Política de Seguridad de la Información y Ciberseguridad

Introducción y Objetivo

SURA Asset Management reconoce la información como un activo valioso que apoya los procesos y decisiones de la compañía, por lo tanto, está comprometida con mantener segura la información propia y de terceros mediante estrategias de gestión y control que permitan preservar su confidencialidad, integridad y disponibilidad, así como enfrentar las amenazas a las que está expuesta la compañía.

Alcance y Marco de Aplicación

Los lineamientos contenidos en el presente documento aplican a todos los colaboradores y terceros (clientes, proveedores de servicios o aliados) involucrados operativamente y/o funcionalmente en los procesos de SURA Asset Management, sus filiales y subsidiarias con participación relevante (en adelante "La Compañía"), independiente de la modalidad de trabajo en la que se encuentre.

Esta política aplica para toda la información de La Compañía que es gestionada por SURA Asset Management, independientemente del mecanismo bajo el cual se realice su gestión. Así mismo, aplica para todos los sistemas de información y los mecanismos mediante los cuales se usa y almacena la información y los datos, independientemente, si es un sistema basado en la nube, software, aplicaciones y/o herramientas tecnológicas propias o de terceros.

Estas directrices se establecen con el objetivo de identificar, proteger, detectar, responder y recuperar la información a través de la gestión de los riesgos asociados. En aquellos casos en que la Regulación de cada país o localidad sea más estricta que los lineamientos previstos en la presente política, se dará prevalencia a dicha regulación.

Lineamientos Seguridad de la Información y Ciberseguridad

La información como un activo importante de La Compañía debe ser debidamente protegida y la aplicación del presente documento es un compromiso para implementar los mecanismos de protección. Por lo tanto, La Compañía debe:

i. Asegurar la alineación de las funciones de Seguridad de la Información (gobierno, operación y vigilancia) con el Gobierno Corporativo de la compañía.

ii. Establecer e implementar políticas, procesos, procedimientos, instructivos y/o manuales operativos, claramente definidos, aprobados y publicados, para gestionar y desarrollar las capacidades de Seguridad de la Información alineados con las definiciones y lineamientos corporativos.

iii. Garantizar que existan mecanismos necesarios para medir la efectividad operativa, adopción de los lineamientos y realizar monitoreo y seguimiento periódico que permita identificar desviaciones y áreas de mejora contra los lineamientos de las políticas, procesos, responsabilidades y/o controles definidos de Seguridad de la Información y Ciberseguridad y ser informados al Corporativo.

iv. Asegurar que existen mecanismos claros de reporte, escalamiento y comunicación con el Corporativo, que le permita tener una visión consolidada del Gobierno, Operación, Monitoreo, Funcionamiento y Cumplimiento de la Seguridad de la Información.

v. Tener una estrategia corporativa de Seguridad de la Información y presupuesto asignado para la implementación de medidas de mitigación de los riesgos identificados dentro del entorno de los activos de información. Las estrategias y programas locales de Seguridad de la Información deben estar alineadas con la estrategia regional.

vi. Realizar la gestión de riesgos de Seguridad de la Información y Ciberseguridad enmarcados en la gestión de riesgos operacional de los procesos y de la tecnología, con el fin de establecer los controles de Seguridad de Información e identificar, evaluar y monitorear los riesgos. Para esto Las Compañías deben garantizar:

    a. Ser parte del proceso de "Compras, bienes y servicios" para identificar, evaluar, tratar y monitorear los riesgos provenientes de las relaciones con terceros, servicios y nuevas tecnologías

    b. La participación en proyectos en los cuales se contemple los requerimientos de Seguridad de la Información y ciberseguridad con el fin de proteger los activos de información y la tecnología que lo soporta.

vii. Garantizar la Seguridad de la Información en los colaboradores y terceros mediante la alineación con otros procesos internos para que se incluyan aspectos de Seguridad de la Información en la selección, vinculación, desarrollo y desvinculación del talento humano.

viii. Tener programas de capacitación y campañas de concientización anuales de riesgos relacionados a Seguridad de la Información y Ciberseguridad, que se basen en el panorama dinámico de amenazas de las cuales podría ser objetivo La Compañía.

ix. Gestionar los activos de información, para lo cual debe:
   a. Contar con inventario de activos de información

   b. Tener claridad sobre la Propiedad de la información

   c. Clasificar y administrar la información y activos tecnológicos de acuerdo con los criterios Corporativos y regulaciones locales.

   d. Administrar del ciclo de vida de la información

   e. Establecer controles de Seguridad de la Información en el desarrollo, adquisición, implementación, mantenimiento, procesamiento y disposición de los sistemas de información.

   f. Tener un adecuado control y monitoreo de acceso lógico.

x. Administrar y operar la seguridad en la Tecnología que soporta la información, por lo tanto, debe:
   a. Establecer y mantener controles que aseguren la confidencialidad, integridad y disponibilidad de la información en las operaciones de Tecnología; considerando la seguridad y ciberseguridad en todos los activos tecnológicos que soportan la operación de SURA AM, incluyendo Infraestructura, redes y telecomunicaciones, entre otros.

   b. Establecer, realizar y mantener ejercicios periódicos de análisis de vulnerabilidades y pruebas de penetración para la identificación y cierre de posibles brechas de seguridad en el ambiente tecnológico.
   c. Hacer Uso adecuado de la tecnología de información la cual debe ser utilizada únicamente para fines relacionados con el objeto y propósito establecidos.

   d. Establecer y mantener controles de seguridad y ciberseguridad en equipos de usuario final

   e. Establecer mecanismos para el cifrado de la información en tránsito y/o reposo que deben ser implementados en equipos de cómputo, bases de datos, aplicaciones, servidores, dispositivos móviles, y/o cualquier dispositivo de almacenamiento externo, todo lo anterior acorde a la clasificación de los activos de información.

f. Tener Enmascaramiento de datos y establecer mecanismos para proteger la información confidencial y sensible, y al mismo tiempo mantener su legibilidad para que se pueda utilizar libremente, sin poner en peligro la seguridad de esta. Esto aplica para los diferentes ambientes (Producción, Pruebas, QA, Desarrollo).

g. Monitorear los eventos y ciberinteligencia**:** Contar con un monitoreo activo de eventos y debilidades en los activos de información, así como un consumo de fuentes de ciberinteligencia de amenazas como parte de una estrategia de prevención de incidentes de Seguridad de la Información. Este monitoreo de eventos de seguridad debe considerar la identificación de comportamientos inusuales por parte de personal crítico incluido en un programa de analíticos de seguridad.

h. Gestionar la seguridad y protección de la marca a través del monitoreo del uso adecuado por todos los colaboradores de la compañía dentro y fuera de la organización.

i. La gestión de eventos y/o incidentes de Seguridad de la Información que afecten la disponibilidad, confidencialidad e integridad de la información debe estar alineada a los lineamientos definidos para la Gestión de Continuidad del Negocio y/o la Gestión de Crisis con el fin de responder y recuperar de forma eficiente la operación, minimizando con esto afectaciones al cumplimiento de los objetivos, misión y visión de La Compañía. Los eventos en los cuales se presente un secuestro, robo, modificación y/o publicación de información de La Compañía e incluyan extorsión por parte de ciberdelincuentes, deben ser analizados para evaluar el impacto operacional, legal y/o reputacional, además de los mecanismos de control para recuperar o restaurar la información. Así mismo, deberán ser Informados al Oficial de Seguridad de la Información Corporativo, quien Informará y/o Consultará al Comité de Riesgo de la Junta Directiva de Sura Asset Management el plan de acción para el tratamiento del evento.

Principales funciones y responsabilidades de los Órganos de Gobierno

La Compañía garantiza el apoyo a la gestión de la Seguridad de la Información para que pueda implementar, operar, mantener y mejorar continuamente el proceso mediante el establecimiento de:

- **Comité de Riesgos de Junta Directiva:** Además de las funciones y responsabilidades descritas en la “Política para la Gestión de los Riesgos de la Operación”, será responsable de monitorear la estrategia y recursos para la gestión Seguridad de la Información, así como conocer el estado de madurez de la gestión y la exposición al riesgo actual para definir el apetito de riesgo con respecto a esta especialidad, monitorear la gestión de sus riesgos, los incidentes y eventos relevantes de Seguridad de la Información.

- **Comité Regional de Seguridad de la Información y Ciberseguridad:** Responsable de hacer seguimiento al desempeño corporativo sobre la gestión de Seguridad de la Información, es decir, monitorear el cumplimiento de los objetivos estratégicos a nivel regional, la alineación de las iniciativas locales con las corporativas, seguimiento al estado de indicadores de gestión de riesgos de Seguridad de la Información y el seguimiento al contexto global y regional de las amenazas que aplican para la Compañía.

- **Comité de Gestión Integral de Riesgos:** Además de las funciones y responsabilidades descritas en la "Política para la Gestión de los Riesgos de la Operación", es el encargado de vigilar que la gestión de Seguridad de la Información se ajuste a los objetivos, políticas, estrategias, procedimientos y niveles de tolerancia y apetito al riesgo aprobado. Igualmente, debe promover la cultura de Seguridad de la Información y monitorear el cumplimiento de las normativas internas y externas.

- **Oficial de Seguridad de la Información (ISO por sus siglas en inglés):** Es responsable de garantizar el cumplimiento de los objetivos estratégicos de Seguridad de la Información y Ciberseguridad, a través del Gobierno, Gestión y Monitoreo. Se apoya en personal de cada compañía para la ejecución de actividades y cumplimiento de requerimientos normativos.

Gobernabilidad

La aprobación de la presente política está a cargo del Comité de Riesgos de Junta Directiva de SURA Asset Management. Cualquier modificación deberá ser aprobada por este mismo órgano de gobierno. Toda excepción al cumplimiento de la presente política debe ser revisada por el Oficial de Seguridad de la Información y los casos en los que se identifique un riesgo con nivel alto o crítico, serán escaladas al Comité de Gestión de Riesgos de Junta Directiva.

Divulgación y actualización

Todas las personas dentro del alcance de esta Política deberán conocerla y aplicarla, dando cumplimiento a lo aquí establecido. El área de Seguridad de la Información en representación del Oficial de Seguridad de la Información será el responsable de la administración de esta política y en esa medida gestionará con el equipo de Seguridad de la Información, su cumplimiento y divulgación.

La presente política comenzará a regir a partir de su adopción por la Junta Directiva u órgano de gobierno equivalente y se actualizará de acuerdo con las disposiciones legales, los cambios organizacionales u otros aspectos que puedan afectar los lineamientos aquí descritos.