sophos solutions

Proceso: GESTIÓN SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Documento No: **PL-SSI-01**

Versión: **11**

Fecha: **30/03/2022**

Redactado por: **Seguridad de la Información**

DOCUMENTO APROBADO POR

	Reviso	Aprobó
Nombre	Álvaro Barbosa	Felipe Villa Murra
Cargo	Risks and Information Security Manager	Presidente & CEO
Fecha	30/03/2022	30/03/2022

1 ÍNDICE

2 HISTORIAL DE VERSIONES

Fecha	Versión	Autor	Descripción
21/08/2020	08	Risk & Information Security Administrator	Roles y responsabilidades Actividades Área Riesgos y seguridad de la Información Acciones que afectan la seguridad de la información Responsabilidad de Sophos Solutions S.A.S y sus Colaboradores Frente a Seguridad de la Información Política de Control de Acceso Política de Trabajo en Áreas Protegidas.

			Política de Seguridad de los Equipos Fuera de las instalaciones de la compañía Política Protección contra Software Malicioso Política Relación con Proveedores Política de Control de Cambios Operativos Política Gestión de Incidentes de Seguridad de la Información Política Seguridad de la Información en la Continuidad del Negocio Política Criptografía
11/03/2021	09	Risk & Information Security Lead	Se actualiza el alcance del Sistema de Gestión de Seguridad de la Información Se actualiza el apartado respecto al manejo de las excepciones, dado que ahora se gestionan por flow2l.
02/09/2021	10	Risk & Information Security Lead	Política de trabajo en casa Política control de cambios Política de Uso Aceptable de Activos de Información Política Gestión de Registro (log) Se agregan normatividad asociadas.
30/03/2022	11	Risk & Information Security Manager	Se independiza la Política estratégica de las políticas de seguridad Se actualiza la Política de Seguridad Se actualizan los objetivos del Sistema Se actualizan los roles y Responsabilidades

3 INTRODUCCIÓN

La política de seguridad de la Información está orientada a propender por la seguridad de todos los activos de información de la Compañía conforme a su estrategia corporativa, garantizando así, el cumplimiento normativo y regulatorio, además de las políticas, procedimientos y controles establecidos para tal fin.

4 ACTUALIZACIÓN POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Dando cumplimiento en la mejora continua del Sistema de Gestión de Seguridad de la Información, se establece que la Política de Seguridad de la Información deberá revisarse cada 6 meses a partir del último cambio realizado o cuando haya modificaciones o nuevos lineamientos que lo ameriten.

La actualización de la Política de seguridad deberá ser validada y aprobada por el comité de seguridad de la información.

5 NORMATIVIDAD ASOCIADA

Seguridad y Privacidad de la Información	Propiedad Intelectual
Constitución Política de Colombia. Artículo 15.	**Ley 23 de 1982.-**Sobre derechos de autor"

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.	**Decreto 1360 de junio de 1989.-**Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor
Ley 1273 de 2009.- Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	**Ley 44 de 1993.-** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
Ley 1581 de 2012.- Por la cual se dictan disposiciones generales para la protección de datos personales.	**Decisión Andina 351 de 1993.-** Régimen común sobre Derechos de Autor y Derechos conexos
Decreto 1377 de 2013.- Por el cual se reglamenta parcialmente la Ley 1581 de 2012.	**Ley 178 de 1994.-** Adhesión al convenio de Paris para la Protección de la Propiedad Industrial
Ley 1928 de 2018.- Por medio del cual se aprueba el " Convenio sobre la ciberdelincuencia" adoptado el 23 de noviembre de 2001, en Budapest. -confirmado por la Corte Constitucional en la sentencia C 224	**Decreto 460 de 1995.-** Reglamentación Registro Nacional del Derecho de Autor y se regula el Depósito Legal
Circular Externa 029 de 2014 de la Superfinanciera. – Parte I Título I Capitulo IV -- Control interno Incluye continuidad.	**Ley 599 de 2000.-**Bien jurídico de los derechos de autor
Circular Externa 029 de 2014 de la Superfinanciera. – Parte I Titulo II Capitulo --Seguridad--	**Ley 565 DE 2000.-**Adhesión al Tratado de la OMPI sobre derecho de autor
	Ley 1915 de 2018.- Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

6 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Mediante la implementación de la norma ISO/IEC 27001:2013 la compañía Sophos Solutions S.A.S. adopta, establece, opera, comprueba y mejora el Sistema de Seguridad de la Información para los procesos Fábrica de Desarrollo de Software "incluyendo Planificación y Administración de Proyectos, Levantamiento de Requerimientos, Análisis y Diseño, Construcción, Pruebas, Implementación, Soporte y Consultoría".

Sophos Solutions S.A.S es una multinacional colombiana, con oficinas en la ciudad de Bogotá D.C. y Medellín, que provee servicios de Consultoría, Implementación de Core Bancario, Fábrica de Software para todo tipo de organizaciones, especialmente en compañías del sector Financiero y Bursátil.

6.1 POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La compañía Sophos Solutions SAS comprendiendo la importancia de proteger la confidencialidad, integridad y disponibilidad de la información para cada uno de los activos de información y servicios de TI que ofrece a la industria financiera y bursátil, así como también a la industria del Fintech como líder de innovación digital, se ha comprometido a Establecer, Implementar, Adoptar, Operar y Mejorar el Sistema Gestión de Seguridad de la Información como instrumento transversal para identificar, analizar, contener y remediar los riesgos de seguridad identificados con el fin de sostener la mejora continua del sistema, alineado a los requerimientos regulatorios y estratégicos de la compañía.

Por lo anterior, la Política de Seguridad de la Información aplica a las partes interesadas internas de Sophos Solutions SAS de acuerdo con el alcance determinado para el Sistema de Gestión.

Las demás políticas que se deriven como resultado de la implementación del SGSI y de su proceso de mejora continua serán adoptadas y de obligatorio cumplimiento por todos los grupos de interés identificados.

6.2 OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. Evaluar los controles de seguridad actualmente establecidos con el fin de sostener el SGSI en función de la norma ISO27001 y las necesidades de la organización mediante el planteamiento de un perfil actual y un perfil objetivo.
2. Generar conciencia de la seguridad de la información en los colaboradores de la compañía por medio de capacitaciones y sensibilizaciones definidas como medio para controlar incidentes de seguridad.
3. Controlar los incidentes relacionados con seguridad de la información mediante el análisis de los reportes obtenidos de diferentes fuentes con el fin de mitigar sus causas y/o consecuencias.
4. Identificar las Vulnerabilidades a las que está expuesta la entidad por medio de análisis propios y de terceros con el fin de tomar acciones que permitan cerrar las brechas de seguridad que presente la organización y que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de su información.
5. Controlar las brechas de seguridad identificadas en Proyectos de Desarrollo a clientes por medio del análisis de los hallazgos de seguridad obtenidos en auditorías de seguridad de la información.

6.3 ROLES Y RESPONSABILIDADES

La estructura definida para la asignación de Roles y Responsabilidades para la gestión de seguridad de la información será:

ALTA GERENCIA	PRESIDENT & CEO VICEPRESIDENT SPECIAL PROJECTS
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	PRESIDENT & CEO VICEPRESIDENT SPECIAL PROJECTS MANAGER OF STRATEGY AND VALUE CREATION CHIEF OPERATION OFFICER LEGA L MANAGER & DEPUTY SECRETARY GENERAL CORPORATE MANAGER INFORMATIC SECURITY AND TECHNOLOGY MANAGER IT LEADER CHIEF FINANCIAL OFFICER VICEPRESIDENT GLOBAL TALENT VICEPRESIDENT GLOBAL SALES VICEPRESIDENTS PROJECTS VICEPRESIDENT PRODUCTS AND SUBSIDIARIES GLOBAL TALENT MANAGER VICEPRESIDENT REGIONAL SALES COUNTRY HEAD NORTH AMERICA INNOVATION MANAGER QUALITY & PROCESSES MANAGER RISK & SECURITY INFORMATION LEAD RISK LEADER
USUARIO FINAL	COLABORADORES
AUDITORIA INTERNA	GLOBAL INTERNAL AUDIT MANAGER GLOBAL INTERNAL AUDIT LEADER TI

De acuerdo con la estructura de asignación de roles y responsabilidades definidas, a continuación, se relacionan las responsabilidades asignadas a cada rol establecido

6.4 ALTA GERENCIA

La Alta Gerencia es el máximo órgano de la compañía, por tanto, su responsabilidad frente a la mejora continua del Sistema Gestión de Seguridad de la Información es:

- Aprobar las políticas para la gestión de seguridad de la información.
- Apoyar la definición y lineamientos de la estrategia para la gestión de seguridad de la información.
- Proveer los recursos necesarios y asignar los roles, responsabilidades y niveles de autoridad para implementar y mantener la gestión de seguridad de la información.
- Realizar seguimiento de la mejora continuidad del Sistema de Gestión de Seguridad de la Información.

6.5 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información es el encargado de:

- Analizar y entregar sugerencias de mejora a la presidencia sobre todos los lineamientos de la gestión de seguridad de la información.
- Analizar y entregar sugerencias de mejora a la presidencia sobre los modelos de medición y riesgos para la gestión de seguridad la información.
- Recomendar la imposición de medidas disciplinarias para los casos que el Área de Riesgos y Seguridad de la Información reporte por incumplimiento a las políticas de seguridad establecidas dentro de la organización.
- Analizar y recomendar la implementación de controles para la prevención de riesgos de seguridad de la información.
- Analizar e Implementar programas de generación de cultura de seguridad de la información.
- Implementar y realizar seguimiento de indicadores que midan los objetivos asociados al Sistema de Gestión de Seguridad de la Información.
- Analizar cuestiones externas e internas a la luz de seguridad de la información.
- Analizar el desempeño del sistema de Gestión de Seguridad de la información.
- Analizar resultados de las retroalimentaciones de seguridad por parte de proveedores/clientes externos.
- Analizar oportunidades de mejora.

Al comité de seguridad de la información pueden asistir analistas o líderes de diferentes áreas, pero no tendrán voz ni voto.
Este comité se reunirá Trimestralmente y tratará los temas referentes al Sistema de Gestión de Seguridad de la información.
El auditor interno será invitado permanentemente al comité y tendrá voz, pero no voto.

6.6 USUARIO FINAL

- Los Colaboradores de Sophos son responsables de la calidad, integridad y veracidad de los datos ingresados en los diferentes sistemas de información utilizados dentro de la compañía (bien sean propios o de terceros).
- Los colaboradores están obligados a cumplir los lineamientos y permisos otorgados por el propietario sobre sus activos de información.
- Los colaboradores de Sophos deberán Cumplir con las Política de seguridad establecida en el presente documento y todas las políticas derivadas del mismo.

- Los Colaboradores de Sophos deben velar por el cumplimiento de las políticas de Seguridad de la Información dentro de su entorno laboral inmediato (a nivel interno de la compañía y en Cliente).
- Es responsabilidad de los colaboradores, Clientes y proveedores reportar de manera inmediata y a través de los canales establecidos por Sophos Solutions SAS, la sospecha u ocurrencia de eventos y/o incidentes de Seguridad de la Información relacionados con la compañía.
- Es deber de los colaboradores utilizar los sistemas de información y el acceso a la red de la compañía únicamente para los propósitos que lo vinculan con ella.
- Es deber de los colaboradores utilizar únicamente el software y demás recursos tecnológicos autorizados por Sophos y/o el Cliente de Sophos.
- Es deber de los colaboradores y Proveedores de Sophos Solutions SAS velar por la Confidencialidad, Integridad y Disponibilidad de los activos de información utilizados para la ejecución de sus actividades.
- Es deber de los colaboradores utilizar los diferentes canales, herramientas y medios de comunicación proporcionados por el área de Seguridad de la Información e Infraestructura para realizar solicitudes específicas de seguridad, accesos y servicios frente a sus labores diarias.
- Es deber de los Colaboradores y Proveedores participar activamente de los cursos, charlas y sensibilizaciones de Seguridad organizadas por el área Seguridad de la Información.

6.7 AUDITORÍA INTERNA

Validar la aplicación y cumplimiento de la Política de Seguridad de la Información definida en esta Directiva, así como las demás políticas que se deriven del proceso de mejora continua del SGSI, la aplicación de controles sobre los activos de información y los demás requerimientos del Sistema de Gestión de Seguridad de la Información.

"Sophos Solutions S.A.S. se reserva el derecho de modificar el presente documento según los cambios que surjan al interior de la compañía.