POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

JUJU SAS

TABLA DE CONTENIDO

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

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, 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:** Cumplir los requisitos legales y reglamentarios aplicables relacionados con la seguridad de la información.
- **Objetivo 3:** Estructurar planes de capacitación y sensibilización para el logro de la seguridad de la información.
- **Objetivo 4:** 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 11 principios de seguridad que soportan el SGSI de JUJU SAS:

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

b) JUJU SAS 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.

c) JUJU 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.

d) JUJU SAS protegerá su información de las amenazas originadas por parte del personal.

e) JUJU SAS protegerá la infraestructura tecnológica que soporta sus procesos críticos.

f) JUJU SAS controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

g) JUJU SAS implementará control de acceso a la información, sistemas y recursos de red.

h) JUJU SAS garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

i) JUJU 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.

j) JUJU SAS garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

k) JUJU SAS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de **JUJU SAS** 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 la implementación del SGSI.

Además, la Alta Dirección garantizará y asegurará los recursos adecuados (tecnológicos y talento humano calificado), necesarios 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 organizativos.

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

Seguridad de la información en el desarrollo de soluciones tecnológicas, puesta 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 SAS. 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 SAS, 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 (Recursos económicos, formación y recursos tecnológicos).
Equipo Tecnología	Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Analista de Procesos (Oficial de Seguridad)	• 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 establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad.
Gestión Humana	• Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
	cumplan, además de dar aplicación de la seguridad 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 organización. • Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores relacionados con seguridad de la información de la organización. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Control y Mejora	• Incluir la seguridad de la información, dentro de los planes de auditoría organizacionales. • Apoyar en situaciones de posibles vulneraciones a las políticas de seguridad de la información.
Experiencia de Usuario	Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores relacionados con la operación de la organización.
Líderes de Proceso	Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Todos los empleados	• Apoyar a los líderes de proceso en el desarrollo de tareas como 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.

8. SANCIONES

a. Cualquier violación a las políticas de seguridad de la información de JUJU SAS debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana apoyados en las leyes regulatorias de delitos informáticos de Colombia.

b. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

JUJU SAS indica que realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Para el SGSI, el método establecido es la Auditoría interna que debe realizarse al menos cada año.
- Para los objetivos, el método establecido es el análisis de los indicadores y la frecuencia de análisis, es la descrita para cada uno de ellos.
- Para la seguridad de la información, el método establecido son los seguimientos y monitoreos que se realizan semestralmente, utilizando la lista de chequeo sobre los controles descritos en el "**Anexo A**" de la norma NTC ISO 27001:2013.

10. 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 dan cambios estructurales en la organización (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.