Versión: 1	**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**	

1. OBJETIVOS

Establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la CONEXIONES EMPRESARIALES S.A.S teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la entidad.

1.1. Objetivos Específicos.

* Definir la política de seguridad y privacidad de la información de la empresa CONEXIONES EMPRESARIALES S.A.S
* Definir los lineamientos a ser considerados para diseñar e implementar el Sistema de Gestión de Seguridad de la información alineado con las necesidades, los procesos, los objetivos y la operación de la empresa CONEXIONES EMPRESARIALES S.A.S.
* Dar conformidad y cumplimiento a las leyes, regulaciones y normativas que Se aplican a empresa CONEXIONES EMPRESARIALES S.A.S en el desarrollo de su misión.
* Proteger los activos de información de la empresa CONEXIONES EMPRESARIALES S.A.S
* Mantener un sistema de políticas, manuales, procedimientos y estándares actualizados, a efectos de asegurar su vigencia y un nivel de eficacia, que permitan minimizar el nivel de riesgo de los activos de información de la empresa CONEXIONES EMPRESARIALES S.A.S
* Fortalecer la cultura de seguridad de la información en empleados, terceros y clientes de CONEXIONES EMPRESARIALES S.A.S, mediante la definición de una estrategia de uso y apropiación de la política.
* Garantizar la continuidad de negocio frente a la materialización de incidentes de seguridad basad os en la norma ISO 27035.
* Definir una estrategia de continuidad de los procesos de la entidad frente a incidentes de seguridad de la información.

2. ALCANCE.

La política de Seguridad de la información es aplicable en todo el ciclo el ciclo de vida de los activos de información de CONEXIONES EMPRESARIALES S.A.S, incluyendo creación, distribución, almacenamiento y destrucción. De igual forma para todos los empleados, contratistas y terceros qe desenseñen alguna labor en la entidad. EI alcance abarca desde el enunciado de la política, pasando por los lineamientos para la implementación del Sistema Seguridad y Privacidad de la información, la matriz de riesgo, la definición de los indicadores para el monitoreo de cumplimiento de la política hasta la definición de una estrategia para la adopción de la política en la entidad.

3. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de CONEXIONES EMPRESARIALES S.A.S, 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 las organizaciones y clientes, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

3.1. POLITICA ESPECIFICA

Para CONEXIONES EMPRESARIALES S.A.S, 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 Empresa según como se defina en el alcance, sus empleados, terceros, aprendices, practicantes, proveedores y personal 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, partes interesadas 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 empleados, terceros, practicantes y clientes de CONEXIONES EMPRESARIALES S.A.S
- Garantizar la continuidad del negocio frente a incidentes.
- CONEXIONES EMPRESARIALES S.A.S 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.
- implementar mecanismos en la construcción de la seguridad para ayudarla a permanecer funcional (o resistente) a los ataques.
- Determinar sistemas que protegen la infraestructura tecnológica, los datos y los activos de una organización de las amenazas internas y externas.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de CONEXIONES EMPRESARIALES S.A.S:

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
2. CONEXIONES EMPRESARIALES S.A.S protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
3. CONEXIONES EMPRESARIALES S.A.S 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.
4. CONEXIONES EMPRESARIALES S.A.S protegerá su información de las amenazas originadas por parte del personal.
5. CONEXIONES EMPRESARIALES S.A.S protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. CONEXIONES EMPRESARIALES S.A.S controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. CONEXIONES EMPRESARIALES S.A.S implementará control de acceso a la información, sistemas y recursos de red.
8. CONEXIONES EMPRESARIALES S.A.S garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. CONEXIONES EMPRESARIALES 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.
10. CONEXIONES EMPRESARIALES 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.
11. CONEXIONES EMPRESARIALES S.A.S garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
12. CONEXIONES EMPRESARIALES S.A.S con respecto a la protección de los activos de información (los empleados, 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.

Versión: 1	**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**	

CONEXIONES EMPRESARIALES S.A.S, para asegurar la dirección estratégica de la empresa, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

1. Minimizar el riesgo de los procesos misionales de la entidad.
2. Cumplir con los principios de seguridad de la información.
3. Cumplir con los principios de la función administrativa.
4. Mantener la confianza de los empleados, contratistas y terceros.
5. Apoyar la innovación tecnológica.
6. Implementar el sistema de gestión de seguridad de la información.
7. Proteger los activos de información.
8. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
9. Fortalecer la cultura de seguridad de la información en los empleados, terceros, aprendices, practicantes y clientes del CONEXIONES EMPRESARIALES S.A.S
10. Garantizar la continuidad del negocio frente a incidentes. Alcance/Aplicabilidad
11. Esta política aplica a toda la entidad, sus empleados, contratistas y terceros del CONEXIONES EMPRESARIALES S.A.S y clientes en general. 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 complementarias de seguridad que soportan el SGSI de CONEXIONES EMPRESARIALES S.A.S:

CONEXIONES EMPRESARIALES S.A.S 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.

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
2. CONEXIONES EMPRESARIALES S.A.S protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
3. CONEXIONES EMPRESARIALES S.A.S 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.

4. CONEXIONES EMPRESARIALES S.A.S protegerá su información de las amenazas originadas por parte del personal.
5. CONEXIONES EMPRESARIALES S.A.S protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. CONEXIONES EMPRESARIALES S.A.S controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. CONEXIONES EMPRESARIALES S.A.S implementará control de acceso a la información, sistemas y recursos de red.
8. CONEXIONES EMPRESARIALES S.A.S garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. CONEXIONES EMPRESARIALES 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.
10. CONEXIONES EMPRESARIALES S.A.S garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
11. CONEXIONES EMPRESARIALES S.A.S 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 Empresa, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

4. Copias de respaldo de información (Backup):

Se debe contar con un sistema automático para la recolección de copias de respaldo.

Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.

Los medios magnéticos que contienen información deben ser almacenados en lugares triásicamente seguros.

Los usuarios responsables por respaldar la información también son responsables de facilitar la oportuna restauración de la información.

Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.

Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.

Para responder adecuadamente a una contingencia, los respaldos de la información se deben almacenar en sitios externos.

Cualquier medio magnético que contenga información clasificada como restringida o confidencial, debe estar claramente identificada.

AI enviar información clasificada como restringida o confidencial a terceros se debe exigir un acuse de recibo.

Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos o destruidos físicamente para que la información no pueda ser recuperada.

Es responsabilidad de los Administradores de las Plataformas, mantener respaldo de la configuración del sistema operativo y de los servicios que estas proveen.

5. Acuerdos de Confidencialidad.

Todos los empleados, contratistas, proveedores y terceros, que deban realizar labores dentro o para la empresa CONEXIONES EMPRESARIALES S.A.S, ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información.

Se debe revisar a intervalos de tiempo regulares el texto, de los acuerdos de confidencialidad, avalando que reflejan las necesidades de la empresa para la protección y seguridad de la información.

6. Revisión del SGSI.

La Alta dirección y el Comité de Seguridad de la información, debe revisar el Sistema de Gestión de Seguridad de la información (SGSI) de CONEXIONES EMPRESARIALES S.A.S a intervalos planificados, para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del SGSI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben Llevar registros. Esta revisión cumplirá con los lineamientos establecidos en el procedimiento de revisión del Sistema Integrado de Gestión.

De la misma manera, las políticas de seguridad de la información, normas, procedimientos, estándares, controles, formatos y procedimientos, deben ser revisados y actualizados sistemáticamente, de forma periódica y planificada, mínimo una vez por año o cada vez que ocurra un cambio sustancial en los activos de información, por parte del Oficial de seguridad de la información y por el Comité de Seguridad de la información o en su defecto si se requiere una revisión independiente; se debe realizar por un organismo, empresa o consultor externo especializado, en cuyo caso debe seguir los lineamientos de la norma NTC-ISO ser realizada por

alguien con las credenciales de AUDITOR Líder (Lead Auditor) 27001 vigentes o Auditor CISA preferiblemente.

REALIZO:	REVISO:	APROBO:
Ing. Eliana Barreiro Piña Coordinador SGI	LAIDY SEGURA Coordinador de procesos	Luis Alejandro Rodriguez Ariza Gerente