

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
JUJU S.A.S.

TABLA DE CONTENIDO

1. OBJETIVO 3
2. DEFINICIONES/GLOSARIO 3
3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 4
4. COMPROMISO DE LA ALTA DIRECCIÓN 6
5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 6
6. APLICABILIDAD 6
7. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES) 7
8. SANCIONES 10
9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI 10
10. APROBACIÓN Y REVISIONES A LA POLÍTICA 11
11. AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES 11

1. OBJETIVO

Establecer los lineamientos definidos por la Alta Dirección de **JUJU SAS** para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad de la Información y demás requisitos de ley y las necesidades de las partes interesadas.

2. DEFINICIONES/GLOSARIO

2.1 Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

2.2 Integridad: Propiedad de la información que busca preservar su exactitud y completitud.

2.3 Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

2.4 Sistema de Gestión de Seguridad de la Información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

2.5 Controles: Medida que permite reducir o mitigar un riesgo.

2.6 Organización: Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para alcanzar sus objetivos.

2.7 Partes Interesadas: Persona u organización que puede afectar, ser afectada o percibir ser afectada por una decisión o actividad.

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

JUJU SAS desde la Alta Dirección establece directrices que están orientadas a proteger la Confidencialidad, Disponibilidad e Integridad de los activos de información y además se compromete a salvaguardarlos mediante una adecuada gestión de respuesta al riesgo. Esto incluye la detección, análisis, respuesta y recuperación ante incidentes de seguridad de la información, garantizando la continuidad del negocio y la mitigación de impactos. Asimismo, generando un compromiso frente a las partes interesadas, de apoyar todas las actividades para dar cumplimiento de los requisitos legales, reglamentarios y otros aplicables, promoviendo mejores prácticas y controles en todos los niveles de la organización que conlleven a la mejora continua del Sistema de Gestión.

JUJU SAS en su propósito de dar cumplimiento con la política de seguridad de la información, establece los siguientes objetivos y principios:

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

- **Objetivo 1:** Gestionar los riesgos de seguridad de la información y potenciales amenazas del entorno.
- **Objetivo 2:** Fortalecer la gestión de incidentes de seguridad de la información mediante la detección, análisis, manejo y lecciones aprendidas, asegurando la mitigación de impactos y la mejora continua del SGSI.
- **Objetivo 3:** Cumplir los requisitos legales y reglamentarios aplicables relacionados con la seguridad de la información.
- **Objetivo 4:** Estructurar planes de capacitación y sensibilización para el logro de la seguridad de la información.
- **Objetivo 5:** Promover mejores prácticas y controles en todos los niveles de la organización que conlleven a la mejora continua del Sistema.

PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

A continuación, se establecen 10 principios de seguridad que soportan el SGSI de JUJU S.A.S.:

a) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados.

b) JUJU S.A.S. protegerá la información generada, procesada o almacenada por sus procesos de negocio, su infraestructura tecnológica y activos, mitigando los riesgos asociados a los accesos concedidos a terceros, o no autorizados, disminuyendo posibles impactos, financieros, operativos y legales.

c) JUJU S.A.S. protegerá su información de las amenazas originadas por el entorno interno o externo y protegerá la infraestructura tecnológica que soporta sus procesos críticos.

d) JUJU S.A.S fomentará una cultura y un enfoque en gestión basado en la gestión del riesgo.

e) JUJU S.A.S. controlará la operación de sus procesos de negocio garantizando la seguridad de la información, los recursos tecnológicos y las redes de datos.

f) JUJU S.A.S. implementará control de acceso a la información, sistemas y recursos de red.

g) JUJU S.A.S. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

h) JUJU S.A.S. 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.

i) JUJU S.A.S. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos de riesgo.

j) JUJU S.A.S. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en torno a seguridad de la información.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de **JUJU S.A.S.** se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Así mismo, se compromete a realizar revisiones periódicas para evaluar el progreso de su implementación y realizar recomendaciones para su fortalecimiento.

Además, la Alta Dirección garantizará y asegurará los recursos adecuados (tecnológicos, financieros, humanos), para la efectiva implementación y mantenimiento del sistema. La seguridad de la información será integrada como un componente esencial en las decisiones estratégicas, garantizando así su consideración en todos los aspectos clave de la operación. Este compromiso reafirma la importancia que la Alta Dirección asigna a la seguridad de la información en el marco de las prácticas empresariales y el logro de los objetivos organizacionales.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Seguridad de la información en el desarrollo de soluciones tecnológicas, puestas en marcha y acompañamiento de programas que brindan fidelización e incentivos a empleados de las empresas, canales de distribución y consumidores de los clientes.

6. APLICABILIDAD

La presente política junto con sus objetivos, así como los manuales, procedimientos o documentos derivados o complementarios, son de aplicación obligatoria para todos los colaboradores internos y terceros relacionados con JUJU S.A.S. El incumplimiento a la Política de Seguridad de la Información, a sus directrices o lineamientos asociados, traerá consigo las consecuencias legales pertinentes y que apliquen a la normativa de la organización.

7. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

JUJU S.A.S., define los roles y responsabilidades para la implementación del SGSI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.):

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Alta Dirección	• Proporcionar y aprobar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información. • Generar recomendaciones a las salidas resultantes del Sistema de Gestión de Seguridad de la Información.
Equipo Tecnología	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. • Analizar y comunicar las posibles afectaciones que podrían generar los incidentes seguridad y/o vulnerabilidades resultantes de pruebas técnicas y/o datos compartidos por el Oficial de Seguridad de la Información. • Proponer mejoras para el fortalecimiento de los controles tecnológicos a nivel de desarrollo seguro, gestión de la configuración, gestión de la infraestructura, gestión de la continuidad del negocio, entre otros.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Equipo de Seguridad de la Información y Control Interno	• Definir la metodología transversal para abordar los frentes estratégicos y operativos de los lineamientos establecidos por el Sistema de Gestión de Seguridad de la Información. • Analizar las recomendaciones y oportunidades de mejora resultantes de auditorías internas, externas o legales aplicables, y comunicar a las partes interesadas para su gestión. • Apoyar la generación de la estructura documental (manuales, procedimientos, formatos, etc.) que permita la estandarización, trazabilidad y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información. • Acompañar a los responsables de la gestión del riesgo, en la identificación de eventos y controles, y realizar recomendaciones para el fortalecimiento de estos. • Monitorear la aplicación de planes de acción, con el fin de favorecer la madurez del Sistema de Gestión de Seguridad de la Información. • Realizar investigación de amenazas o vulnerabilidades activas en el entorno externo y comunicar al negocio para la gestión preventiva pertinente. • Fomentar que las partes interesadas tomen conciencia de nuestro compromiso con el Sistema de Gestión y sus responsabilidades frente al logro de los objetivos del mismo. • Gestionar la identificación de posibles vulneraciones a las Políticas de Seguridad de la Información

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Equipo de Gestión Humana	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la conciencia en todos los niveles de la organización. • Implementar los controles de tipo organizacional, físicos y de personas que ayuden a mitigar los riesgos de seguridad de la información, fortaleciendo la gestión con los proveedores relacionados con seguridad de la información y la gestión de activos. • Garantizar la confidencialidad, integridad y disponibilidad de la información sensible de cara a la protección de datos personales.
Líderes de Proceso	• Tomar conciencia de las Políticas de Seguridad de la Información y garantizar su entendimiento a todo nivel. • Implementar las directrices y lineamientos establecidos desde el Sistema de Gestión de Seguridad de la Información. • Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores relacionados con la operación. • Identificar, evaluar, tratar y monitorear los eventos de riesgos que puedan generar afectaciones moderadas o críticas en la seguridad de la información. • Comunicar y reportar señales de alerta en torno al Sistema de Gestión de Seguridad de la Información.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Todos los Colaboradores	• Ser consciente de su rol dentro del esquema de seguridad de la información, apoyando a los líderes de proceso en la implementación de controles, gestión de activos, gestión de riesgos y demás actividades del sistema. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados. • Comunicar y reportar señales de alerta en torno al Sistema de Gestión de Seguridad de la Información.

8. SANCIONES

Cualquier violación a las Políticas de Seguridad de la Información de JUJU S.A.S. deberá ser tratada de acuerdo con los lineamientos establecidos en el Reglamento Interno de Trabajo y a las normas aplicables.

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

JUJU S.A.S. realizará revisiones periódicas (mínima una vez al año) a los componentes del SGSI, teniendo en cuenta los siguientes aspectos:

- Oportunidades de mejora generadas por auditoría interna y auditoría externa.
- Cambios o actualizaciones metodológicas y normativas.
- Desviaciones resultantes en el análisis de indicadores internos.
- Disposiciones de ley o requerimientos de entes de control.
- Cambios en la estrategia del negocio o proyectos de alto impacto organizacional.
- Cambios en la estructura organizacional.
- Incidentes de Seguridad de la Información.
- Reestructuración de cadenas de suministro.

10. APROBACIÓN A LA POLÍTICA

Esta política será efectiva desde su aprobación por la Alta Dirección, una vez sea revisada por el proceso de Seguridad de la Información y Control Interno.

11. AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES

JUJU S.A.S., en cumplimiento de la normativa vigente en materia de protección de datos personales, informa que los datos personales recolectados en el marco de la presente política serán tratados conforme a los principios de legalidad, confidencialidad, seguridad y finalidad legítima.

Los colaboradores, contratistas y terceros relacionados con JUJU S.A.S. autorizan expresamente el tratamiento de sus datos personales para fines relacionados con la gestión de la seguridad de la información, incluyendo, pero no limitándose a la implementación de controles de acceso, monitoreo de actividades en los sistemas de información, gestión de incidentes de seguridad y cumplimiento de requisitos legales y regulatorios aplicables.

Los titulares de los datos personales podrán ejercer sus derechos de acceso, rectificación, actualización o supresión conforme a lo establecido en la legislación vigente, a través de los canales habilitados por JUJU S.A.S. para la atención de consultas y reclamos en materia de protección de datos personales.