terceros, independientemente del medio o formato en el que se encuentre.
- La información empresarial debe preservar su integridad independientemente de su residencia temporal o permanente, o de la forma en que se transmita.
- La información comercial debe estar disponible cuando se solicite.
- Se debe preservar la privacidad de la información del Banco de Occidente.

1.1.2. Objetivo General

El objetivo principal de la Política de Seguridad de la Información y Ciberseguridad es que el Banco de Occidente asegure que su información sea accedida únicamente por aquellos que tengan una necesidad legítima para el desempeño de sus funciones comerciales (Confidencialidad); que está protegido contra modificaciones no planificadas, realizadas intencionalmente o no intencionalmente (Integridad); que esté disponible cuando se requiera (Disponibilidad); y que se utilice para los fines para los que se obtuvo (Privacidad).

1.1.3. Objetivos Específicos

- Los objetivos específicos que persigue la Política de Seguridad de la Información y Ciberseguridad son:
- Establecer las bases para el desarrollo e implementación del Modelo de Seguridad de la Información.
- Definir la conducta a seguir en relación con el acceso, uso, gestión y administración de los recursos de información.
- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas de negocio.
- Gestionar los riesgos en Seguridad de la Información y Ciberseguridad.

- Establecer canales de comunicación que permitan a la Alta Dirección mantenerse informada de los riesgos y uso inadecuado de los activos de información, y de las acciones emprendidas para su mitigación y corrección, generando cultura y compromiso en todos los niveles.

- Sensibilizar a la Comunidad sobre los riesgos de ciberseguridad y asegurar que disponen de los conocimientos, habilidades y medios tecnológicos necesarios para mantener los objetivos de la Seguridad de la Información.

- Proteger la imagen, los intereses y el buen nombre del Banco de Occidente.

Este documento proporciona los estándares para respaldar las Políticas de Seguridad de la Información y Ciberseguridad del Banco de Occidente.

Esta Política forma parte del Modelo de Seguridad de Banco de Occidente encabezado por el Líder en Seguridad de la Información, son revisadas y aprobadas por el Consejo de Administración y el Comité de Seguridad de la Información del Banco de Occidente y difundidas a los Titulares de la Información, a la Comunidad y a los diferentes roles de Seguridad de la Información.

Los cambios que surjan debido a la dinámica de la tecnología o por otras razones durante la implementación de estas normas y que tengan un impacto en las Políticas de Seguridad de la Información y Ciberseguridad, serán documentados y podrán promover modificaciones a la Política.

1.2 OBJETIVOS DE LAS NORMAS DE SEGURIDAD DE LA INFORMACIÓN

Las Normas de Seguridad de la Información del Banco de Occidente tienen como objetivo desarrollar la Política de Seguridad de la Información y Ciberseguridad, documentando formalmente las reglas para la protección de la información de la Institución que se procesa, transporta o almacena por medios informáticos como software, hardware, redes y otras instalaciones asociadas.

Al aplicar los estándares establecidos en este documento, el Banco de Occidente define cómo se protege la información de manera homogénea y coherente con su criticidad para el negocio, en todos los recursos informáticos.

1.2.1 Ámbito de aplicación

Los Estándares de Seguridad de la Información responden y desarrollan los lineamientos establecidos por la Política de Seguridad de la Información y Ciberseguridad, y están obligados a implementar un Modelo de Seguridad de la Información confiable y flexible, que se apoya en los procedimientos internos de Seguridad de la Información y Ciberseguridad, que tienen como objetivo documentar las principales acciones operativas a ejecutar con el fin de salvaguardar la confidencialidad. integridad y disponibilidad de la información,

manteniendo los niveles de seguridad aceptados por el Banco de Occidente.

Estos estándares forman parte del Modelo de Seguridad de la Información, y se aplican a todos los niveles de la organización: Usuarios (que incluye empleados y accionistas), Clientes, Terceros (que incluye proveedores y contratistas), Entidades de Control, Entidades Relacionadas y Subsidiarias del Banco de Occidente, que acceden, ya sea interna o externamente, a cualquier activo de información que se almacene, procese o transporte, Uso de hardware, software, redes y otras instalaciones asociadas.

1.2.2 Cumplimiento

Las reglas deben ser cumplidas por todas aquellas personas que tengan acceso o hagan uso de la información del Banco de Occidente a través de software, hardware, redes y facilidades asociadas.

El cumplimiento de las normas es obligatorio y las excepciones deben ser documentadas como un riesgo incurrido por el Banco de Occidente, lo cual debe ser aceptado formalmente por el Titular de la Información. La Comunidad debe comprender las implicaciones de las normas y las responsabilidades de su estricto cumplimiento.

El incumplimiento de las normas puede dar lugar a acciones disciplinarias o pecuniarias en el caso de proveedores o contratistas, que pueden llegar incluso hasta la terminación de la relación contractual y/o acciones legales. El desconocimiento de las normas no exime de su aplicación.

Para nuevos desarrollos o nuevas adquisiciones de recursos informáticos, las normas están vigentes desde el periodo de vigencia de las mismas. Se debe establecer un plan detallado para ajustar los recursos informáticos adquiridos con anterioridad a esta vigencia para hacer efectivo el cumplimiento de la norma.

Las Políticas de Seguridad de la Información son una declaración de las responsabilidades y de la conducta aceptada para mantener un ambiente seguro en el Banco de Occidente. Estas Políticas establecen las directrices y los lineamientos relacionados con el manejo seguro de la información

Alcance de las Políticas.

La Política de Seguridad de la Información y Ciberseguridad **proporciona las directrices requeridas para implantar un Modelo de Seguridad de la Información confiable y flexible.**

Define el marco básico que guía la implantación de cualquier norma, proceso, procedimiento, estándar y/o acción, relacionados con la Seguridad de la Información en el Banco de Occidente y filiales.

Aplica para todos los niveles de la organización que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación.

- Usuarios (que incluye empleados y accionistas)
- Clientes
- Terceros (que incluye proveedores y contratistas)
- Entes de Control
- Entidades Relacionadas y Filiales del Banco de Occidente

La política aplica a toda la información creada, procesada o utilizada en el soporte al negocio, y la información personal de los empleados, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Políticas Definidas - 20

- **Seguridad de la Información**
- **Ciberseguridad**
- **Propiedad Intelectual**
- Dueño de la Información
- Cumplimiento de Regulaciones
- **Administración del riesgo en Seguridad de la informacion (SI) y ciberseguridad (CS).**
- **Capacitación y creación de cultura en SI y CS**
- Seguridad en el personal
- **Terceros que Acceden Información del Banco** de Occidente Local o Remotamente
- Identificación y Autenticación Individual
- Control y Administración del Acceso
- **Clasificación de la Información**
- Continuidad del Negocio
- **Seguridad Física**
- No Repudio
- Administración de Alertas
- **Auditabilidad**
- Conectividad
- Uso de los Recursos Informáticos
- Seguridad en la Administración de Sistemas