DIXHI COMPANY

TOP UP, BILLETERA DIGITAL

Políticas de seguridad y ciberseguridad.

2023

La Billetera para estar activos

www.topup.com.co

HISTORIAL

Version	Fecha	Cambios Introducidos
1.0.0	08/03/2023	Versión inicial del documento

Contents

Pag

1. OBJETIVO 4
2. INTRODUCCIÓN 4
3. POLITICA GENERAL DE SEGURIDAD Y CIBERSEGURIDAD DE LA INFORMACIÓN 5
4. ALCANCE Y APLICABILIDAD 6
5. NIVEL DE CUMPLIMIENTO 7
6. CIBERSEGURIDAD 8
   6.1. PRINCIPIOS DE LA CIBERSEGURIDAD 8
7. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN 9
8. GOBIERNO CORPORATIVO 11
9. DIVULGACIÓN DE REPORTES DE GESTIÓN 12
10. ACTUALIZACIÓN DE LA POLITICA 12
11. IMPLEMENTACIÓN DE LA POLITICA 12
12. ANTECEDENTES NORMATIVOS 13

1. OBJETIVO

Establecer las directrices, lineamientos, responsabilidades y conductas que seguirán todos los colaboradores de la Entidad para mantener los principios de confidencialidad, integridad, disponibilidad y privacidad de la información, desarrollando habilidades y conocimientos requeridos para tener y aplicar buenas prácticas de Seguridad de la Información y Ciberseguridad, de acuerdo con las necesidades de la Entidad y las normativas que apliquen.

2. INTRODUCCIÓN

DIXHI COMPANY SAS identifica la información como uno de los activos más importantes, ya que ésta se considera pilar para brindar sus servicios y cumplir con los objetivos propuestos. Información que se almacena, procesa y transporta en sistemas tecnológicos que soportan la operación de los diferentes procesos; siendo vital el servicio de la plataforma tecnológica para el funcionamiento de aplicaciones internas, externas, redes y en general equipos tecnológicos que se conectan entre sí en el ciberespacio para mantener la operación de la Entidad.

El presente documento describe la Política General de Seguridad de la Información y Ciberseguridad en **DIXHI COMPANY SAS**, la cual se basa en estándares, buenas prácticas y normativas aplicables. La Política General de Seguridad de la Información y Ciberseguridad, definida y aprobada por la Gerencia General es la base para definir la metodología de riesgos, implantación de controles y toma de decisiones de Seguridad de la Información y Ciberseguridad.

3. POLÍTICA GENERAL DE SEGURIDAD y CIBERSEGURIDAD DE LA INFORMACIÓN

De manera genérica a continuación se entrega un texto guía para la elaboración de la política general de seguridad de la información, este puede ser base del desarrollo de dicho documento ya que contempla los principios básicos a tener en cuenta en su elaboración dentro de la planeación del sistema de gestión de seguridad de la información en una entidad.

La dirección de **DIXHI COMPANY SAS**, 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 el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para **DIXHI COMPANY SAS**, 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 la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

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

- Minimizar el riesgo en las funciones más importantes de la entidad.
- 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 tecnológicos.
- 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, practicantes y clientes de **DIXHI COMPANY SAS**
- Garantizar la continuidad del negocio frente a incidentes.
- **DIXHI COMPANY SAS** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en

lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de **DIXHI COMPANY SAS** con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

DIXHI COMPANY SAS, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- 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, practicantes y clientes del **DIXHI COMPANY SAS**
- Garantizar la continuidad del negocio frente a incidentes.

4. ALCANCE Y APLICATIVIDAD

- Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del NOMBRE DE LA ENTIDAD y la ciudadanía en general.

5. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de **DIXHI COMPANY SAS**:

- **DIXHI COMPANY SAS** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- **DIXHI COMPANY SAS** protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- **DIXHI COMPANY SAS** 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.
- **DIXHI COMPANY SAS** protegerá su información de las amenazas originadas por parte del personal.
- **DIXHI COMPANY SAS** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- **DIXHI COMPANY SAS** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- **DIXHI COMPANY SAS** implementará control de acceso a la información, sistemas y recursos de red.
- **DIXHI COMPANY SAS** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- **DIXHI COMPANY SAS** 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.
- **DIXHI COMPANY SAS** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- **DIXHI COMPANY SAS** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

6. CIBERSEGURIDAD

Ciberseguridad, es el conjunto de políticas, conceptos de seguridad, recursos, controles de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación, desarrollo, formación y buenas prácticas en general, utilizadas para prevenir y proteger los datos, sistemas y aplicaciones; salvaguardando a los consumidores financieros y activos de la Entidad en el ciberespacio, preservando los principios de la Seguridad de la Información e incluyendo las características de:

- **Control de accesos:** Proceso mediante el cual se permite o no el acceso de un usuario a aplicaciones, servidores, equipos tecnológicos entre otros, según los perfiles asignados.

- **No repudio:** Condición por medio de la cual no se puede negar la ejecución de una actividad realizada sobre la plataforma tecnológica, de acuerdo con los registros de auditoría o log's.

6.1. PRINCIPIOS DE LA CIBERSEGURIDAD

Con el fin de dar cumplimiento al marco normativo, regulatorio y a los objetivos de negocio, **DIXHI COMPANY SAS** considera los siguientes principios de la Ciberseguridad para preservar la información y correcto funcionamiento de la plataforma tecnológica para que no se afecten los procesos de la Entidad:

- **Mínimo privilegio:** Son todos aquellos privilegios que tienen los sistemas y aplicaciones que se encuentran interconectados pero que solo deben tener los usuarios, configuración y conexión de red necesarios para que funcionen de acuerdo con lo requerido por el proceso.

- **Mínima superficie de exposición:** Deben diseñarse las tareas o actividades a realizar en cada uno de los procesos de la Entidad, de tal forma que no queden o se habiliten canales, privilegios, IP's, usuarios, publicación o puertos que faciliten a un ciberdelincuente

acceder a los sistemas, producto de estas debilidades de configuración en la red y plataforma tecnológica.

- **Defensa en profundidad:** Debe existir seguridad por niveles o anillos, es decir, que la arquitectura de red o controles de ciberseguridad que se implementen, tales como: firewall, IPS, IDS, Antivirus, WAF, antispam, honeypot, etc., deben configurarse en diferentes zonas de red. Así como usar diferentes dispositivos para dificultar el trabajo de un ciberdelincuente, obstaculizando su paso por las diferentes capas y evitando que cumpla con su objetivo.

7. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes son los objetivos en materia de Seguridad de la Información y Ciberseguridad definidos por **DIXHI COMPANY SAS**:

- Cumplir con las obligaciones legales vigentes relacionadas con Seguridad de la Información y Ciberseguridad que apliquen a la Entidad, tomando las medidas necesarias de acuerdo con la operación que se realiza en **DIXHI COMPANY SAS**.
- Gestionar los riesgos de Seguridad de la Información y Ciberseguridad en todos los procesos de manera eficiente, con el fin de proporcionar continuidad y calidad a las operaciones del negocio.
- Facilitar la discusión al interior de la Entidad en temas de Seguridad de la Información y Ciberseguridad, ayudando a que todos los colaboradores, clientes y contratistas sean conscientes de las amenazas potenciales de Seguridad de la Información y Ciberseguridad con los riesgos asociados al negocio.
- Soportar y mejorar la calidad de las operaciones de **DIXHI COMPANY SAS**, permitiendo un equilibrio entre funcionalidad y seguridad, a la luz de las mejores prácticas de la industria.

DIXHI COMPANY SAS, como el aliado estratégico para sus clientes, empresas del sector financiero y crediticio digital a través de su producto digital TOP UP, billetera digital; generando valor a partir de procesos como recaudos y dispersión de dinero y para sus usuarios pertenecientes a segmento social 1, 2 y 3 prestando servicios de billetera para transacciones digitales tales como compras, pagos, recargas, transferencias y acceso a créditos digitales,

define sus procesos y brinda sus servicios de forma diligente y segura, generando confianza con los beneficiarios, Intermediarios Financieros, proveedores, colaboradores y demás grupos de interés o personas que tienen relación con **DIXHI COMPANY SAS**, administrando los recursos e información de forma segura.

Para **DIXHI COMPANY SAS**, la información es considerada como uno de los activos importantes para el negocio y los procesos que soportan su operación, por este motivo se implementan buenas prácticas de Seguridad de la Información y Ciberseguridad que permiten cumplir con la normativa o requerimientos legales aplicables de los Entes de Control.

DIXHI COMPANY SAS encamina los esfuerzos de los colaboradores y recurso técnico, para preservar la información y conservar la confidencialidad, integridad y disponibilidad de los activos de información, protegiendo y asegurando en el ciberespacio, los datos, sistemas y aplicaciones que son esenciales para la operación de la Entidad. Igualmente, **DIXHI COMPANY SAS** se compromete a proteger los datos sensibles, ejecutando los procesos de manera óptima y manteniendo su privacidad.

Por tanto, **DIXHI COMPANY SAS** debe:

- Establecer los fundamentos para el desarrollo y la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad, que esté alineado con la estrategia corporativa y los objetivos del negocio.
- Definir los lineamientos y mejores prácticas que permitan la prevención, gestión y respuesta de incidentes de Seguridad de la Información y Ciberseguridad.
- Establecer que todos los colaboradores y terceros son responsables de registrar y reportar las violaciones y eventos sospechosos de Seguridad de la Información y Ciberseguridad, de acuerdo con los procedimientos correspondientes.
- Clasificar, proteger y asignar responsables de los Activos de Información, de acuerdo con la metodología que se establezca y con los criterios de valoración, en relación con la importancia que posee para la Entidad. Realizando igualmente el análisis de riesgos correspondiente, para definir los controles que preserven la información y plataforma tecnológica de la Entidad.

- Establecer los requisitos y buenas prácticas de Seguridad de la Información y Ciberseguridad, uso aceptable y controles relacionados con el acceso y utilización de los activos de la información de **DIXHI COMPANY SAS**, que mantengan y protejan las características de confidencialidad, integridad y disponibilidad de éstos.

- Definir los lineamientos y mejores prácticas que permitan la prevención, gestión y respuesta de incidentes de Seguridad de la Información y Ciberseguridad de forma oportuna.
- Designar un equipo de Seguridad de la Información y Ciberseguridad, que se encargue de la guía, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, dando cumplimiento a la normativa.
- Definir las directrices y lineamientos relacionados con la gestión del recurso humano, para la concientización y pertenencia de la Seguridad de la Información y Ciberseguridad en todos los colaboradores.

8. GOBIERNO CORPORATIVO

Para la aplicación y cumplimiento de la política, se establece el gobierno de Seguridad de la Información y Ciberseguridad, donde:

- La Gerencia General aprueba la Política General.
- El Comité de Seguridad de la Información, aprueban las Políticas de Dominio.
- El Oficial de Seguridad de la Información, será el responsable de la gestión y estrategia para el cumplimiento y madurez de la Seguridad de la Información y Ciberseguridad en la Entidad.
- Los líderes de área deben asumir las responsabilidades que les sean asignadas para apoyar la ejecución de las Políticas de Dominio.
- Todos los colaboradores o comunidad **DIXHI COMPANY SAS** deben cumplir con las políticas definidas.

9. DIVULGACIÓN DE REPORTES DE GESTIÓN

Semestralmente el Oficial de Seguridad de la Información de la Entidad, presentará a la gerencia general los resultados de la gestión realizada frente a Seguridad de la Información y Ciberseguridad.

10. ACTUALIZACIÓN DE LA POLÍTICA

Se espera que la Política de Seguridad de la Información y Ciberseguridad se preserve en el tiempo, sin embargo, ante modificaciones por cambios en la regulación o marco legal aplicable, cambios estructurales que afecten a **DIXHI COMPANY SAS** o incidentes graves, la política debe ser revisada y/o modificada y estos cambios aprobados por la Gerencia General de **DIXHI COMPANY SAS**.

11. IMPLEMENTACIÓN DE LA POLÍTICA

La Política General de Seguridad de la Información y Ciberseguridad involucra el desarrollo e implantación de un Sistema de Gestión de Seguridad de la Información y Ciberseguridad integrado en el día a día de la operación de la Entidad. Como sistema de gestión, debe tener una madurez continua, para alcanzar los objetivos establecidos en el presente documento. Se anticipa y autoriza el desarrollo de políticas de dominio, normas, procedimientos, estándares, guías, instructivos y otras medidas administrativas que sean necesarias incluyendo la definición de una unidad o grupo de Seguridad de la Información y Ciberseguridad, así como el desarrollo o la adquisición de las herramientas, software y demás recursos que se requiera como apoyo a la gestión realizada.

El Sistema de Gestión de Seguridad de la Información y Ciberseguridad se desarrolla con base en las siguientes etapas:

- Prevención: **DIXHI COMPANY SAS** desarrolla e implementa controles para velar por la Seguridad de la Información y la gestión de la Ciberseguridad, que permiten evitar incidentes sobre la información o plataforma tecnológica.
- Protección y detección: **DIXHI COMPANY SAS** implementa controles y actividades de monitoreo que permiten identificar eventos de Seguridad de la Información y Ciberseguridad, para tener una detección temprana que permita tomar acciones de contención o realizar la gestión que corresponda para atender los eventos evitando que estos se conviertan en incidentes.

- Respuesta y comunicación: **DIXHI COMPANY SAS** establece planes de respuesta a incidentes de Seguridad de la Información y Ciberseguridad, para proceder a ejecutar actividades de análisis y contención, incluyendo la comunicación, en caso de ser necesario el apoyo de entes externos.
- Recuperación y aprendizaje: **DIXHI COMPANY SAS** define las actividades que permiten restaurar los servicios afectados por un incidente de Seguridad de la Información o Ciberseguridad, documentando posteriormente las lecciones aprendidas para identificar debilidades en controles, como se desarrolló el ataque, afectación y mejoras que puedan aplicarse a los planes de respuesta a incidentes.

12. ANTECEDENTES NORMATIVOS

El marco Normativo aplicable a **DIXHI COMPANY SAS** en asuntos relacionados con Seguridad de la Información y Ciberseguridad, el cual es la base de la implementación del Sistema de Gestión se presenta a continuación:

- Circular Básica Jurídica de Superintendencia Financiera de Colombia.
- Ley 23 de 1993 y Ley 44 de 1993: Derechos de autor.
- Ley 679 de 2001 y Ley 1336 de 2009: Pornografía Infantil.
- Ley 1266 de 2008: Habeas Data.
- Ley 1273 de 2009: Delitos Informáticos.
- Ley 1581 de 2012: Protección de datos personales.
- Circular Externa 042 de 2012: Capitulo décimo segundo: Requerimientos mínimos de seguridad y calidad para la realización de operaciones.
- Circular Externa 007 de 2018: Requisitos mínimos para la gestión de riesgos de Ciberseguridad.

Atentamente,

Marcela Santiago Rizo
CEO – Gerente General
marcela.santiago@dixhi.com.co
Cel: 3218947395
Dixhi Company S.A.S.