POLITICA DE SEGURIDAD DE LA INFORMACION

Administrador

CONTENIDO

1. OBJETIVOS

1.1 General

Considerar la información, como un activo vital de DIBANKA para alcanzar sus **objetivos estratégicos**, razón por lo cual se preocupa por establecer lineamientos que garanticen su adecuada gestión y correcta custodia.

1.2 Específicos

Establecer la política principal de **seguridad de la información**, la cual orientará la creación del sistema de gestión de Seguridad, la generación de políticas específicas, procedimientos y estándares que deben ser conocidos y cumplidos por el público general con el fin de **mitigar los riesgos**.

Las actividades de la organización se rigen en torno a lo definido en la **presente política** con el fin de que se promuevan prácticas responsables frente a la información de nuestra organización. Para lo anterior se usa como modelo los estándares de ITIL y las buenas prácticas en materia de controles aplicadas a la norma ISO 27000.

2. ALCANCE/APLICABILIDAD

Esta política es de aplicación para toda la organización, cualquiera sea su situación contractual, integrando a sus colaboradores, directivos y a la totalidad de los procesos internos o externos vinculados con la operación de **DIBANKA**, a través de contratos o acuerdos de confidencialidad, logrando con esto delimitar roles y responsabilidades al interior en el manejo de la información.

3. PARTES INTERESADAS: ROLES Y RESPONSABILIDADES

Con el fin de garantizar la confiabilidad del sistema de gestión de seguridad de la información, se establecen los roles y responsabilidades de los actores del sistema en donde se describen las funciones de cada una de las partes:

Alta Dirección: compuesta por la presidencia y vicepresidencias quienes serán responsables:

- Establecer los roles y responsabilidades con relación a la seguridad de la información en los niveles directivo y operativo.
- Revisar y aprobar las políticas de seguridad de la información definidas en este documento.
- Promover activamente la cultura en relación con la seguridad de la información.
- Facilitar la divulgación de las políticas de seguridad de la información a todos los colaboradores, proveedores y terceros.
- Apoyar al comité de seguridad de la información para establecer, promover, divulgar y sancionar en caso de ser necesaria, todo lo relacionado con las políticas de seguridad de la información y los controles implantados.

Líder Seguridad de la información: persona encargada de gerenciar la implementación y el mantenimiento del sistema de seguridad de la información con las siguientes responsabilidades:

- Generar y construir las políticas de seguridad necesarias para el correcto establecimiento del sistema de gestión de seguridad de la información.
- Actualizar y presentar ante la alta dirección las políticas de seguridad de la información, además, las metodologías de análisis de riesgos y de clasificación de la información, según lo considere pertinente.
- Verificar el cumplimiento de las políticas y controles de seguridad de la información establecidos.
- Identificar, validar y monitorear de manera periódica los riesgos y controles que se requieran para garantizar el tratamiento de los primeros, en materia de seguridad de la información.
- Dar tratamiento a los incidentes y eventos de seguridad que sean reportados por los colaboradores y/o terceros.

Colaboradores y Terceros: Todos los colaboradores contratados por **DIBANKA** para la ejecución de funciones definidas para el cumplimiento de la actividad propia de **DIBANKA**, al igual que los contratistas y proveedores contratados por **DIBANKA**. Para ellos se definen las siguientes funciones y responsabilidades:

- Cumplir las políticas, procedimientos y estándares, definidos por el sistema de seguridad de la información.
- Reportar los incidentes o eventos de seguridad de la información a los que pueda estar expuesta la organización.

Gerencia de tecnología: área encargada de administrar y gestionar todos los activos de información, se definen las siguientes responsabilidades:

- Implementar todos los controles que estén orientados a garantizar los tres pilares de la seguridad de la información: Confidencialidad, integridad y Disponibilidad.
- Asignar funciones y responsabilidades a los colaboradores del área de tecnología de manera que se cumplan los principios de gobernabilidad y buenas prácticas en el tratamiento y seguridad de la información.

4. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La alta Dirección de **DIBANKA**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con sus partes interesadas, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la compañía.

Para **DIBANKA**, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica **DIBANKA** según como se defina en el alcance, sus funcionarios, terceros, aprendices y proveedores, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema de seguridad de la información estarán determinadas por las siguientes premisas:

- ✓ Minimizar el riesgo en las funciones más importantes de **DIBANKA**.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de sus clientes, socios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos de tecnología.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices y clientes de **DIBANKA**
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ **DIBANKA** ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros ajustados a las necesidades del negocio, y a los requerimientos regulatorios.

4.1 PRINCIPIOS DE SEGURIDAD

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros:

- ✓ **DIBANKA** protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros: clientes o proveedores.
- ✓ **DIBANKA** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- ✓ **DIBANKA** protegerá su información de las amenazas originadas por parte del personal.
- ✓ **DIBANKA** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ✓ **DIBANKA** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ✓ **DIBANKA** implementará control de acceso a la información, sistemas y recursos de red.
- ✓ **DIBANKA** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- ✓ **DIBANKA** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- ✓ **DIBANKA** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- ✓ **DIBANKA** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

4.2 POLITICAS ESPECIFICAS

4.2.1 ACUERDOS DE CONFIDENCIALIDAD Y NO DIVULGACIÓN

Todos los colaboradores de **DIBANKA** y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la compañía, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de **DIBANKA** a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

4.2.2 USO DE RECURSOS DE TECNOLOGIA

El uso adecuado de los recursos tecnológicos asignados por nuestra compañía a cada uno de sus colaboradores y/o proveedores se reglamenta bajo los siguientes lineamientos:

- ✓ La instalación de cualquier tipo de software o hardware en los equipos de cómputo de **DIBANKA** es responsabilidad de la Dirección de Tecnología, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por el área de tecnología. En caso solo y únicamente laborales, un colaborador requiriera instalar y ejecutar una aplicación para su uso personal, por cumplimientos de labores internas, dicho colaborador es responsable de gestionar su licenciamiento, se autoriza el uso de versiones Trial, Beta o Software GNU, realizando su respectiva desinfección y chequeo.
- ✓ Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por la Dirección de Tecnología.
- ✓ El área de Tecnología debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
- ✓ Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la compañía; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Dirección de Tecnología.
- ✓ La sincronización de dispositivos móviles, tales como tablets, smartphones u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la Dirección de Tecnología y podrá llevarse a cabo sólo en dispositivos al interior de la organización y de requerirse una auditoria sobre el dispositivo en mención, esta podrá ser ejecutada ya que se encuentra dentro de la red de la Organización.

4.2.3 PROTECCION CONTRA SOFTWARE MALICIOSO

DIBANKA establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de Seguridad como antivirus, antispam, antispyware y otras aplicaciones

que brindan protección contra código malicioso y prevención del ingreso de este a la red y entorno corporativo, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causa dos por código móvil y malicioso. Será responsabilidad del área de Tecnología autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados en ninguna circunstancia, así como de su actualización permanente.

No está permitido:

- ✓ La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por el área de Tecnología de la compañía.
- ✓ Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- ✓ Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.
- ✓ El uso de Código móvil. Este sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de Seguridad definidas y debidamente autorizado por el área de Tecnología.

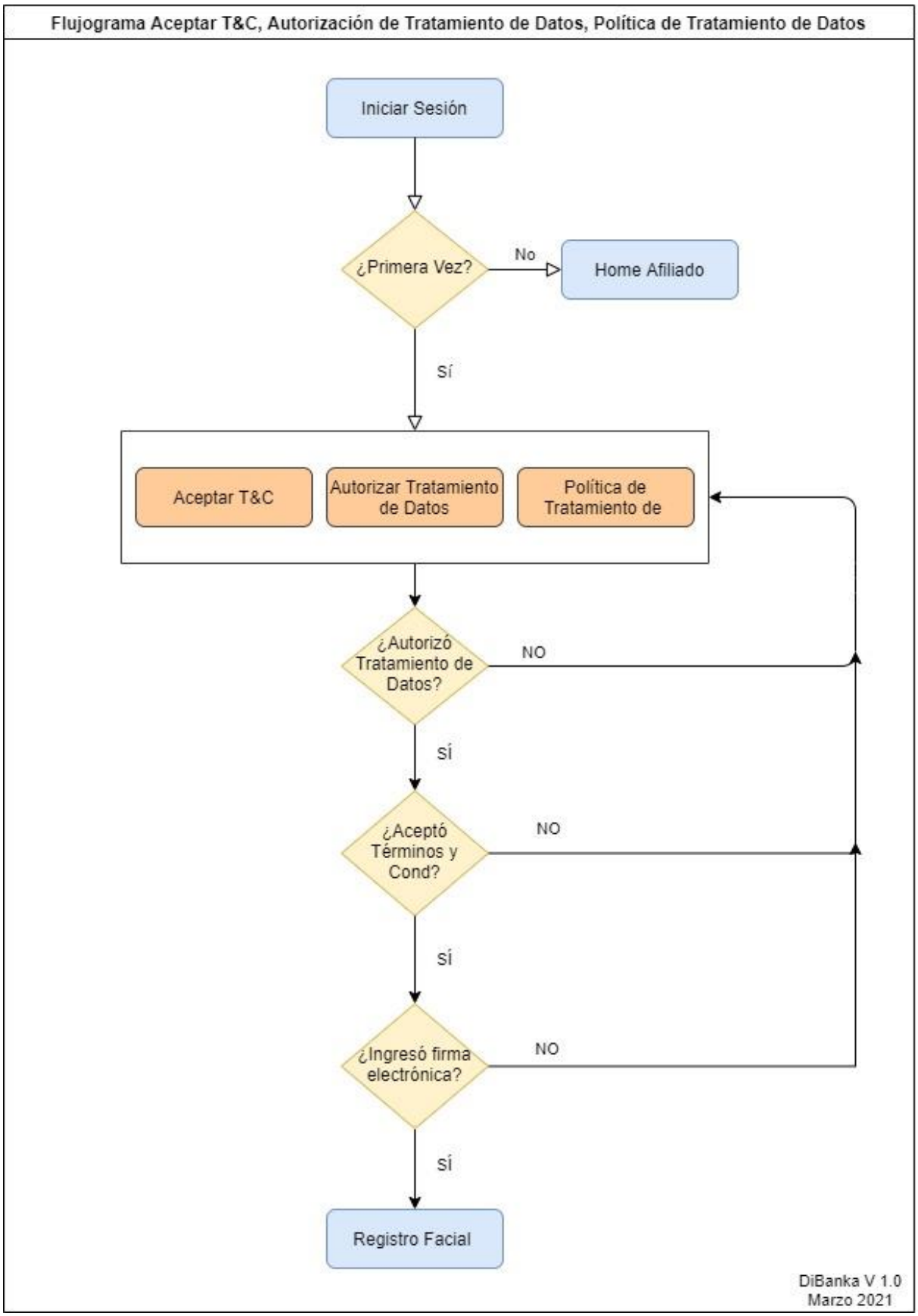
4.2.4 COPIAS DE RESPALDO

DIBANKA debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el área de Tecnología y las áreas responsables de la misma, contenida en la plataforma tecnológica de la compañía, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente respaldada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El área de Tecnología establecerá procedimientos explícitos de respaldo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá juntamente con las áreas los períodos de retención de esta. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información respaldada.

5 REVISIONES Y APROBACIONES

Versión	Fecha	Autor	Estado	Revisado por	Aprobado por	Descripción modificación
1.0	03/05/2021	Alejandro Martinez	Creación	Andres Giraldo	Bernabé Barragan	Creación del documento


Flujograma Aceptar T&C, Autorización de Tratamiento de Datos, Política de Tratamiento de Datos
Iniciar Sesión
¿Primera Vez?
No
Home Afiliado
Sí
Aceptar T&C
Autorizar Tratamiento de Datos
Política de Tratamiento de
¿Autorizó Tratamiento de Datos?
NO
Sí
¿Aceptó Términos y Cond?
NO
Sí
¿Ingresó firma electrónica?
NO
Sí
Registro Facial
DiBanka V 1.0
Marzo 2021