POLÍTICA SEGURIDAD DE LA INFORMACIÓN
GRUPO EMPRESARIAL COLOMBINA

OBJETIVO

Establecer la política general de seguridad de la información para las sociedades del Grupo Empresarial Colombina, con el fin de cumplir con los requisitos definidos en el sistema de gestión de seguridad y las cuales apoyarán la implementación de controles que permitan preservar la confidencialidad, integridad y disponibilidad de la información en las Compañías.

ALCANCE

La presente política debe ser cumplida por los directivos(as), colaboradores(as) y proveedores(as) que desempeñen actividades dentro del área de Tecnología Informática.

CONDICIONES

El propósito de este documento es dar a conocer a los colaboradores(as) del Grupo Empresarial Colombina, la Política de Seguridad de la Información establecida para la protección de la información de la organización.

En el presente documento se incluyen los aspectos que deben tenerse en cuenta por parte de todos los colaboradores(as) para que la información sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones en la organización (Confidencialidad); que esté protegida contra modificaciones no autorizadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad), que sea utilizada para los propósitos que fue obtenida (Privacidad) y que se deje el rastro de los eventos que ocurren al tener acceso a la información (Auditabilidad).

Por lo tanto, los colaboradores(as) del Grupo Empresarial Colombina, deben actuar teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en cada Política de Seguridad particular, estándares y procedimientos que hagan parte de la seguridad de la información; en el entendido que la alta gerencia tiene el firme propósito de apoyar todas las actividades necesarias para alcanzar las metas y principios de seguridad de la información, de acuerdo con las responsabilidades asignadas dentro de los Roles y Responsabilidades definidos en relación con este tema.

Este documento describe el objetivo, alcance, principios fundamentales, roles y responsabilidades, así mismo esta política relaciona de forma general las Políticas de seguridad individuales, que especifican la postura aceptada por el Grupo Empresarial Colombina, en el manejo de su información y las acciones que deben ser tomadas para lograr los objetivos de la presente Política. Estas Política individuales son desarrolladas con mayor amplitud en el documento “Manual de Políticas de Seguridad Informática”

PASOS A SEGUIR

DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Grupo Empresarial Colombina, aplica estrategias de seguridad de la información teniendo en cuenta el contexto organizacional y la gestión de riesgos, con el fin de asegurar el cumplimiento de los requisitos legales, reglamentarios, contractuales, normativos, tecnológicos, de sus partes interesadas.

Así mismo, es consecuente que la información es un activo vital para la organización, razón por la cual establece y mantiene la gestión en seguridad de la información encaminados a identificar y tratar oportunamente los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, los datos personales y sus contenedores, así como protegerlos de posibles ataques maliciosos o ciberataques, brindando seguridad y confianza, con el fin satisfacer las necesidades de las partes interesadas en la prestación de los servicios.

Teniendo en cuenta los objetivos de seguridad de la información establecidos en el presente documento, las sociedades del Grupo Empresarial Colombina, dentro del SGSI, desarrollarán actividades que permitan el cumplimiento, monitoreo y actualización de estos.

Compromiso de la Alta Gerencia

Como parte del compromiso, la alta gerencia asigna los recursos necesarios (humanos, tecnológicos y financieros) y promueve la sensibilización, la formación y la toma de conciencia para la generación de cultura en seguridad para el mejoramiento continuo.

Finalmente, para el cumplimiento de esta política se apoya en el Manual de Políticas de Seguridad Informática, la política de protección de datos personales y un conjunto controles procedimentales y tecnológicos.

Actualizaciones a la Política de Seguridad de la Información

El área de Tecnología Informática establece una revisión anual de las políticas de seguridad de la información y su actualización dependerá factores internos y externos. Los factores internos pueden ser: necesidades de las sociedades en materia de seguridad de la información, cambios estructurales. Los factores externos pueden ser: cambios o actualizaciones el estándar ISO/IEC 27001:2013 y/o en la Legislación Colombiana en temas relacionados con la privacidad de los datos o de la seguridad de la información, regulación del mercado, tecnología u otros que apliquen.

Excepciones

Las excepciones a estas políticas deberán ser aprobadas por el responsable de Seguridad de la información, Jefatura o Líder de Tecnología Informática de cada una de las sociedades del Grupo Empresarial Colombina o la persona que él/ella designe.

ACEPTACIÓN DE LA POLÍTICA

Debe considerarse que, por el uso de cualquier activo de información de las sociedades del Grupo Empresarial Colombina, es de carácter mandatorio respetar y aceptar los términos y condiciones en esta política. Se puede dar el caso, debido a disposiciones de ley, se le solicite firmar un acuerdo de confidencialidad en el cual se comprometa a seguir las reglas y condiciones del uso de cualquier activo de la información. En todo momento, deberá ajustarse a todos los requerimientos de licenciamiento y acuerdos de confidencialidad solicitados por las sociedades.

PRINCIPIOS FUNDAMENTALES

El Grupo Empresarial Colombina ha establecido como fundamentales los siguientes principios que soportan la Política de Seguridad de la Información:

a. La Información es uno de los activos más importantes del Grupo Empresarial Colombina y por lo tanto debe ser utilizada acorde con los requerimientos de la organización y conservando los criterios de seguridad (Confidencialidad, Integridad y Disponibilidad).

b. La confidencialidad de la información en la organización, así como aquella perteneciente a terceros, debe ser mantenida, independientemente del medio o formato donde se encuentre.

c. La Información de la organización debe ser preservada en su integridad, independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.

d. La Información de la organización debe estar disponible cuando sea requerida y por quienes tengan autorización de utilizarla; asimismo, presentarse de forma oportuna cuando por requisitos legales y reglamentarios así se requiera.

e. La información de la organización que sea almacenada, recolectada y/o procesada a través de tecnologías que utilicen componentes de inteligencia artificial (IA), minería de datos y demás tecnologías emergentes, deberán ser protegidos contra posibles riesgos y vulnerabilidades a las que estén expuestos, garantizando así la exactitud, veracidad y completitud de los datos.

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

El Grupo Empresarial Colombina, consciente de la necesidad de cumplir con los requerimientos que demandan sus partes interesadas y los requisitos legales y normativos, establece un marco de referencia de gestión para iniciar, controlar la implementación y la operación de la seguridad de la información dentro de la organización. Con base en lo anterior y teniendo en cuenta la política de seguridad de la información Grupo Empresarial Colombina ha definido los siguientes objetivos de seguridad de la información:

a. Garantizar el adecuado funcionamiento de todos los sistemas de información de la organización y el uso de tecnologías emergentes (inteligencia artificial, minería de datos, analítica de datos, etc.) en el desarrollo de los procesos, apoyados en la implementación de una estrategia de seguridad de la información y ciberseguridad.

b. Garantizar que los riesgos de seguridad de la información correspondientes al alcance del SGSI de Colombina sean identificados, valorados y tratados bajo los criterios de aceptación del riesgo permitidos por la Gerencia.

c. Dar cumplimiento a los requerimientos legales, regulatorios, contractuales apoyados en la estrategia de seguridad de la información.

d. Crear cultura y conciencia de la importancia de la seguridad de la información, en las labores ejecutadas por todos los colaboradores(as) de la organización.

ROLES Y RESPONSABILIDADES

Todos los roles y responsabilidades para la seguridad de la información están definidos en el manual de "Roles y Responsabilidades de Seguridad de la Información". La seguridad de la información debe involucrarse en la organización a través de políticas o creación de procedimientos, estándares, formatos e instructivos.

POLÍTICAS INDIVIDUALES DE SEGURIDAD

Las políticas individuales para la seguridad de la información están definidas en el manual de "Manual de Políticas de Seguridad de la Información", publicado para consulta en el repositorio interno.

REFERENCIAS DOCUMENTALES

ISO IEC 27001

ANEXOS

Manual de políticas de seguridad de la información

Manual de roles y responsabilidades de seguridad de la información

DEFINICIONES

Activo de información: Todo aquello que posee valor para la organización y por tanto debe protegerse, como, por ejemplo: Información física y digital, software, hardware, servicios y/o personas.

Confidencialidad: Característica que indica que el activo de información solo sea accedido por el personal, procesos, sistemas o entidades que se encuentran autorizadas.

Disponibilidad: Característica que indica que el activo de información sea oportuno, es decir, que pueda ser consultado y usado por la persona, entidad o proceso autorizados cuando sea requerido.

Integridad: Característica que garantiza la precisión, calidad, veracidad y completitud del activo de información.

Inteligencia Artificial: Campo de la informática, que abarca el aprendizaje automático y el aprendizaje profundo, esto implica el desarrollo de algoritmos de IA, modelados a partir de los procesos de toma de decisiones del cerebro humano, que pueden "aprender" de los datos disponibles y realizar clasificaciones o predicciones cada vez más precisas con el tiempo, esto permite que las computadoras simulen la inteligencia y las capacidades humanas de resolución de problemas.

Dispositivos Móviles: Aparatos de tamaño reducido, que generalmente poseen las siguientes características: capacidades especiales de procesamiento, conexión permanente o intermitente a una red, memoria limitada, tanto su posesión como operación se asocia al uso individual de una persona, quien puede configurarlo a su gusto.

Aliados: Empresas con las cuales se halla firmado un contrato de alianza.

Sistema de Gestión de la Seguridad de la Información: Conjunto de procesos y procedimientos encaminados a la planeación, construcción, monitoreo y mejora continua de la seguridad de la información de una organización.