1. PROPOSITO

Conexred, reconoce la importancia de identificar y proteger la información que recibe, produce, almacena, transmite y comparte por cualquier medio, incluyendo los medios digitales, para ello ha definido la siguiente política general de seguridad de la información, ciberseguridad y protección de la privacidad que se construye a través de la triada de seguridad de la información (confidencialidad, integridad y disponibilidad).

La tecnología y su continuo avance es de gran importancia para la evolución de la compañía y conseguir sus objetivos estratégicos, por lo que el correcto uso de la información, los recursos y su seguridad deben ser gestionados, conocidos y cumplidos por todos sus colaboradores, contratistas, proveedores y personas que hagan uso de los activos de información de Conexred.

2. ALCANCE

La Política general de Seguridad de la Información, ciberseguridad y protección de la privacidad de Conexred cubre todos los activos de información, haciéndose extensiva a colaboradores, clientes, contratistas, practicantes, temporales, proveedores de servicios y terceros relacionados, que interactúen de cualquier manera con la información y los activos de información de la entidad.

3. GLOSARIO

- **ACTIVO DE INFORMACIÓN:** Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...), que tenga valor para la organización. ISO/IEC 27000:2018.

- **AMENAZA:** Causa potencial de un incidente no deseado, que puede ocasionar daños a un sistema u organización. ISO/IEC 27000:2018.

- **CIBERESPACIO:** Es un entorno complejo que consta de interacciones entre personas, software y servicios destinados a la distribución mundial de información y comunicación. ISO/IEC 27032:2012.

- **CIBERSEGURIDAD:** Es la disciplina que se encarga de aplicar diferentes medidas de seguridad (conjunto de herramientas, conceptos de seguridad, acciones, formación, directrices, prácticas idóneas, seguros, tecnología y métodos de riesgos) con el fin de proteger los activos digitales, desde las redes hasta el hardware y la información que es procesada, almacenada o transportada por sistemas de información interconectados, de las amenazas provenientes del ciberespacio dentro de la organización.

- **CONEXRED S.A.S:** Es la empresa identificada con NIT 830.513.238 – 9; para efectos de esta política cuando se haga referencia a Conexred S.A.S. se entenderá que se hace referencia y/o se incluyen también sus matrices, subordinadas, filiales,

además de las empresas VECI S.A.S, SERVIPUNTO – SERVICIOS DE INFORMACIÓN S.A.S. y cualquier otra que se llegare a determinar.

- **CSIRT:** Tradicionalmente se define un CSIRT como un equipo o una entidad dentro de un organismo que ofrece servicios y soporte a un grupo en particular (comunidad objetivo) con la finalidad de prevenir, gestionar y responder a incidentes de seguridad de la información. Estos equipos suelen estar conformados por especialistas multidisciplinarios que actúan según procedimientos y políticas predefinidas, de manera que respondan, en forma rápida y efectiva, a incidentes de seguridad, además de coadyuvar a mitigar el riesgo de los ataques cibernéticos.

- **INCIDENTE DE SEGURIDAD:** Toda acción, premeditada o no, que indica una violación confirmada a la Política de Seguridad de la Información o que compromete la confidencialidad, integridad, disponibilidad de los activos de información o la información misma. Corresponde a un Evento de Seguridad materializado.

- **PRIVACIDAD DE DATOS:** Se refiere a la protección de la información personal de los usuarios contra accesos y tratamientos no autorizados. ISO/IEC 27701:2019.

- **RIESGO:** Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos en un activo, un dominio o en toda la organización. Está medido en términos de consecuencias y probabilidad de ocurrencia.

- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas. ISO/IEC 27000:2018.

- **SGSI:** Sistema de Gestión de Seguridad de la Información. Conjunto de políticas, procedimientos y controles para gestionar los riesgos relacionados con la seguridad de la información.

- **VULNERABILIDAD:** Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución. Ejemplos: Deficiente control de accesos, poco control de versiones de software, entre otros.

4. RESPONSABILIDAD Y AUTORIDAD

El CEO (Chief Executive Officer) de Conexred, asigna las funciones relativas a la Seguridad de la Información de la compañía al Director de Seguridad y Ciberseguridad, quien tendrá a cargo las funciones relativas a este rol, lo cual incluye la supervisión de todos los aspectos inherentes tratados en la presente Política.

Se asigna al Comité de Seguridad de la Información o ente que tome sus veces, al cual debe pertenecer el responsable de la Seguridad de la Información, la función de

supervisar el control y cumplimiento de la Política general de Seguridad de la Información, y Ciberseguridad y protección de la privacidad, así como de garantizar que las políticas específicas, procesos, procedimientos y/o controles que se deriven de ésta, estén alineados con la misma, con las estrategias y modelos del negocio.

Todo el personal, sea cual fuere su nivel jerárquico, es responsable de la implementación y cumplimiento de las políticas de Seguridad de la Información dentro y fuera de sus dependencias.

La violación a la Política general de Seguridad de la Información, ciberseguridad y protección de la privacidad será motivo para adelantar acciones disciplinarias, civiles y penales según aplique. Conexred también llevará a cabo acciones judiciales donde lo considere apropiado.

5. NORMATIVIDAD

- **Ley 23 de 1982** de Propiedad Intelectual - Derechos de Autor
- **Ley 527 de 1999** Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 1032 de 2006** por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales,
- **Ley 1273 de 2009** "Delitos Informáticos" protección de la información y los datos.
- **Ley 1266 de 2008** Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1581 de 2012** "Protección de Datos Personales".
- **Decreto 1377 de 2013.** Reglamenta parcialmente la Ley 1581 de 2012, que establece el Régimen General de Protección de Datos Personales en Colombia.
- **Ley 1341 de 2009** "Tecnologías de la Información y aplicación de seguridad".
- **Constitución Política de Colombia** Artículos 15, 20, 23, 61, 74, entre otros. Por ejemplo, Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

El CEO de Conexred entiende que la información es uno de sus activos más valiosos y que por la importancia de ésta se requiere una adecuada gestión de seguridad sobre la misma, con base en ello, se ha comprometido con la implementación, operación y mejora continua de un SGSI alineado a los estándares internacionales, las mejores prácticas de la industria y el sector, buscando establecer un marco de confianza en el ejercicio de sus deberes con los involucrados. Todo, enmarcado en el estricto

cumplimiento de las leyes locales y en concordancia con la misión, visión, estrategias y necesidades de la compañía.

Para Conexred, la protección y el buen uso de los activos de Información, el crear una cultura de seguridad de la información y una debida atención y tratamiento de los incidentes de seguridad busca la disminución del impacto generado por amenazas y riesgos a los que la información está expuesta, fomentando el compromiso de mantener un nivel de atención que permita responder por la integridad, confidencialidad y disponibilidad de la misma protegiendo y asegurando en el ciberespacio y de manera física los datos, sistemas y aplicaciones que son esenciales para la operación de la Entidad y en apoyo al espíritu de innovación de la compañía.

Esta política será revisada con una periodicidad mínima anual y sus cambios deben ser aprobados por el CEO.

7. OBJETIVOS

1. Implementar y mantener el **SGSI** ajustado a las necesidades y dimensión de la organización promoviendo la mejora continua.

2. Proteger los activos de información, especialmente los más críticos de acuerdo con el inventario de activos de información.

3. Identificar, evaluar y mitigar los riesgos asociados con la seguridad de la información, asegurando que los controles adecuados estén implementados de forma correcta para proteger los activos de información de la organización.

4. Promover la conciencia y la capacitación en seguridad de la información y protección de la privacidad entre los empleados, contratistas y otras partes interesadas, para que puedan comprender los riesgos y desempeñar un papel activo en la protección de los activos de información de la organización.

5. Asistir en materia de seguridad de la información todos los proyectos de innovación tecnológica.

6. Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en materia de privacidad y seguridad de la información.

8. CONTROL DE VERSIONES

VERSIÓN	FECHA	DESCRIPCIÓN	COLABORADOR QUE ACTUALIZA
001	11/03/2014	Creación de la Política	David Ávila
002	16/04/2016	Actualización Política orientada ISO 27000:2013	Yamile Rocha

003	01/12/2017	Actualización Formato, actualización alcance, actualización periodicidad	Paola Castillo
004	03/01/2019	Actualización Cargos, periodicidad cambio de contraseñas	Paola Castillo
005	06/03/2020	Actualización responsabilidades frente a los activos, adición no repudio, actualización general, cambio codificación.	Paola Castillo
006	01/06/2021	Ajustes glosario, Adición Normatividad, Ajustes objetivos política general, adición información interna y no clasificada, ajustes en control de acceso frente a carpetas compartidas, ajustes restricción de acceso a la información, ajustes accesos código fuentes.	Vanessa González
007	11/02/2022	Actualización y separación de la política general del SGSI	Vanessa González
008	10/04/2023	Actualización del glosario, inclusión de Ciberseguridad en el documento, ajuste en la periodicidad de revisión del documento, cambio en el tipo de etiquetado del documento.	Vanessa González
009	30/07/2024	Se actualizan los Ítems #1 Introducción ,#2 Alcance , #3 Glosario, #4 Responsabilidad y autoridad, además del #6 Objetivos (numerales 2,3,4 y 5).	Stiven Sánchez
010	06/05/2025	Se actualiza el nombre de la política a "Política general de Seguridad de la Información, ciberseguridad y protección de la privacidad" Se actualizan los ítems 1. Propósito, 2. Alcance y 3. Glosario En el ítem #4 Responsabilidad y autoridad – Se actualiza el cargo del responsable a "Director de Seguridad y Ciberseguridad"	Diego Gómez

9. REVISIÓN Y APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ
**** El documento que contiene estas 3 firmas se puede encontrar en el sistema gestión documental de Puntored (Conexred S.A.S.) bajo el código CMGRI-SARO-POL-013 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD****		
COORDINADOR DE SEGURIDAD DE LA INFORMACIÓN	**DIRECTOR DE SEGURIDAD Y CIBERSEGURIDAD**	**CEO**
Diego Gómez	Stiven Sánchez	Andrés Albán