POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

En Grupo SURA la información es considerada un activo estratégico para el ejercicio de nuestros negocios. Por esto, resulta relevante reconocer que su adecuado tratamiento supone grandes retos y tareas que exigen una responsable planeación, organización, gestión, conservación y protección.

Para la organización, la protección, calidad, confidencialidad, integridad y disponibilidad de la información, es un asunto de relevancia, que permite mantener la confianza de la Compañía con sus grupos de interés y minimizar los riesgos financieros, legales, operativos y reputacionales, que están asociados al manejo de la información.

Las presentes instrucciones son complementarias a la normatividad nacional e internacional aplicable y establece los lineamientos generales y específicos que definen el marco de actuación respecto a la Seguridad de la Información y Ciberseguridad en la Compañía, conformado por manuales, procesos, procedimientos, instructivos y estándares, entre otros documentos vinculantes que la complementan.

Alcance y Marco de Aplicación

Los lineamientos contenidos en el presente documento aplicarán a los Miembros de la Junta Directiva, Alta Gerencia y colaboradores de Grupo SURA (en adelante, "la Compañía"). Esta política también se hará extensiva a proveedores que accedan, conserven y gestionen información de la Compañía.

Objetivos generales

- Desarrollar e implementar un modelo de seguridad de la información que permita a la Compañía gestionar los riesgos relacionados con el manejo de la información y cumplir con todos los requerimientos legales y contractuales en dicha materia.

- Definir e implementar las mejores prácticas para proteger de manera adecuada, la información que recibe, genera, procesa y almacena la Compañía en los diferentes medios (físicos o digitales) en que se encuentre.

- Incentivar una cultura organizacional que promueva la gestión de riesgos de seguridad de la información y ciberseguridad.

Lineamientos generales

- La Compañía, a través de la Vicepresidencia de Asuntos Corporativos, definirá la estructura y garantizará los recursos necesarios para la implementación de un modelo de Gobierno de la Información, que permita la aplicación de los mecanismos definidos para la identificación, análisis, evaluación, gestión, monitoreo y reporte de los riesgos asociados a la seguridad de la información y ciberseguridad.

- La Alta Gerencia es la encargada de promover los lineamientos para la gestión de los riesgos de seguridad de la información y ciberseguridad, incorporándolos en los planes estratégicos de la Compañía, garantizando la adopción de un modelo de Gobierno de la Información y la disponibilidad de los recursos que se requieran para tal efecto.

- Se deberán establecer procesos y procedimientos para la adecuada gestión del riesgo de seguridad de la información y ciberseguridad, contemplando las etapas de prevención, protección, detección, respuesta, comunicación, recuperación y aprendizaje.

- Los colaboradores y proveedores que acceden y/o gestionen la información de la Compañía son responsables de identificar, valorar y clasificar la información, así como garantizar su protección y conservación, aplicando los controles necesarios para proteger la información de todos los riesgos de seguridad y ciberseguridad a los que pueda estar expuesta.

- Existirá un Comité Seguridad de la Información y Ciberseguridad responsable de la estrategia y mejora continua del Modelo de Gobierno de Información, el cual estará conformado por las áreas de Servicios Internos y Compartidos, Asuntos Legales Corporativos, Auditoría y Riesgos Corporativos.

- El modelo de Gobierno de la Información que se defina e implemente, deberá responder a las necesidades particulares de la Compañía y será revisado y actualizado por parte del Comité de Seguridad de la Información y Ciberseguridad, como mínimo cada año o cada que aparezcan circunstancias en el entorno que por su naturaleza ameriten revisar el modelo.

- La Compañía deberá contar con una política de protección de datos personales, que permita proteger la información obtenida de sus accionistas, inversionistas, proveedores, empleados, filiales y empresas relacionadas y cualquier otra persona natural que tenga contacto con Grupo SURA, además establecerá los procedimientos necesarios para el manejo adecuado de los datos de carácter personal contenidos en sus bases de datos.

- El reporte de los eventos o incidentes de seguridad es de carácter obligatorio para todos los destinatarios de la presenta política.

- Los destinatarios de la presente Política deben reportar al área de Servicios Internos y Compartidos, en el correo notificaciones_seguridad@gruposura.com.co cualquier anomalía o evento que pueda significar una afectación, real o potencial, con la información de la Compañía.

- Todos los incidentes o eventos se deben registrar, verificar, clasificar, priorizar, valorar e investigar de acuerdo con el procedimiento definido para tal fin.

- La documentación sobre los incidentes o eventos de seguridad de la Información o ciberseguridad debe ser tratada como información confidencial. Esta información, deberá ser tenida en cuenta para la prevención y/o gestión de futuros incidentes, así como para adoptar los correctivos que fueren conducentes.

- Toda decisión sobre eventos de seguridad de la información que amerite contacto con las autoridades o emprenda acciones legales, deberá contar con

la participación de las áreas de Asuntos Legales Corporativos, Cumplimiento, Riesgos Corporativos y Servicios Internos y Compartidos.

- Se hará una evaluación de los riesgos de seguridad de la información y ciberseguridad, así como del Modelo de Gobierno de la Información, y se informará, sobre los resultados de la misma, al Comité de Riesgos de la Junta Directiva trimestralmente.

Formación y Cultura

La Compañía definirá una estrategia de formación dirigida a los destinatarios de la presente política, promoviendo una cultura basada en el adecuado tratamiento y protección de la información y aplicando los lineamientos definidos para tal fin.

Gobernabilidad

La aprobación de la presente política está a cargo de la Junta Directiva de Grupo SURA. Cualquier modificación deberá ser aprobada por este mismo órgano. La vigilancia y actualización de la misma será responsabilidad del área de Servicios Internos y Compartidos.

Divulgación y actualización

La presente política se divulgará a los Miembros de la Junta Directiva, Alta Gerencia, colaboradores y proveedores que gestionen información de la Compañía. Se actualizará de acuerdo con los cambios organizacionales, disposiciones legales u otros aspectos que puedan afectar los lineamientos aquí establecidos.