CONTROL DE CAMBIOS			
Versión n°	**Fecha**	**Descripción del Cambio**	**Responsable**
01	11/08/2022	Creación del documento	Edwin Leonardo Tello
02	09/01/2023	Se revisa la política y se establece los parámetros de una contraseña segura	Andrés Mauricio Rojas
03	04/09/2023	Se realizan ajustes generales y se cambia codificación	Tulio Niño
04	13/11/2023	Se actualiza la prestación del servicio	Tulio Niño
	04/09/2024	Se realiza la revisión de la política y no se genera ningún cambio.	Alta Dirección - Tulio Niño
	12/09/2025	Se genera revisión de la política, no se realiza ningún cambio.	Tulio Niño

Elaboró: Tulio Armando Niño	Revisó: Fernando Ávila	Aprobó: Andrés Mauricio Rojas
Firma: Tulio N	Firma: Fernando J. Ávila Insuasty	Firma:
Cargo: Information Security Officer	Cargo: Chief Engineer Data Center Officer	Cargo: Country Manager

LDSAHDR

1. OBJETIVO

Definir las políticas, responsabilidades, principios y directrices que deben de cumplir las personas frente al uso de los activos con el fin de regular la gestión de la seguridad de la información en la compañía.

2. ALCANCE

Las políticas contenidas en este documento se establecen, aplican y deberán ser conocidas, aceptadas y cumplidas por todos los empleados, contratistas, practicantes, terceros, entre otros. El incumplimiento de las mismas se considerará un incidente de seguridad que, de acuerdo al caso, podrá dar lugar a un proceso disciplinario para los empleados o una causa válida para terminación de contratos establecidos con los terceros involucrados, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

3. DESARROLLO

3.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

HOSTDIME GLOBAL DATA SAS empresa dedicada a la prestación de **Servicio de Colocación en Data Center***,* reconoce que la información es un activo fundamental para su funcionamiento y toma de decisiones que puede ser objeto de amenazas deliberadas o accidentales.

Por consiguiente *Hostdime Global Data,* define como objetivo proteger la información contra diversas amenazas e implementar el Sistema de Gestión de Seguridad de la Información como una estrategia para garantizar la continuidad del negocio, minimizar los riesgos, reducir el impacto ocasionado por la materialización de incidentes de seguridad y dar cumplimiento a los estándares legales y regulatorios aplicables a la compañía.

Para el desarrollo de la estrategia se implementará una cultura organizacional enfocada en identificar y evaluar los riesgos de acuerdo con los objetivos de la compañía tomando como base los criterios de clasificación, evaluación y valoración, descritos en la metodología de riesgo para la definición de controles relacionados con la seguridad y la búsqueda hacia la mejora continua, teniendo en cuenta los requerimientos de nuestras partes interesadas para incrementar la credibilidad y la confianza de los procesos y garantizar la confidencialidad, integridad y disponibilidad de la información y de los activos tecnológicos.

3.2 COMPROMISO DE LA DIRECCIÓN

La alta dirección aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Compañía, y demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información.
- La promoción activa de una cultura de seguridad.
- La promoción y divulgación de las políticas a todos los colaboradores de la compañía.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas de seguridad de la información.

HDR LDSA

Con el objetivo de mantener alineadas las políticas de seguridad de la información con los procedimientos y actividades de la compañía, estas deben ser revisadas anualmente o cada que se presenten cambios representativos que ameriten su revisión.

3.3 RESPONSABILIDADES

- *La alta dirección debe* establecer una estructura organizacional responsable de la seguridad de la información, con roles y responsabilidades claramente definidos, teniendo en cuenta actividades para la gestión de riesgos, análisis de las tecnologías y del entorno, con el fin de garantizar la continuidad de la operación de la compañía.

- El encargado de la seguridad de la información en conjunto con la alta dirección son los responsables de la definición, revisión y vigilancia de las Políticas de Seguridad de la Información.

- El proceso de gestión operativa es el encargado de ejecutar las políticas de seguridad de la información.

- El Comité de Seguridad de la Información es el responsable de tratar los incidentes de seguridad que se presenten y tomar las decisiones apropiadas que permitan mantener correctamente el sistema de gestión de seguridad de la información en la compañía.

- Los propietarios de activos de información son responsables del uso adecuado y de la preservación del correcto estado de los mismos.

- El proceso administrativo es responsable por determinar y ejecutar las sanciones que se deriven del incumplimiento de las políticas de Seguridad de la Información por parte del personal de la compañía.

- Todos los empleados, contratistas, practicantes y terceros son responsables y deben comprometerse a cumplir con todas las Políticas de Seguridad de la Información.

3.4 SANCIONES POR INCUMPLIMIENTO

El incumplimiento de las Políticas de Seguridad de la Información se gestiona mediante procedimientos administrativos, cuando se identifique un incumplimiento a la presente Política se deberá reportar al comité de seguridad de la información de la compañía utilizando los canales definidos para dicho fin, para los efectos de su competencia y atribuciones. Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la compañía o los delitos informáticos contemplados en el artículo 269 de la ley 1273 de 2009.

12 de Septiembre 2025

Andres Mauricio Rojas Pardo
Representante Legal

LDSAMDR