DOCUMENTO GENERAL

Política de Ciberseguridad

Código: SI-DC-13

Versión: 02

TERMINOS DE CONFIDENCIALIDAD

Este documento es resultado del trabajo desarrollado por el área de Seguridad de la Información del Grupo Empresarial en Línea S.A y para uso exclusivo del Grupo Empresarial en Línea S.A. Por razones de Confidencialidad de la información, las ideas, conceptos, definiciones, aplicaciones, planes de trabajo y en general las soluciones contenidas en esta línea base de seguridad de la información, no debe ser revelado, usado, duplicado o publicado total o parcialmente, fuera de la compañía u organización, sin una autorización expresa escrita del Grupo Empresarial en Línea S.A.

Contenido

1. PROPÓSITO

Presentar en forma clara y coherente un conjunto de directrices que conforman la política de Ciberseguridad del Grupo Empresarial en Línea S.A, estableciendo medidas organizacionales, tecnológicas, físicas y legales necesarias para proteger los activos de información de la compañía.

2. ALCANCE

La presente política es aplicable para todos los aspectos administrativos, operativos y de control, debe ser aplicada por los directivos, funcionarios, contratistas, clientes, socios estratégicos y terceros que presten sus servicios o tengan algún tipo de relación con las operaciones de la compañía.

3. DEFINICIONES

A continuación, se presentan las principales definiciones aplicables para la correcta interpretación de la presente política del SGSI.

- **ACTIVO DE INFORMACIÓN:** Cualquier cosa que tenga un valor de importancia relevante para los procesos de la organización. Entre los activos de información más relevantes de una organización se encuentra hardware, software, documentos electrónicos o físicos, infraestructura, servicios, personal, entre otros. El término Activo es sinónimo de Activo de Información.
- **AMENAZA:** Es una fuente generadora de eventos o acciones que puede producir o causar un daño representativo al activo de información, generando un factor o escenario de riesgo que originaría a la organización pérdidas por riesgo de seguridad de la información. La amenaza es un contexto de seguridad de la información que se manifiesta a través de actos deliberados, intencionados o impredecibles y que pueden ser provocados por las personas, la tecnología, la infraestructura, acontecimientos externos entre otros.
- **ACUERDO DE CONFIDENCIALIDAD:** Es un convenio que genera obligaciones a una o a ambas partes que intervienen, con respecto al uso, manejo y divulgación de la información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la misma, como parte de una relación contractual o comercial.
- **CIBERESPACIO:** Entorno complejo que resulta de la interacción de las personas, el software y los servicios a través de internet, por medio de dispositivos tecnológicos y redes conectados al mismo, que no existe en forma física alguna.
- **CIBERSEGURIDAD:** La ciberseguridad o seguridad digital busca proteger la información digital que se procesa en los sistemas interconectados a través de la internet.
- **CISO:** El CISO (Chief Information Security Officer) es el director de seguridad de la información. Básicamente es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio.
- **CONFIDENCIALIDAD:** Propiedad de salvaguardar el activo de información de personas, individuos, procesos o entidades no autorizados.
- **CONTROLES:** Medidas de protección o salvaguardas dispuestas para reducir el nivel de riesgo. Las cuales pueden ser políticas, procedimientos, directrices, prácticas, estructuras de la organización, soluciones tecnológicas, entre otras.
- **CUSTODIO:** Se refiere al responsable de la custodia o protección del activo de información utilizado para el desarrollo de las operaciones del negocio. El custodio tiene la misión de preservar la seguridad del mismo; por lo tanto, el propietario de la información tiene el rol de custodio del activo de información a cargo.
- **DATO PERSONAL:** Cualquier pieza de información vinculada a una o varias personas determinadas o que pueden asociarse con una persona natural o jurídica. Los datos personales pueden ser públicos, semiprivados y privados o sensibles.

- **DATO PÚBLICO:** Son aquellos datos que las normas y la Constitución han determinado expresamente como públicos, cuya recolección y tratamiento, no requiere autorización del titular de la información.
- **DATO SEMIPRIVADO:** Es el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios. Para su tratamiento se requiere la autorización expresa del titular de la información y deben ser tratados conforme a los fines y propósitos de la autorización impartida por su titular. (Ej. Dato financiero y crediticio, Dirección, teléfono, nivel escolaridad).
- **DATO PRIVADO O SENSIBLE:** Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular. No puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular y este se encuentre incapacitado, o en los casos que haya sido autorizada expresamente. (Ej. Origen racial o étnico, orientación política, convicciones religiosas, datos biométricos, relativos a la salud, orientación sexual).
- **DISPONIBILIDAD:** Propiedad de garantizar que el activo de información sea accesible y utilizable en el momento que se requiera, por parte de las personas, procesos o entidades autorizadas.
- **DUEÑO DEL RIESGO:** Responsable de hacer seguimiento a la mitigación de los riesgos a los que están expuestos los activos de información de sus procesos.
- **EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** Es la ocurrencia identificada de un estado del activo de información (sistema, servicio, red, etc.) que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles existentes, o una situación desconocida que puede ser pertinente para la seguridad (ISO/IEC 27000).
- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Se define como un evento o una serie de eventos indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar las propiedades de la información "Confidencialidad, Integridad y Disponibilidad" (ISO/IEC 27000).
- **INFORMACIÓN:** Conjunto de datos ordenados con el objetivo específico de generar conocimiento. Tipo de activo de información que se puede materializar en diferentes formas. La información puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada. La información electrónica, siempre se encuentra asociada a un activo de información determinado.

- **INFORMACIÓN PÚBLICA:** Es aquella información que ha sido declarada de conocimiento público por disposición de los dueños de procesos del Grupo Empresarial en Línea S.A, obligación contractual, ley o norma jurídica, y por tanto puede ser

publicada o entregada sin restricciones, sin implicar daños a terceros ni a Grupo Empresarial en Línea S.A.

- **INFORMACIÓN CONFIDENCIAL:** Es aquella información que Grupo Empresarial en Línea S.A utiliza para la ejecución de su objeto económico o social, y debe ser accedida solo por un grupo limitado de usuarios o personas autorizados. La divulgación de esta clase de información sin previa autorización de su propietario expone en riesgos extremos al Grupo Empresarial en Línea S.A, sus clientes, proveedores y terceros.
- **INFORMACIÓN USO INTERNO:** Es aquella información que Grupo Empresarial en Línea S.A utiliza para la ejecución de su objeto económico o social, y puede ser accedida por usuarios o personas autorizadas, para el desarrollo exclusivo de sus actividades diarias en cumplimiento de las funciones de su cargo o labor contractual acordado con la organización. La divulgación de esta clase de información al interior de las áreas del Grupo Empresarial en Línea S.A, está sujeta al criterio de su propietario. Su divulgación sin previa autorización del propietario expone en riesgos leves o moderados al Grupo Empresarial en Línea S.A.
- **INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo del activo de información.
- **MEJORA DEL SGSI:** Mejora continua, acciones correctivas y acciones preventivas requeridas con el fin de minimizar impactos a todo nivel para la organización.
- **PARTES INTERESADAS:** Hace referencia a los empleados, clientes, usuarios, proveedores, socios estratégicos, accionistas, grupos u organizaciones que forman parte activa o pasiva de la organización.
- **PROTEGER LA ORGANIZACIÓN:** Reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste se materializa.
- **PROCESAMIENTO DE INFORMACIÓN:** Es la capacidad que tiene un sistema de información de efectuar cálculos con base a una secuencia de operaciones preestablecidas, permitiendo la transformación de datos fuentes en información para ser utilizada en la toma de decisiones.
- **RIESGO:** Se entiende por riesgo, la posibilidad de incurrir en pérdidas económicas, operativas, legales o de imagen para la organización por deficiencias, fallas o al no adecuado uso y/o manejo del activo de información, a causa de amenazas o vulnerabilidades que le altere su correcto funcionamiento u operatividad.
- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad y disponibilidad del activo de información, adicionalmente se deben preservar otros criterios o propiedades tales como la autenticidad, no repudio, confiablidad, propiedad y/o responsabilidad, entre otros.
- **SGSI:** Sistema de gestión de Seguridad de la Información, fundamentado en la orientación al riesgo del negocio a través de los procesos críticos y activos de información para establecer, implementar, operar, monitorear, revisar, mantener y

mejorar la seguridad de la información en la organización tomando como guía la norma ISO/IEC 27001.

- **TRATAMIENTO DEL RIESGO:** Proceso de selección e implementación de controles o acciones para ajustar el nivel de riesgo del activo a los niveles aceptables para la organización.
- **VULNERABILIDAD:** Es la debilidad o incapacidad de resistencia de un activo de información frente a una amenaza.
- **SISTEMA DE INFORMACIÓN:** Disposición de personas, actividades o procedimientos y recursos tecnológicos integrados entre sí, para apoyar y mejorar las operaciones diarias de la organización, con la finalidad de satisfacer las necesidades de información a nivel general y facilitar la toma de decisiones por parte de los directivos de la organización. Los ejemplos aplicados más representativos: sistemas de automatización de oficina, sistemas de procesamiento de transacciones y sistemas de información de gestión.

4. POLÍTICA DE CIBERSEGURIDAD

INTRODUCCIÓN

La protección de la información es fundamental para salvaguardar los intereses de la compañía en el ámbito físico como en el digital, en pro de prevenir impactos que afecten o generen pérdidas a la organización y partes interesadas; por lo cual identificamos, controlamos y monitoreamos toda evento que tenga una probabilidad potencial de poner en riesgo la confidencialidad, integridad y disponibilidad de la información, en este sentido la alta dirección del Grupo Empresarial en Línea S.A establece la política de Ciberseguridad, la cual se encuentra fundamentada en los marcos de referencia ISO 27001 e ISO 27032.

ALCANCE

Protección de los activos de información de la organización a nivel físico, digital, aplicaciones y plataformas tecnológicas tanto en la red interna como las que interactúan con internet.

PRINCIPIOS

Preservar la Confidencialidad, Integridad y Disponibilidad" de la información de la organización y de las partes interesadas que sea objeto de tratamiento, tanto en la red interna como en el ciberespacio.

OBJETIVOS

Los objetivos de la presente política están orientados a salvaguardar los activos de información en el entorno físico, de red local y los que se encuentran interconectados a través de internet.

- Asegurar la Confidencialidad, Integridad y Disponibilidad de los activos de información a través de la ejecución de políticas, gestión de riesgo y aseguramiento informático de plataformas IT.
- Definir e implementar controles informáticos robustos para mitigar ataques cibernéticos conocidos, a los que se encuentran expuestas las aplicaciones y plataformas IT de la organización.
- Planear y ejecutar un programa de auditoría para verificar la adecuada implementación de los controles de seguridad y ciberseguridad en las plataformas IT.
- Gestionar la vulnerabilidad técnica y tratar el riesgo asociado a través de los análisis de vulnerabilidades sobre las plataformas IT.
- Establecer contactos de la industria de la ciberseguridad para hacer frente a ataques de día cero.

RESPONSABILIDADES

Las responsabilidades en la organización, frente a la seguridad de la información y la ciberseguridad se encuentra jerárquicamente establecidas así:

- Alta dirección, revisa y aprueba de forma periódica la eficacia y aplicabilidad de la política de acuerdo con la dinámica del negocio.
- CISO, diseña y gestiona la política de Ciberseguridad y las políticas relacionadas.
- CISO, revisa y evalúa la aplicación de procedimientos de seguridad de la información y controles de ciberseguridad para asegurar la adecuada ejecución de las políticas relacionadas.

POLÍTICAS RELACIONADAS

La Política de Ciberseguridad se encuentra soportada sobre diferentes políticas de tipo procedimental y de tipo tecnológico, las cuales se encuentran relacionadas en el manual **SI-M-02 Políticas de SI & Ciberseguridad,** que tienen como propósito reglamentar el cumplimiento de los lineamientos de la política integral y la política de ciberseguridad.

- Política Organización interna Roles y responsabilidades
- Política separación de deberes
- Política autoridades y grupos de interés
- Política Seguridad de la Información en la gestión de proyectos

- Política para dispositivos móviles, medios removibles y teletrabajo
- Política de Seguridad para los recursos humanos
- Política de Gestión de Activos
- Política de Gestión de Medios
- Política de Control de Acceso a aplicaciones y servicios de red
- Política de controles criptográficos
- Política de Seguridad Física y del entorno
- Escritorio y pantalla limpia
- Política de Seguridad en las operaciones
- Política Copias de Respaldo
- Política para la seguridad de redes y los servicios de red
- Política de Transferencia de Información
- Política para la adquisición, y mantenimiento de sistemas de información
- Política de Desarrollo Seguro
- Política de Relación con Proveedores
- Política para la Gestión de Incidentes de Seguridad de la Información
- Política de Continuidad de la Seguridad de la Información
- Política de Cumplimiento
- Política para la protección de la propiedad intelectual

CENTRO EMPRESARIAL ARRECIFE
Av - El Dorado No. 69D - 91 Piso 7
PBX 3 78 8888 www. pagatodo.com.co