POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Protegemos tu información: Conoce nuestra Política de Seguridad y Privacidad

En **JJ NETWORKS SAS**, nos tomamos muy en serio la seguridad y privacidad de tu información. Por eso, hemos implementado la Política General de Seguridad y Privacidad de la Información.

¿Qué encontrarás en este documento?

Esta política detalla nuestros compromisos y prácticas para proteger tus datos personales y la información que nos confías. En ella encontrarás información sobre:

- Cómo recopilamos, usamos y protegemos tu información.
- Tus derechos con respecto a tus datos personales.
- Las medidas de seguridad que implementamos para prevenir accesos no autorizados.
- Nuestra política de cookies.
- Cómo contactarnos si tienes alguna pregunta o inquietud.

Te invitamos a revisar cuidadosamente nuestra Política General de Seguridad y Privacidad de la Información, disponible para descarga en el siguiente enlace:

CONOCE CÓMO PROTEGEMOS TU INFORMACIÓN EN JJ NETWORKS SA:

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La dirección de **JJ NETWORKS SAS**, entendiendo la importancia de una adecuada gestión y protección de los activos de información, se ha comprometido con 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, 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 compañía.

2. OBJETO

Disminuir, mediante el Sistema de Gestión de Seguridad de la Información, el impacto generado por los riesgos identificados de manera sistemática, mediante la protección de la información, basados en los tres principios de seguridad de la información: **integridad, confidencialidad y disponibilidad**, determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de **JJ NETWORKS SAS** Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de nuestros 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.
- Garantizar la continuidad del negocio frente a incidentes.
- **JJ NETWORKS SAS** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros y alineados a las necesidades del negocio.

3. ALCANCE

La presente política general de seguridad y privacidad de la información es de aplicación y obligado cumplimiento para todos los empleados de **JJ NETWORKS SAS**, así como para aprendices, practicantes, proveedores, contratistas, terceros y la ciudadanía en general.

4. GLOSARIO

- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar los activos de información.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Controles:** Medidas que permiten reducir o mitigar un riesgo.

5. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para lograr el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información, **JJ NETWORKS SAS** establece las siguientes políticas:

5.1 Definir las responsabilidades frente a la seguridad de la información y garantizar que estas sean compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio y/o terceros.

5.2 Proveer los controles de seguridad necesarios para que la información corporativa sea accedida únicamente por funcionarios o terceros autorizados según su rol.

5.3 Proteger la información generada, procesada o resguardada por los procesos del negocio, su infraestructura tecnológica y activos, de riesgos derivados del acceso otorgado a terceros (ej.: proveedores o clientes) o como resultado de servicios en outsourcing.

5.4 Proteger la información creada, procesada, transmitida o resguardada, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto.

5.5 Proteger la información frente a amenazas originadas por parte del personal.

5.6 El personal administrativo y directivo deberá mantener escritorios y equipos limpios, ordenados y seguros, previniendo accesos no autorizados.

5.7 Controlar la operación de los procesos de negocio garantizando la seguridad de recursos tecnológicos y redes de datos.

5.8 Integrar la seguridad como parte esencial del ciclo de vida de los sistemas de información.

5.9 Garantizar la mejora continua de la gestión de eventos y debilidades de seguridad.

5.10 Asegurar la disponibilidad de los procesos de negocio y la continuidad frente a incidentes.

5.11 Cumplir las obligaciones legales, regulatorias y contractuales.

5.12 Aplicar controles criptográficos para la información clasificada como confidencial o crítica.

5.13 Diferenciar y controlar el uso de dispositivos móviles corporativos y personales, estableciendo lineamientos de seguridad en ambos casos.

5.14 Generar copias de respaldo periódicas de la información clasificada como crítica y verificar su integridad.

5.15 Controlar la transferencia de información mediante canales autorizados, asegurando la confidencialidad, integridad y disponibilidad.

5.16 Incluir criterios de seguridad en el ciclo de vida de los desarrollos de software y sistemas de información.

5.17 Establecer acuerdos con proveedores que garanticen la protección de la información involucrada en los servicios o productos contratados.

El incumplimiento de esta política generará consecuencias legales y disciplinarias según la normativa interna y la legislación colombiana.

6. ROLES Y RESPONSABILIDADES

Rol / Instancia	Responsabilidades
Alta Dirección	• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación ‘(recursos tecnológicos). • Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información.
Grupo TIC	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. • Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. • Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el

Rol / Instancia	Responsabilidades
	establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad.
Control Interno	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Talento Humano	• Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la segundad de la información de acuerdo con las políticas y procedimientos establecidos. • Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad. • Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurarla la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Líderes de Proceso	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGS (Por ejemplo: gestión de activos, gestión de riesgos, entre otros)
Todos los funcionarios y contratistas	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

7. SANCIONES

A. Cualquier violación a las políticas de seguridad de la información de **JJ NETWORKS SAS** será sancionada de acuerdo con el Reglamento Interno de Trabajo, las normas legales vigentes en Colombia y las disposiciones sobre delitos informáticos.
B. Las sanciones variarán según la gravedad, las consecuencias y la intencionalidad de la falta.
C. Si la entidad considera agregar más factores en este punto, puede hacerlo con base a las normas, leyes y estatutos vigentes)

8. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

JJ NETWORKS SAS realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.

9. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la **Alta Dirección**. La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se presentan cambios estructurales en la entidad (reestructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran modificaciones a la política.

ELABORÓ

Nombre: Juan Carlos Muñoz Amado
Cargo: Representante Legal Suplente / Responsable designado
Fecha: (17/06/2026)

REVISÓ

Nombre: Juan Carlos Muñoz Amado
Cargo: Representante Legal Suplente / Responsable designado
Fecha: (17/06/2026)

APROBÓ

Nombre: Juan Carlos Muñoz Amado
Cargo: Representante Legal Suplente / Responsable designado
Fecha: (17/06/2026)