Proceso: GESTIÓN SEGURIDAD DE LA INFORMACIÓN

Política de Seguridad de la Información

Documento No:	**PL-SSI-01**
Versión:	**08**
Fecha:	**21/08/2020**

Redactado por: **Seguridad de la Información**

Documento aprobado por:

	REVISO	APROBO
NOMBRE	**Álvaro Barbosa**	**Mauricio Mosseri**
CARGO	**Risks and Information Security Lead**	**Presidente**
FECHA	**21/08/2020**	**21/08/2020**

1. Índice

2. Historial de Revisiones

Fecha	Versión	Autor	Modificación
25/04/2017	01	Infraestructura	Creación del documento
28/12/2017	02	Infraestructura	Se incluye: - comité de seguridad de la información - terminología - Responsabilidad de Sophos Solutions S.A.S y sus colaboradores frente a seguridad de la información - Responsabilidades de los colaboradores en el control de acceso - Política de Instalación de Equipo Electrónico - Política de Destrucción o Reubicación de Equipos Electrónicos - Copias De Seguridad - Seguridad y Contenido de Internet - Se eliminan las secciones: uso de carpeta asignada, correo electrónico corporativo, firma de correo corporativo, manejo de hardware y manejo de telecomunicaciones Nota: La aprobación de esta versión la realizo Juan Camilo Rodriguez teniendo en cuenta que Mauricio Mosseri se encuentra en vacaciones.
05/07/2018	03	Seguridad de la Información	Se modifica: - Proceso de Gestión de Infraestructura por Proceso de Gestión Seguridad de la Información - Del ítem 9.11 Políticas de Instalación, uso y administración de equipos de cómputo se modifica en el numeral 1.11.1 el literal n) en dónde se pasa de 1 minuto el tiempo de bloqueo por inactividad a 3 minutos, ya que es recomendable para no impactar la operatividad.

Fecha	Versión	Autor	Modificación
10/10/2018	04	Seguridad de la Información	- Se agrega en el ítem 9.3 en el numeral a) el formato F-SSI-04 Acuerdo uso Credenciales Internos para la solicitud y asignación de credenciales sobre sistemas adicionales a los colaboradores. c) el formato F-SSI-02 Acuerdo Uso Credenciales Externos para las responsabilidades de los externos sobre los sistemas de Sophos Solutions S.A.S Solutions - Se agrega en el ítem 9.9. en el numeral b) el formato F-SSI-05 Acuerdo uso Conexión Remota a VPN Client to Site para las conexiones remotas de colaboradores. - Se agrega en el ítem 9.11 en el numeral e) el formato F-SSI-03 Acuerdo uso Privilegios Internos, para los funcionarios que requieren permisos de administrador sobre los equipos. - Se agrega en el ítem 9.12 en el numeral b) el formato F-SSI-07 Responsabilidad para Desbloqueo de Puertos creado para las excepciones del bloqueo de puertos. - Se quita en el ítem 9.12, a) Redes inalámbricas no autorizadas.
03/06/2019	05	Seguridad de la Información	-Robustecimiento de la periodicidad de las reinducciones a 2 veces al año -Creación de Repositorios a cargo del área de Infraestructura, de acuerdo con check list. -Restricción de acceso no autorizado al correo corporativo desde dispositivos móviles y sus excepciones - Adición de sección de prohibiciones en Seguridad y Contenido de Internet.
26/09/2019	06	Information Security Administrator	- Se incluye la política de desarrollo de código seguro - Actualización del logo corporativo
15/04/2020	07	Information Security Administrator	- Alcance de Seguridad de la Información - Objetivos de Seguridad de la Información - Política de Seguridad de la Información - Política de activos de información - Política copia de Seguridad - Política de pantalla y escritorio limpio.

Fecha	Versión	Autor	Modificación
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

3. Introducción

Está política está orientada a propender por la seguridad de todos los activos de información de la Compañía conforme a la estrategia del mercado; garantizando así el cumplimiento normativo, políticas y procedimientos establecidos para tal fin.

4. Objetivos

Sophos Solutions S.A.S consciente de los riesgos a los cuales se encuentra expuesta la infraestructura y los activos de información decidió:

- Mantener controles que permitan minimizar los riesgos actuales y potenciales con el fin de soportar la implementación de un procedimiento de Seguridad de la Información.
- Garantizar una adecuada protección de la información, teniendo en cuenta los criterios de Confidencialidad, Integridad y Disponibilidad de la información.
- Propender un modelo con el fin de prevenir el acceso no autorizado, el daño o robo de información que pueda generar interrupciones a las actividades de la compañía.
- Divulgar trimestralmente temas de seguridad de la información, con el fin de garantizar el entendido por parte de los colaboradores de Sophos Solutions S.A.S.

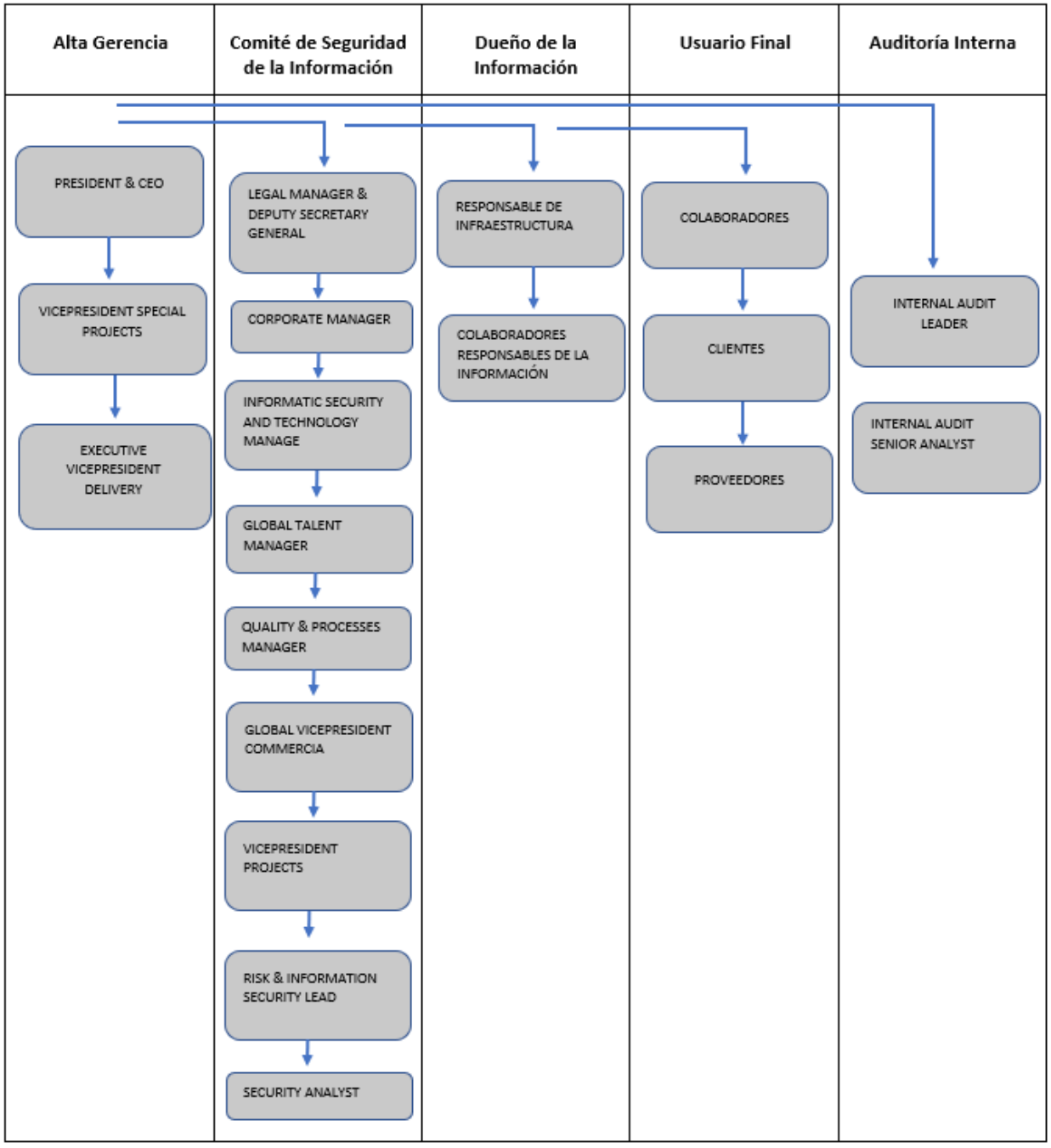
5. Terminología

Nombre	Descripción
Activos de Información	Son los Recursos que se generan, procesa y/o resguarda Información necesaria para que Sophos Solutions S.A.S funcione y consiga el cumplimiento de los objetivos
Controles	Conjunto de acciones, normas, documentos, procedimientos y medidas técnicas adoptadas para propender porque cada amenaza, identificada y valorada con un cierto nivel de riesgo sea minimizada.
Criterios de Seguridad de la Información	**1. Confidencialidad:** La Información se revela sólo de forma autorizada, a personas, procesos o entidades autorizadas y en el momento autorizado. **2. Integridad**: Se debe salvaguardar la exactitud y estado completo de la información y de los activos de información. **3. Disponibilidad:** La información debe ser accesible y utilizable cada vez que sea requerida por los interesados autorizados.
Criterios de calidad de la Información	**Confiabilidad:** La Información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones. **Efectividad:** La Información relevante debe ser pertinente y su entrega oportuna, correcta y Consistente. **Eficiencia:** El procesamiento y suministro de Información debe hacerse utilizando los Activos de Información de la mejor manera posible.
Dominio	Conjunto de objetivos de control orientados a un mismo subproceso del SGSI.
Información	Es un conjunto organizado de datos procesados que generan valor a la ejecución de los procesos.
Medios de Almacenamiento	Son elementos técnicos destinados a proveer espacio físico para albergar Información. Estos pueden ser físicos, magnéticos, ópticos, magnético - ópticos, entre otros.
Objetivo de Control	Conjunto de controles específicos con un objetivo en común, que busca minimizar los riesgos de un aspecto particular.

Nombre	Descripción
Sistemas de Información	Es un conjunto de elementos orientados al tratamiento y administración de datos e información organizados y listos para su uso; compuestos por software (bases de datos entre otros), infraestructura (servidores y equipos de telecomunicaciones) e Información (parámetros, bases de datos, entre otros).
Sistema de Gestión de Seguridad de Información (SGSI)	Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
Software Malicioso (Malware)	Todo tipo de programa o código informático malicioso cuya función es dañar un sistema, robar información o causar un mal funcionamiento.

6. Roles y Responsabilidades

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



6.1 Alta Gerencia

De acuerdo con la estructura de asignación de roles y responsabilidades definidas anteriormente, la presidencia es el máximo órgano, el cual es el responsable de:

- 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.

6.2 Comité de Seguridad de la Información

- 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.
- Analizar e Implementar programas de generación de cultura de seguridad de la información.
- Implementar y realizar seguimiento de indicador de Riesgos en seguridad de la información.
- Analizar y realizar seguimiento al programa de implementación de seguridad de la información para ser aprobado por el comité de presidencia.
- Recomendar la imposición de medidas disciplinarias para los casos en que el responsable de seguridad de la información reporte un incumplimiento de la política establecida en la adopción de prácticas de seguridad de la información.
- Analizar y recomendar la implementación de controles para la prevención de riesgos de seguridad de la información.

Este comité se reunirá bimestralmente y tratará los temas referentes a la gestión de seguridad de la información.

El auditor interno será invitado permanentemente al comité y tendrá voz, pero no voto.

6.3 Área Riesgos y Seguridad de la información

- Definir los instrumentos, metodologías y procedimientos con el fin de administrar correctamente los riesgos.
- Desarrollar los programas de capacitación en riesgos de seguridad de la información.
- Realizar seguimiento en la ejecución de los procedimientos, planes de acción y proponer su actualización.
- Reportar al comité de seguridad los controles implementados, la evolución y monitoreo de los riesgos.

- Desarrollar e implantar un sistema de gestión de la seguridad que permita identificar y dar respuesta a los nuevos riesgos de la organización.
- Prevención y detección de vulnerabilidades en la infraestructura y sistemas de información de Sophos Solutions S.A.S Solutions SAS.
- Generación de políticas, procedimientos y lineamientos de seguridad y ciberseguridad para la protección de los activos de información alineados con la confidencialidad, integridad y disponibilidad de esta.
- Definir estrategias de seguridad y posición misma en la organización para orientar los objetivos de la seguridad en la consecución de los objetivos de la organización.
- Educación y sensibilización de los empleados. Concienciación y cultura de seguridad en toda la organización destacando el valor que aporta. Toda la organización debe entender el propósito de la seguridad.
- Estar a cargo de la planificación de respuesta de incidentes, así como la investigación de vulneración de la seguridad, y ayudar con las cuestiones disciplinarias y legales relacionados con las infracciones que sean necesarias
- Formular y conducir la elaboración de los documentos normativos de gestión para el ordenamiento y mejora de las acciones a desarrollar por el resto de las áreas.
- Establecer, revisar, aprobar y mantener actualizada, junto con el Comité de Seguridad, la Política de Seguridad de la organización y las responsabilidades generales en materia de seguridad de la información en cada área de la organización.
- Evaluar la pertinencia y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Alinear la estrategia de ciberseguridad con los objetivos de la empresa.
- Mejora continua en el sistema de gestión de seguridad de la información.

6.4 Auditoría Interna

Validar la aplicación y cumplimiento de las políticas de Seguridad de la Información definidas en esta Directiva, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.

6.5 Gestión de Recursos Humanos

Incluir en los programas de inducción el tema de seguridad de la información asegurando que los colaboradores conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos.
Garantizar la seguridad de los recursos humanos.

6.6 Líderes de Área y Proyectos

Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como

6.7 Propietarios de los activos de información

- Los colaboradores son responsables de la calidad de la información ingresada en los diferentes sistemas de información usados en Sophos Solutions S.A.S, para lo cual deben alimentar los datos que son editables en forma íntegra y veraz.
- Comunicar sus requerimientos de seguridad de información al líder del Área de Seguridad de la Información de la Oficina de Informática y Sistemas.
- Determinar y autorizar todos los privilegios de acceso a sus activos de información.
- Comunicar al Área de Seguridad de la Información sus requerimientos en capacitación sobre temas de seguridad.
- Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.

6.8 Usuario final

- Cumplir con las políticas de Seguridad de la Información, contempladas en el presente documento.
- Velar por el cumplimiento de las políticas de Seguridad de la Información dentro de su entorno laboral inmediato.
- Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.
- Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.
- Utilizar únicamente software y demás recursos tecnológicos autorizados.
- Velar por la Confidencialidad, Integridad y disponibilidad de los activos de información.

6.9 Acciones que afectan la seguridad de la información

A continuación, se describen algunas acciones que afectan la Seguridad de la Información en Sophos Solutions S.A.S, las cuales ponen en riesgo la integridad, confidencialidad y disponibilidad.

I. Permitir que personas ajenas a Sophos Solutions S.A.S ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
II. No clasificar la información y/o etiquetar la información.
III. No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.
IV. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
V. Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre los escritorios.

VI. Hacer uso de la red de Sophos Solutions S.A.S para difundir, obtener o mantener material publicitario o sacando provecho para beneficios personales, los cuales sean ajenos a las actividades laborales.
VII. Instalar software en la plataforma tecnológica de la Sophos Solutions S.A.S cuyo uso no esté autorizado por el Área de Seguridad de la Información y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.
VIII. Enviar información clasificada de la compañía por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los lineamientos para la transferencia de información.
IX. Guardar información de Sophos Solutions S.A.S o Clientes en cualquier dispositivo de almacenamiento que no pertenezca a la compañía.
X. Conectar dispositivos móviles y/o equipos de cómputo personales a la red de Sophos Solutions S.A.S sin autorización del Área de Seguridad de la Información.
XI. Ingresar a la red tecnología de Sophos Solutions S.A.S por cualquier servicio de acceso remoto sin la autorización del Área de Seguridad de la Información.
XII. Uso de la identidad corporativa digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro colaborador.
XIII. Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de la compañía o de clientes.
XIV. Realizar cambios no autorizados en la Plataforma Tecnológica de la compañía o en Clientes.
XV. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de Seguridad de la Información
XVI. Otorgar privilegios de acceso a los activos de información a colaboradores o terceros no
XVII. autorizados.

La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información de Sophos Solutions S.A.S, son consideradas como incidentes de seguridad las cuales acarrearán medidas administrativas, acciones disciplinarias y/o penales que haya lugar.

7. 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 nuevas políticas que lo ameriten.
La actualización de la Política de seguridad o algún lineamiento referente al Sistema de Gestión de Seguridad de la Información deberá ser validado y aprobado en el comité de seguridad de la información.

8. Normatividad Asociada

El desarrollo e implementación del modelo de seguridad de Información de Sophos Solutions S.A.S, adopta algunas prácticas de la Norma ISO 27001. Así mismo, servirán de referencia las normas planteadas en las siguientes legislaciones:

I. Ley 1273 de 2009, Ley de Delitos Informáticos en Colombia
II. Ley 23 de 1982 y Ley 44 de 1993, Derechos de Autor-Propiedad Intelectual
III. Decreto 1360 de junio de 1989, Derechos de Autor-Soporte Lógico (software)
IV. Ley estatutaria 1581 de 2012, Protección de datos personales
V. Decreto 1377 de 2013, Protección de datos personales
VI. Circular Externa 029 de 2014 de la Superfinanciera – Parte I Titulo II Capitulo --Seguridad--
VII. Circular Externa 029 de 2014 de la Superfinanciera – Parte I Título I Capitulo IV -- Control interno Incluye continuidad--

9. Políticas

Las consideraciones presentadas a continuación deben ser tenidas en cuenta por los colaboradores de Sophos Solutions S.A.S.

Se debe velar por el cumplimiento de los siguientes numerales:

9.1 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”, Fabrica de Pruebas, Consultoría y Outsourcing estableciendo mecanismos que preserven la confidencialidad, integridad y disponibilidad de los activos de información.

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 Pruebas y Fábrica de Software para todo tipo de organizaciones, especialmente en compañías del sector Financiero y Bursátil.

9.2 Objetivos del Sistema de Gestión de Seguridad de la Información

I. Incrementar la eficacia de SGSI mediante el análisis y tratamiento de riesgos de seguridad en la información.
II. Establecer lineamientos para administrar, proteger y resguardar objetivamente los activos de información propiedad de Sophos Solutions S.A.S Solutions SAS, mitigando el riesgo y las amenazas internas y/o externas, con la finalidad de asegurar el cumplimiento de la Confidencialidad, integridad y disponibilidad.
III. Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
IV. Determinar y gestionar las competencias necesarias para el personal que realiza tareas en la gestión y mantenimiento del SGSI.
V. Concientizar a todos los colaboradores referente a las políticas, procedimientos y lineamientos descritos en el Sistema de Gestión de Seguridad de la Información, garantizando el conocimiento del Sistema.
VI. Monitorear el cumplimiento de los requisitos de seguridad de la información implementados en Sophos Solutions S.A.S, garantizando la confidencialidad, integridad y disponibilidad.

9.3 Política del Sistema de Gestión de Seguridad de la Información

Para Sophos Solutions S.A.S, la protección de la información busca la disminución del impacto generado sobre sus activos de información, por los riesgos de seguridad identificados de manera sistemática con la finalidad de mantener un nivel de exposición que permita responder por la disponibilidad, integridad y confidencialidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados, promoviendo la mejora continua, así mismo fortaleciendo la cultura de seguridad de la información en los colaboradores, terceros, aprendices, practicantes y clientes de Sophos Solutions S.A.S.

9.4 Responsabilidad de Sophos Solutions S.A.S y sus Colaboradores Frente a Seguridad de la Información

I. Sophos Solutions S.A.S debe garantizar que los colaboradores y terceros conozcan y entiendan sus responsabilidades y deberes frente a la Seguridad de la Información, y que estén capacitados para cumplir con las Políticas establecidas en ejercicio de sus labores frente a la seguridad de la Información.

II. La periodicidad para reinducciones corresponde a 2 veces al año y para Inducción se imparte al ingreso del Colaborador

III. Los colaboradores de Sophos Solutions S.A.S son responsables del manejo adecuado de la información y los activos de información, mediante el cumplimiento de las políticas, procesos, procedimientos y controles establecidos.

IV. Todos los colaboradores deben respetar y cumplir las políticas, normas y procedimientos de Seguridad de la información establecidos, con el fin de garantizar la seguridad de los recursos tecnológicos de la compañía. Además, son responsables de informar al Responsable de Seguridad de la Información cualquier brecha o incidente que ocurra.

V. Los colaboradores que dentro de sus funciones manejen información clasificada como confidencial o restringida, deben cumplir con los controles asociados a cada nivel de seguridad de la información establecidos por Sophos Solutions S.A.S.

VI. Cuando se sospeche o se cuente con evidencia de fraude que vaya en contra de las políticas o lineamientos de Sophos Solutions S.A.S, se debe reportar inmediatamente al área legal.

VII. Reportar incidentes de seguridad y/o ciberseguridad de los sistemas de información de la compañía.

VIII. Velar por la protección de los activos de información entregados por parte de la compañía.

IX. Contribuir en la mejora continua del sistema de gestión de seguridad de la información.

9.5 Política de Activos de Información

SOPHOS SOLUTIONS S.A.S como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.
La información, archivos físicos, los sistemas, los servicios y los equipos (equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad o bajo la responsabilidad de SOPHOS SOLUTIONS S.A.S son activos de la compañía y se proporcionan a los colaboradores y terceros autorizados, para cumplir con los propósitos del negocio. Toda la información sensible de la organización, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados

I. Los Activos de Información de Sophos Solutions S.A.S deben ser identificados por los responsables de cada uno de los procesos

II. Todo colaborador interno o externo, que acceda a los activos de la información de la compañía o de nuestros clientes, tiene la responsabilidad de velar por la Integridad, Confidencialidad y Disponibilidad de la información que sea almacenada o manejada en función de sus labores.

III. Los colaboradores deben garantizar el buen manejo de todos los activos de información propios o del cliente, que tenga conexión local o desde un sitio externo con la organización; conexiones que podrán ser supervisadas o auditadas sin autorización previa. Cualquier evidencia del uso inadecuado o no autorizado, podrá ser utilizado para tomar las acciones administrativas o legales a las que haya lugar.

IV. El responsable de seguridad de la información deberá divulgar y velar por el cumplimiento de las políticas ante colaboradores, contratistas, consultores, proveedores y toda persona que tenga contacto con la información e infraestructura de la compañía.

V. La información accedida, procesada o generada por los colaboradores, consultores, contratistas, temporales o cualquier otro tercero, en el ejercicio de sus labores o en relación con la prestación de los servicios objeto del contrato, es propiedad de Sophos Solutions S.A.S.

VI. Los Activos de Información, sin importar su sensibilidad o criticidad, deben tener un responsable definido, quien será el responsable de vigilar que estos se encuentren debidamente protegidos contra amenazas que puedan afectar los criterios de Seguridad de la Información que generan, procesan o resguardan; además deberá realizar la clasificación de este con el apoyo del Responsable de Seguridad de la Información.

VII. Los Activos de Información deben ser tratados de acuerdo con los criterios de uso establecidos por Sophos Solutions S.A.S. Cualquier violación a este tratamiento debe ser notificada al responsable del Activo de Información y al Responsable de Seguridad de la Información.

VIII. Los activos de información se deben alinear al procedimiento R-SSI-01 Seguridad de la Información/ Activos de información.

9.6 Política de Control de Acceso

Se debe establecerse medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y servicios de TI. Los controles de acceso deben ser conocidos por todos los colaboradores de la compañía y limitar el acceso hacia los activos de información que no esté dentro de sus funciones.

I. Sophos Solutions S.A.S proveerá los recursos y accesos que cada colaborador requiera para sus funciones. Los accesos adicionales deben ser autorizados por el líder del colaborador y el responsable de seguridad de la información mediante el formato firmado y diligenciado F-SSI-04 Acuerdo uso Credenciales Internos.
II. El Área de Infraestructura será la encargada de la creación de los usuarios y la gestión de accesos en los diferentes sistemas y aplicativos. Para esto, se deberá aplicar las matrices y los respectivos procedimientos definidos por la organización.
III. La creación de repositorios a nivel de los proyectos debe ser efectuada por el área de Infraestructura, de acuerdo con previa solicitud de servicio la cual debe venir aprobada por el Líder del Proyecto y adjuntar la lista de chequeo repositorio que indica todos los parámetros del repositorio.
IV. Las solicitudes de usuarios externos deben ser aprobadas por el responsable del activo de información y el responsable de seguridad de la información antes de ser atendido. En caso de aplicarse, esto se dará por el tiempo requerido para efectuar el trabajo y será el dueño del proceso o proyecto y el externo los responsables de garantizar su uso adecuado.

9.6.1 Responsabilidades de los Colaboradores en el Control de Acceso

I. Los colaboradores deben ser informados sobre sus responsabilidades y compromisos frente a las políticas que la entidad dispone para el control de acceso.
II. Cualquier colaborador deberá identificarse y autenticarse bajo los mecanismos de acceso entregados por la organización (contraseñas, llaves, tarjetas de proximidad, tokens, biometría o demás) para el acceso a los activos de información de Sophos Solutions S.A.S de manera local o remota. Estos mecanismos no deberán ser compartidos o entregados a ninguna persona, a menos que sea bajo un procedimiento formal de custodia o exista un requerimiento legal.
III. Está prohibida la suplantación de un usuario y el uso de una sesión de trabajo iniciada por otro colaborador; si el colaborador sospecha que ha sido suplantado es su responsabilidad modificar su contraseña y notificar al responsable de seguridad de la Información.
IV. Para los sistemas y aplicaciones que requieran autenticación, se deberán aplicar las políticas que la entidad dispone para este fin.
V. Se debe evitar almacenar contraseñas en texto claro, en activos de información de uso compartido o en lugares públicos.

9.7 Política de Administración de Accesos

El Área de Infraestructura junto con el Área de Seguridad de la Información y los administradores de los aplicativos deberán velar por una administración adecuada para garantizar los accesos adecuados, con la finalidad de mitigar riesgos y vulnerabilidades que puedan atentar contra la confidencialidad, integridad y disponibilidad de los activos de información.

I. Es responsabilidad del Área de Infraestructura cuando se requiera, reportar los accesos de los diferentes sistemas y aplicativos a los líderes de proceso o proyecto, los cuales deberán hacer una revisión de estos y garantizar que sean adecuados de acuerdo con sus responsabilidades y que no dé lugar a conflicto de interés, adicionalmente deben reportar las novedades que considere necesarias de acuerdo con el procedimiento establecido.
II. Los líderes de procesos o proyectos y/o el Área de Gestión Humana deberán informar al Área de Infraestructura, las novedades de los colaboradores a su cargo.
III. El Área de Infraestructura deberá mantener un registro formal de todas las solicitudes de creación de usuarios, de la solicitud de asignación de accesos.
IV. Es responsabilidad del Área de Infraestructura cancelar inmediatamente los accesos de los colaboradores y usuarios externos reportados por el Área de Gestión Humana; a los que se les revoque la autorización, se desvinculen de la compañía o sufran pérdida/robo de sus credenciales de acceso.
V. El responsable del Área de Seguridad de la Información deberá efectuar revisiones periódicas con el objeto de identificar usuarios retirados o en período de vacaciones que se encuentren activos en el sistema. (Frecuencia mensual)
VI. Para casos de fuerza mayor en que se requiera la activación de un usuario que se encuentra en vacaciones o inactivado, el líder de proceso o proyecto deberá tramitar dicha autorización ante el Área de Seguridad de la Información.
VII. El Área de Gestión Humana debe reportar al Área de Infraestructura, los colaboradores que cesan sus actividades por más de 10 días hábiles y solicitar el bloqueo o redireccionamiento de su cuenta hasta el regreso.
VIII. Las herramientas de Office 365 cuenta con factor de doble autenticación para el ingreso y se renovara el token de manera periódica.

9.8 Política de Acceso a la Red

SOPHOS SOLUTIONS S.A.S cuenta con infraestructura de red (alámbrica e inalámbrica) en sus instalaciones, de la cual todos los colaboradores pueden acceder desde varios puntos de la organización. Las redes deberán contar con lineamientos de seguridad para mitigar cualquier vulnerabilidad o riesgos que atente contra la disponibilidad, integridad y confidencialidad de la información que se transmite.

I. Los colaboradores no deben interferir en los procesos de Infraestructura, ni en el buen funcionamiento de los servicios y recursos de esta mediante acciones deliberadas y deben velar porque el uso del internet sea aceptable.

i. No usar Internet o sistemas de la organización para acceder o descargar material que sea inapropiado, ofensivo, ilegal o que ponga en peligro la seguridad de la información.
ii. El uso de Internet para efectos distintos a las actividades laborales no es permitido.
iii. Las restricciones a ciertos sitios Web (que se consideren riesgosos o que afectan el rendimiento de la red y el entorno laboral) establecidas por la compañía deben ser acatadas.

II. Los puntos de accesos de red que no se estén utilizando no deben permanecer habilitados, en especial aquellos que se encuentren en salas y sitios públicos que no puedan ser vigilados.
III. Es obligatorio que todos los equipos de cómputo que se conectan a la red de la compañía estén dentro del dominio Sophos Solutions S.A.S.col.com que permitirá identificar y autenticar al usuario antes de ingresar al sistema o dispositivo y en el cual se especifiquen los usuarios autorizados y los niveles de acceso de acuerdo con su rol en la compañía.
IV. Los terceros que requieran acceso a internet deberán hacer uso únicamente de la red de *Invitados*; previa autorización por el Área de Seguridad de la Información.
V. Los equipos que se encuentren dentro de las instalaciones de la organización únicamente deberán conectarse a la red corporativa.
VI. La asignación de privilegios o excepciones a los colaboradores en los equipos y/o servicios, estarán determinados por el Área de Seguridad de la Información y deben revisarse a intervalos regulares y modificar o reasignar estos cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados de áreas, cambios de cargo, cambio de proyectos o terminación de la relación laboral.

9.9 Política de Acceso a Bases de Datos

Es responsabilidad del administrador de la Base de Datos garantizar el cumplimiento de las siguientes políticas:

I. Garantizar el cambio inmediato de la contraseña por defecto de los usuarios, en especial los que son administradores de la base de datos, al igual que inactivar las cuentas que no se utilicen.
II. Los administradores de la base de datos son los únicos autorizados para crear, modificar o eliminar objetos.
III. Se deberá definir lineamientos para la administración de los permisos “grant” o “Asignar permisos”
IV. Crear cuentas de usuarios personalizadas para la operación de la base de datos, incluso de aquellos usuarios que tengan privilegios de solo consulta.
V. No se podrá utilizar el usuario “root”, “administrador”, “administrator” o cualquier otro usuario con privilegio administrador por defecto.
VI. Realizar copia de seguridad de las bases de datos en medios que permitan su recuperación bajo criterios de integridad y disponibilidad.

9.10 Política de Conexiones Remotas

I. Todas las conexiones remotas dentro de la compañía están restringidas excepto para el Área de Infraestructura.

Nota: Si se requiere conexión remota, esta debe ser gestionada a través de una solicitud de servicio para su estudio, con previa aprobación del Área de Infraestructura y de Seguridad de la Información.

II. Las conexiones a la red de Sophos Solutions S.A.S desde sitios externos autorizadas en la compañía, para colaboradores y personas externas podrán ser realizadas únicamente a través de conexiones cifradas por medio de VPN Site to Site y Client to Site, en los casos de este último, para los colaboradores deberá estar consignadas en el formato F-SSI-05 Acuerdo uso Conexión Remota a VPN Client to Site, donde los colaboradores se comprometen con el uso adecuado y aplicación de buenas prácticas en el uso de la conexión.

III. Debe garantizarse que las conexiones remotas a servidores, equipos de comunicaciones, sistemas operativos o aplicaciones, se haga a través de conexiones seguras (https, sftp etc.)

IV. El Área de Infraestructura es responsable del bloqueo de las cuentas de usuarios VPN una vez el colaborador o externo se haya retirado de la compañía.

V. Debe garantizarse un proceso de desconexión automática por tiempos de inactividad en conexiones VPN.

VI. Las conexiones a escritorio remoto deben estar limitadas a una lista de control de acceso definido en la compañía.

VII. Se debe garantizar que las conexiones VPN sean efectivas exclusivamente al equipo asignado al colaborador o en su defecto a los equipos autorizados por el líder del proceso, proyecto y responsable de seguridad de la información.

VIII. El Área de Infraestructura utilizara herramienta licenciada para el soporte remoto a los colaboradores.

IX. Al usar tecnologías de VPN de Sophos Solutions S.A.S con equipos ajenos a la compañía, los colaboradores entienden y aceptan que sus máquinas deberán tener instalado antivirus y contar con las ultimas actualizaciones de seguridad en el sistema operativo.

X. Al usar tecnologías de VPN de Sophos Solutions S.A.S con equipos ajenos a la compañía, los colaboradores entienden y aceptan que no se podrá almacenar ningún tipo de información en de la compañía y/o de clientes.

9.11 Política de Acceso Físico

9.11.1 Política de Acceso a las Instalaciones

I. Debe existir un área de recepción que sólo permita la entrada de personal autorizado.

II. En caso de existir actividades de terceros en la compañía, la persona responsable del outsourcing al interior de la compañía debe garantizar la ejecución de los controles que apliquen según sus actividades.

III. Es necesario que exista una autorización previa por parte del Área de Infraestructura o cargo superior para el ingreso de personal externo a los cuartos técnicos. Este ingreso debe contar con un acompañamiento permanente por parte del área de infraestructura.

IV. Se debe exigir a todos los colaboradores, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ellos por Sophos Solutions S.A.S mientras permanezcan dentro de sus instalaciones.

V. Los visitantes se deben registrar en la recepción y deberán permanecer acompañados de un funcionario cuando se encuentren dentro de las instalaciones de la Entidad.
VI. Es responsabilidad de todos los colaboradores y externos acatar las normas de seguridad y mecanismos de control de acceso de la compañía.

9.11.2 Política de Acceso a Áreas Restringidas

I. El sitio escogido para ubicar los sistemas de información, equipos de cómputo y comunicaciones, deben estar protegidos por controles físicos (Tarjeta de Proximidad, lector biométrico u otros), para evitar el ingreso de personal no autorizado.
II. El perímetro de seguridad debe ser claramente definido y con un circuito de cámaras de seguridad que garanticen el control.
III. En caso de pérdida de llaves, deberán existir procedimientos que garanticen que las mismas no puedan ser utilizadas por extraños.
IV. Se deben tener extintores de incendios vigentes y debidamente probados, con categoría de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
V. Colaboradores, visitantes o terceras personas que ingresen a un área definida como restringida, deberán tener una identificación a la vista la cual será intransferible.
VI. Los Activos de Información deberán estar salvaguardados bajo los controles ambientales de acuerdo con su naturaleza y a las normas y regulaciones vigentes para edificaciones, instalaciones y protección de cualquier desastre natural o artificial.
VII. Para cambiar o trasladar un activo de información, los colaboradores deberán recibir aprobación previa de forma clara y expresa del dueño del activo de información y del responsable de seguridad de la información. Dicha aprobación no podrá ser superior a 3 meses.
VIII. Los Activos de Información que prestan servicios críticos deben recibir mantenimiento preventivo y correctivo para asegurar la continua disponibilidad de los servicios que soportan.
IX. El cableado de energía eléctrica y comunicaciones que transportan datos o brindan apoyo a los servicios de información estarán protegidos contra intercepción o daños.
X. Se deberá garantizar la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas:
Sistema Eléctrico suplementario
Sistema de Control de acceso
Sistema de aire acondicionado
Sistema de protección contra incendios

9.11.3 Política de Trabajo en Áreas Protegidas.

I. En las áreas donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:

i. No se deben consumir alimentos ni bebidas.
ii. No se deben ingresar elementos inflamables.
iii. No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.

iv. No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
v. No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
vi. No se permite el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

II. Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.

9.11.4 Política de Seguridad de los Equipos Fuera de las instalaciones de la compañía.

I. Los colaboradores que requieran usar los equipos fuera de las instalaciones de Sophos Solutions S.A.S deben velar por la protección de estos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometidos la imagen o información del sector.
II. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información sensible, se deberá realizar inmediatamente el respectivo reporte de acuerdo con el procedimiento Gestión de Incidentes de Seguridad y se deberá poner la denuncia ante la autoridad competente, si aplica.

9.12 Política de Creación de Contraseñas

El Área de Infraestructura deberá velar por que la infraestructura tecnología y los sistemas de información desarrollados y administrados por SOPHOS SOLUTIONS S.A.S cuenten con lineamientos de seguridad para garantizar un ingreso seguro mediante la creación de políticas en los sistemas para garantizar que la contraseña sea adecuada, con la finalidad de mitigar riesgos y vulnerabilidades que puedan atentar contra la confidencialidad, integridad y disponibilidad de los activos de información.

I. Las contraseñas de sistemas y aplicativos deberá contener como mínimo 8 caracteres dentro de los cuales deben contener:
    i. Al menos un número (0, 1…,9)
    ii. Letras mayúsculas y minúsculas de la a-z, A-Z
    iii. Al menos un carácter especial ($ & @ #)
    iv. No contener palabras de diccionario
II. Como características adicionales de la administración de las contraseñas se deberá cumplir con los siguientes parámetros de configuración:
    i. Deberán caducar por lo menos cada 42 días
    ii. El sistema deberá validar que no se puedan reutilizar las últimas 5 contraseñas utilizadas
    iii. Bloquear la cuenta después de 3 intentos fallidos
    iv. Solicitar la contraseña anterior antes de asignar una nueva contraseña.

III. Todas las contraseñas de las cuentas administradoras del sistema (root, administradores de servidores Windows, cuentas de administración de aplicaciones y bases de datos) deben ser cambiados cada seis meses y de forma controlada.
IV. Las herramientas de corporativas de Office 365 cuentan con factor de doble autenticación para el ingreso y se renovara el token de manera según aplique
V. Esta política aplica únicamente a las herramientas desarrolladas por Sophos Solutions S.A.S y/o herramientas la cuales se tenga integración con el directorio activo de la organización.
VI. Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:
    i. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios. Las contraseñas no deberán ser reveladas.
    ii. Los funcionarios y contratistas deben digitar siempre su usuario y contraseña para acceder a las diferentes aplicaciones de la compañía; la contraseña no se debe guardar de forma automática en los inicios de sesión de las aplicaciones, igualmente al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.
    iii. Es deber de los colaboradores reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

9.13 Política de Creación y Deshabilitación de Usuarios

El Área de infraestructura deberá velar por que la infraestructura tecnología y los sistemas de información desarrollados y administrados por SOPHOS SOLUTIONS S.A.S cuenten con lineamientos de seguridad para garantizar un ingreso seguro mediante la creación de usuarios centralizados, con la finalidad de mitigar riesgos y vulnerabilidades que puedan atentar contra la confidencialidad, integridad y disponibilidad de los activos de información.

I. La solicitud de una nueva cuenta deberá hacerse mediante el procedimiento establecido.
II. Los colaboradores que reciben los usuarios asignados deberán aceptar la responsabilidad y políticas de la entrega de los nuevos recursos.
III. No debe concederse una cuenta a personas que no sean colaboradores de la empresa, a menos que estén debidamente autorizados por el Área de Gestión Humana.
IV. El Área de Gestión Humana notificara al Área de Infraestructura mediante correo electrónico la desvinculación de un colaborador para su respectivo bloqueo y deshabilitación de usuario.

9.14 Políticas de Instalación, Uso y Administración de Equipos de Cómputo

9.14.1 Política de Instalación de Equipos

I. Todos los computadores, servidores y dispositivos móviles, propios o de terceros que sean conectados a la red de datos de la compañía, deberán contar con un software,

antivirus o alguna otra herramienta actualizada para detectar software malicioso (malware).

II. Todo equipo que sea asignado a un usuario y que haya sido utilizado por otro, deberá entregarse libre de información, programas y/o configuraciones que utilizaba el usuario anterior y deberá eliminarse los perfiles que correspondan a usuarios previos. La información podrá ser entregada al líder del proceso o proyecto a través de los procedimientos que disponga la entidad para tal fin.

III. Las actualizaciones de sistemas operativos deberán estar en las últimas versiones disponibles. Para los casos en que las configuraciones actuales no permitan garantizar esto, se debe definir un plan de migración para actualizar la configuración no superior a 6 meses.

IV. Únicamente los usuarios administradores de dominio podrán crear o modificar otros usuarios administradores de dominio.

V. No se debe conceder permisos de usuario administrador de máquina a ningún usuario. Para los casos que sea necesario, se deberá contar la autorización del líder del proceso o proyecto, el Área de Infraestructura y el Área de Seguridad de la Información en el cual se deberá diligenciar y firmar el formato F-SSI-03 Acuerdo uso Privilegios Internos y se deberá establecer por un periodo de tiempo; una vez finalizado este tiempo, el colaborador deberá gestionar ante infraestructura la restricción ya que en caso contrario este tendrá toda la responsabilidad de lo ocurrido en el equipo por fuera del tiempo permitido y las acciones disciplinarias que la organización determine.

VI. Se deberá inhabilitar la cuenta "*Administrador"* por defecto de la máquina y crear la cuenta "*Sophosadmin*" y debe tener definida una contraseña fuerte y conocida únicamente por el Área de Infraestructura.

VII. El Área de Infraestructura deberá tener un registro de todos los equipos propiedad de la compañía.

VIII. El Área de Infraestructura debe mantener un inventario actualizado de los equipos de cómputo instalados en los centros de procesamiento de datos; adicionalmente se debe llevar una bitácora con los cambios que se realicen.

IX. Los equipos que sean de propósito específico y tengan una misión crítica asignada, deben estar ubicados en un área que cumpla con los requerimientos de seguridad física, condiciones ambientales y con fuentes de energía temporal en casos de contingencia.

X. Se debe garantizar que los equipos de comunicaciones (Switch, Router, Access Point, entre otros) no tengan configuraciones por defecto (usuarios, claves comunidades, etc.) y deberán ser configurados según la necesidad, antes de ponerlos en producción.

XI. Se deberá etiquetar los equipos de cómputo instalados en los centros de procesamiento de datos, permitiendo ubicar el equipo de forma rápida y precisa.

XII. Los equipos que estén en modalidad de leasing y sean entregados al proveedor, deberán pasar por el procedimiento de borrado seguro el cual es ejecutado por parte del Área de Infraestructura.

XIII. Únicamente el personal del Área de Infraestructura está autorizado para instalar nuevos equipos. Es necesario garantizar que dichos equipos cuenten con las medidas de seguridad requeridas, antes de la puesta en producción.

XIV. Los colaboradores que cuenta con usuarios administrador local NO están autorizados para la instalación de herramientas que requieran licenciamiento, en el caso de que el

proyecto o el área requiera la herramienta con la licencia deberá ser escalado formalmente mediante Flow2l al Área de infraestructura.

XV. Los servicios críticos que estén expuestos en Internet deberán contar con pruebas de Ethical Hacking al menos a 1 vez al año. Los sistemas internos deberán contar con pruebas de vulnerabilidades al menos cada 2 años.
Debe garantizarse que los computadores se bloquen automáticamente después de 3 minutos de inactividad, con el objetivo de prevenir suplantaciones o accesos no autorizados.

9.14.2 Políticas de Uso de Computadores, Servidores, Impresoras y Periféricos

I. La infraestructura tecnológica: servidores, computadores, impresoras, UPS, escáner y equipos en general; no pueden ser utilizados en funciones diferentes a las de la compañía.
II. Se debe asegurar que los equipos estén conectados a las instalaciones eléctricas apropiadas según corresponda, cuando se trabaja desde las instalaciones de la compañía.
III. Los equipos deben estar ubicados en sitios adecuados bajo condiciones que garanticen su seguridad y buen estado, cuando se trabaja desde las instalaciones de la compañía. En el caso de trabajo remoto asegurar que los equipos no queden desatendidos en lugares públicos y/o en zonas inseguras.

9.14.3 Política de Destrucción o Reubicación de Equipos Electrónicos

I. Para los equipos que se den de baja o sean donados, se debe garantizar que no contengan información de la entidad, haciendo uso de herramientas especializadas para tal fin.
II. Para todo equipo (desktop, laptop, equipos de red, entre otros) que sea reasignado, el Área de Infraestructura deberá garantizar que no contenga información de usuarios anteriores o rastros de servicios, configuraciones o aplicaciones antes alojados.
III. Solo el Área de Infraestructura está autorizada para reubicar equipos una vez se cuente con autorización del área administrativa por medio de una solicitud de servicio.
IV. Se debe actualizar todas las novedades derivadas del traslado y/o reubicación de los equipos.
V. Ningún equipo podrá ser retirado de las instalaciones de la compañía, sin la autorización por escrito por parte del líder de proceso o proyecto. Para los colaboradores cuyas labores requieran retirar los equipos de forma recurrente o periodos prolongados (superior a 1 mes) se deberá solicitar autorización del área de infraestructura y seguridad de la información. En ningún caso una autorización podrá superar 1 año de validez. En el caso de una pandemia, manifestaciones y/o riesgos que comprometa a las instalaciones de la compañía y/o el bienestar de los colaboradores, se validara en el comité para otorgar el permiso general.
VI. Para los equipos que se entreguen al proveedor, deberán ser entregados totalmente formateados, contando con los lineamientos para el borrado seguridad de la información.

9.14.4 Política Protección contra Software Malicioso

I. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información deberán estar protegidos mediante herramientas y software

de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos dados por código malicioso.

II. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización del Área de Seguridad de la Información, y deberán ser actualizados permanentemente.

III. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o la red tecnológica de Sophos Solutions S.A.S o de cualquier Cliente.

IV. Todos los medios de almacenamiento que se conecten a equipos de la infraestructura de la compañía deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la Seguridad de la Información.

9.14.5 Política Gestión de Registro (log)

I. Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática deberán generar registros de eventos (logs) que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información.

II. El tiempo de retención de los logs estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red.

III. Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica y sistemas de información deberá ser reportado al Área de Seguridad de la Información mediante el procedimiento de Gestión de Incidentes de seguridad.

9.14.6 Política Gestión de Vulnerabilidades Técnica

I. El Área de infraestructura y Seguridad de la Información se en cargaran de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.

II. El Área de Seguridad de la Información será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la Entidad.

III. El Área de Seguridad de la Información de la compañía realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

IV. Periódicamente, la correspondiente Área de Seguridad de la Información realizará una verificación de alertas de seguridad emitidas por organizaciones y foros de Seguridad de la Información de orden nacional y/o internacional, con el fin de verificar la información más reciente que se encuentre disponible respecto a vulnerabilidades y eventos de seguridad que se hayan presentado o que sean susceptibles de ocurrencia y ser notificadas al Área de Infraestructura.

V. Únicamente el Área de Seguridad de la Información estará autorizada para la ejecución de los análisis de vulnerabilidad y pruebas de hacking ético en los sistemas de información e infraestructura tecnología de Sophos Solutions S.A.S.

VI. Se deberá contratar un proveedor de seguridad al menos una vez al año para la ejecución de los análisis de vulnerabilidad y pruebas de hacking ético en los sistemas de información e infraestructura tecnología de Sophos Solutions S.A.S.

9.15 Política de Uso de Dispositivos Móviles y Extraíbles

I. Por defecto todos los computadores de la compañía deberán tener bloqueado los puertos USB, Unidad CD/DVD. En caso de ser requerido, se deberá contar con autorización del líder de proceso o proyecto y el responsable de seguridad de la información.
II. La autorización de acceso USB, CD-ROM u otros dispositivos, deben ser consignadas en el formato F-SSI-07 Responsabilidad para Desbloqueo de Puertos para su respectivo control.
III. Todos los servidores deberán mantener inhabilitado los puertos de conexión USB, y unidades de CD-ROM y DVD, las cuales deberán habilitarse únicamente por el administrador del servidor en caso de mantenimientos o actualizaciones de software.
IV. Se debe evitar el almacenamiento de información confidencial y restringida de la compañía en dispositivos móviles.
V. Está prohibido el uso de dispositivos móviles por personal externo en los centros de procesamiento de datos. En caso de ser necesario se deberá contar con la autorización del área de Infraestructura y dicho acceso deberá ser registrado en la bitácora.
VI. No está autorizado el uso del correo corporativo desde dispositivos móviles, exceptuando Presidencia, Vicepresidencias, Delivery Manager y PMO´s.
VII. No está dentro de las funciones del área de Infraestructura dar soporte técnico a los dispositivos móviles que no sean propiedad de la organización.
VIII. En el caso de que se requiera acceder a la información de Sophos Solutions S.A.S mediante dispositivos móviles personales, deberá ser autorizado por parte del Área de Seguridad mediante caso en Flow2l o en su defecto por correo electrónico.
IX. En el caso de que se requiera acceder a la información de Sophos Solutions S.A.S mediante dispositivos móviles personales, el colaborador deberá acceder al correo electrónico o al repositorio de Sophos Solutions S.A.S mediante la cuenta corporativa accediendo únicamente a través de la aplicación Portal Empresas de Microsoft.

9.16 Política Copias de Seguridad

El Área de Infraestructura deberá garantizar que la información generada, procesada y custodiada por Sophos Solutions S.A.S Solutions SAS, se encuentre respaldada, mediante copias de seguridad, que preservarán la disponibilidad de los datos empresariales

Todas las copias de respaldo de la Entidad deben ser incrementales. El backup incremental sólo copia los datos que han variado desde la última operación de backup de cualquier tipo

I. Está prohibida la generación de copias de seguridad para uso personal.
II. Se deben definir y ejecutar procedimientos para la generación de copias de seguridad y la restauración de estas, con una periodicidad definida de acuerdo con los lineamientos de la organización.
III. Una vez cumplido el tiempo establecido de custodia para una copia de seguridad, se debe aplicar los lineamientos de disposición final establecidos por la organización para tal fin.
IV. Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de

emergencia.

V. Para garantizar que la información de los colaboradores sea respaldada, es responsabilidad de cada uno mantener copia de la información que maneja en los repositorios de la compañía (OneDrive y/o SharePoint).

VI. La política se complementa con la política de Backup que maneja el Área de Infraestructura.

9.17 Política Seguridad y Contenido de Internet

Internet es una herramienta de trabajo que permite navegar en sitios relacionados o no con las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes políticas:

I. Se deben implementar mecanismos para monitorear que no se modifiquen los enlaces de los sitios Web de Sophos Solutions S.A.S o la resolución de su DNS por personal no autorizado (interno o externo).

II. Los controles de acceso a páginas de Internet deben ser definidos de acuerdo con la necesidad del área o proyecto, sin ir en contra del cumplimiento de las demás políticas de Seguridad de la Información.

III. Está prohibido el acceso a Internet a través de dispositivos distintos a los proporcionados por la organización (módems, páginas túnel, proxy anónimo). En caso de ser necesario el uso de estos, deben contar con la aprobación previa del responsable de Seguridad de la Información.

IV. El acceso al WIFI para Visitantes debe estar aprobado por el Área de Seguridad de la Información y el acceso al WIFI corporativo está sujeto a condiciones propias del proyecto y debe estar aprobado por el área de Seguridad

V. Está prohibida la descarga de archivos ejecutables, archivos de música, video o software, el uso de programas de mensajería instantánea diferente a la establecida por la organización, juegos en línea o cualquier otro componente que pueda generar propagación de virus, software malicioso o cualquier otra amenaza que comprometa los criterios de seguridad de la Información en los Activos.

VI. Publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos

VII. Prohibiciones en manejos de contenido:

   i. Tomar Fotos del código fuente
   ii. Transferencia de información de propiedad de la compañía o del cliente como direcciones IP, usuarios, passwords, código fuente, facturación a través de chats, correos no corporativos…
   iii. Envío de información confidencial o restringida por mensajería instantánea ejm: WhatsApp.

VIII. La navegación deberá estar alineada a los grupos que se definen en la consola de antivirus.

9.17.1 Uso de Computación en la Nube

I. Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos sin autorización.
II. Sophos Solutions S.A.S podrá implementar servicios privados en la nube, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.
III. Para el ingreso a los servicios de Nube (Azure, AWS, Google Cloud, etc) únicamente se podrá realizar con la cuenta corporativa o credenciales que sean otorgadas por los clientes para la ejecución de sus actividades laborales.

9.18 Política Desarrollo Seguro

Durante el desarrollo de los sistemas de información se deberán cumplir con los lineamientos de seguridad definidos basado en buenas prácticas para desarrollo seguro de aplicativos acorde a la necesidad de cada proyecto, así como con metodologías y procedimientos para la realización de pruebas de seguridad.

I. Para el análisis y diseño de las aplicaciones, se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

II. Asegurar que se realice el análisis e implementación de los requerimientos de seguridad en el software y/o sistemas de información que se desarrollen o se adquieran, debe incluir controles de autenticación y auditoría de usuarios, verificación de los datos de entrada y salida, y que se implementen buenas prácticas para un desarrollo seguro, acorde a la necesidad del proyecto.

III. Realizar las pruebas para asegurar que se cumplen con los requerimientos de seguridad establecidos en los ambientes, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción, considerando nuevos sistemas, nuevas funcionalidades, mantenimientos en aplicaciones construidas internamente, construidas por proveedores, aprovisionadas en la nube o híbrido de las anteriores acorde a la necesidad del proyecto y el alcance.

IV. Administración de Claves:

    I. Todas las claves serán protegidas contra modificación y destrucción, y serán protegidas contra copia o divulgación no autorizada mediante almacenamiento cifrado en las bases de datos.

V. Control de Acceso a los Códigos Fuente:

    Para reducir la probabilidad de alteración de programas fuentes, se aplicarán las siguientes normas:

    i. Administrar las distintas versiones de una aplicación.
    ii. Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.

iii. Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuente.

iv. Realizar las copias de Seguridad y pruebas de restauración de los programas fuente cumpliendo los requisitos de seguridad establecidos por la organización y Soluciones en los procedimientos que surgen de la presente política, acorde a la necesidad del proyecto y el alcance.

VI. Lineamiento de Control de Cambios:

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la realización de cambios, acorde a la necesidad del proyecto y el alcance.
Para ello se deben contemplar los siguientes controles.

i. Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso, acorde a la necesidad del proyecto y el alcance.

ii. Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.

VII. Se deberá estandarizar el ciclo de vida, criterios de seguridad y de calidad en el desarrollo de software.

VIII. Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.

9.18.1 Separación de ambientes

Sophos Solutions S.AS proveerá los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.

I. No deberán realizarse pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.

II. El ambiente de prueba debe emular el ambiente de producción lo más estrechamente posible.

III. No se permite la copia de información sensible desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia debe ser previamente ofuscada y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida y se elimine de forma segura después de su uso.

IV. Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.

9.19 Política Pantalla y Escritorio Limpio

Las áreas de trabajo de los colaboradores deben localizarse preferiblemente en ubicaciones que no queden expuestas al acceso de personal externas.

Los equipos que queden ubicados cerca de zonas de atención o tránsito de público deben situarse de forma que las pantallas no puedan ser visualizadas por personas no autorizadas y deben ser aseguradas, en lo posible, mediante candado de seguridad u otro medio que impida que sean sustraídos.

I. Equipo desatendido por el usuario:
   i. Toda vez que el usuario se ausente de su lugar de trabajo debe bloquear su estación de trabajo de forma de proteger el acceso a las aplicaciones, documentos y servicios que proporciona Sophos Solutions S.A.S Solutions.
   ii. Las estaciones o puestos de trabajo y equipos de cómputo deben tener aplicado el estándar relativo a protector de pantalla definido por la Organización.
   iii. La pantalla de autenticación a la red debe requerir solamente la identificación de la cuenta y clave; y no entregar o solicitar información.
   iv. La autentificación de usuarios debe ser requerida cada vez que el equipo se encienda, reinicie, bloque o después de aparecer el protector de pantalla.

II. Escritorio y Pantallas limpias.
   i. Toda vez que un colaborador se ausenta de su lugar de trabajo, junto con bloquear su equipo de trabajo, debe guardar en un lugar seguro documentos, medios magnéticos, u óptico removible que contenga información confidencial.
   ii. Al finalizar la jornada laboral, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, clasificados como confidencial y/o restringido.
   iii. Si el usuario está ubicado cerca de zonas de atención al público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.
   iv. Los equipos de reproducción de información (por ejemplo: impresoras, fotocopiadoras), deben estar ubicados en lugares con acceso controlado y cualquier documentación confidencial o sensible debe ser retirada inmediatamente del equipo).
   v. No almacenar ningún tipo de documento en el escritorio de los equipos de la compañía.

9.20 Política Relación con Proveedores

La presente política reúne lineamientos que deben cumplir los proveedores que tengan acceso a la información de Sophos Solutions S.A.S Solutions SAS e intercambien, procesen, almacenen,

modifiquen o creen nueva información confidencial propiedad de Sophos Solutions S.A.S Solutions SAS., o los que utilicen sus equipos de cómputo en la red de compañía, esto con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

III. Todo proveedor y/o tercero que tenga acceso a los activos de información y preste servicios a Sophos Solutions S.A.S debe contar con políticas, normas y estándares de Seguridad de la Información al interior de su organización; las cuales deben desarrollarse y mantenerse actualizadas acorde con los riesgos a los que se ve enfrentada su organización.

IV. Todo proveedor y/o tercero que deba acceder a la red de datos Sophos Solutions S.A.S deberá pasar por la aprobación del Área Riesgos y Seguridad de la Información previo a un análisis de seguridad en el equipo de cómputo el cual requieran conectar.

V. Establecer con Sophos Solutions S.A.S el procedimiento adecuado para el borrado seguro de la información propiedad de la compañía, sus clientes y/o terceros. Este procedimiento deberá ser desarrollado antes o durante el transcurso de la relación contractual.

VI. Controlar la salida de información propiedad de Sophos Solutions S.A.S. que se encuentre alojada bajo los dispositivos que administra y controla EL PROVEEDOR, estos controles deberán ser notificados a Sophos Solutions S.A.S. durante el transcurso de la relación contractual.

VII. Informar a Sophos Solutions S.A.S a través del correo seguridad.info@sophossolutions.com cualquier fuga, pérdida o alteración de información de propiedad de la compañía, sus clientes y/o usuarios y la correspondiente medida de mitigación

VIII. Intercambiar la información confidencial de Sophos Solutions S.A.S. de forma segura, cifrándola de acuerdo con los lineamientos y buenas prácticas de seguridad definidas por Sophos Solutions S.A.S.

IX. EL PROVEEDOR responde directamente por el acceso que sus empleados tengan a documentos confidenciales o accesos a herramientas de Sophos Solutions S.A.S. y deberá entenderse que este acceso es estrictamente temporal, sin otorgarle derecho alguno de titularidad o copia sobre dicha información. Así mismo, el empleado deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación contractual entre EL PROVEEDOR y Sophos Solutions S.A.S.

X. Se prohíbe expresamente el uso de los recursos proporcionados por Sophos Solutions S.A.S para actividades no relacionadas con el servicio contratado.

XI. Se prohíbe expresamente Introducir voluntariamente en la red de Sophos Solutions S.A.S. cualquier tipo de malware (programas, macros, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos y sistemas de información.

XII. Reportar evento sospechoso o incidente de seguridad de la información que comprometa la confidencialidad, integridad y confidencialidad de la información asociado a las actividades que desarrolla para Sophos Solutions S.A.S

XIII. Permitir a SOPHOS SOLUTIONS S.A.S SOLUTIONS, visitas a instalaciones y revisión de auditoria relacionados con los servicios prestados, así mismo proporcionar información de evidencia cuando aplique, siguiendo los lineamentos de protección de información entre las partes.

XIV. En el caso del que el PROVEEDOR deba tener colaboradores en las oficinas de Sophos Solutions S.A.S deberán estar identificados durante la permanencia en las instalaciones. La identificación deberá estar en un lugar visible.

9.21 Política de Control de Cambios Operativos

I. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte del Área de Seguridad de la Información y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

II. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica deberá ser validado por parte del Área de Seguridad de la información, con la finalidad de realizar los análisis de vulnerabilidades determinados previo a la publicación del servicio.

9.22 Política Gestión de Incidentes de Seguridad de la Información

I. Los colaboradores de Sophos Solutions S.A.S deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

II. Para gestionar los incidentes de Seguridad de la Información deberá existir como mínimo un colaborador con conocimientos en el manejo de incidentes en las Áreas de Seguridad de la Información.

III. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con el Área Legal.

IV. Se debe establecer y mantener actualizado la Matriz RACI de los colaboradores involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad de la Información.

V. Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

VI. La compañía deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

9.23 Política Seguridad de la Información en la Continuidad del Negocio

I. La Seguridad de la Información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.
II. La compañía deberá contar con un Plan de Continuidad de Negocio (BCP) que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.
III. Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Continuidad de Negocio.

9.24 Política Criptografía

El Área de Infraestructura desarrollará e implementará los lineamientos para los controles criptográficos en los sistemas de información y comunicaciones soportados sobre la infraestructura tecnología de Sophos Solutions S.A.S teniendo en cuenta las siguientes directrices.

I. Los lineamientos sobre uso, protección y duración de las claves criptográficas se realizarán a través del directorio activo durante todo su ciclo de vida.
II. Las comunicaciones mediante VPN deberán contar con algoritmos de cifrado para garantizar la confidencialidad e integridad de la información.
III. Deberá verificar que todo sistema de información que requiera realizar transmisión de información clasificada como confidencial o restringida cuente con mecanismos de cifrado de datos.
IV. Deberá utilizar controles criptográficos para la transmisión de información mediante herramientas autorizadas (Office 365).
V. Los equipos de todos los colaboradores de Sophos Solutions S.A.S, que se encuentren unidos al dominio de la compañía tendrán mecanismos para el cifrado de disco mediante la herramienta que designe el Área de Infraestructura.
VI. Los servicios que sean publicados a internet desde la infraestructura tecnológica de Sophos Solutions S.A.S contaran con certificados digitales.
VII. Adoptar los controles para el etiquetado digital de la información.

9.25 Política de Correo Electrónico e Intercambio de Información

La asignación de una cuenta de correo electrónico de Sophos Solutions S.A.S se da como herramienta de trabajo para cada uno de los colaboradores que la requieran para el desempeño de sus funciones, así terceros previa autorización.

I. Los medios de intercambio de Información (Internet, correo electrónico, mensajería instantánea, drives, entre otros.) deben contar con un análisis de riesgos, que permitan diseñar e implementar controles efectivos para la protección de la Información que viaja a través de estos.

II. Esta restringido el envío de correos electrónicos a dominios no autorizados por la compañía, sujetos a la condición del proyecto.
III. El acceso a cuentas de correo electrónico personal debe estar restringido.
IV. Los colaboradores no deben realizar actividades que impliquen pérdida o degradación del rendimiento de los activos de Información, incluyendo aquellas utilizadas para el intercambio de información, tales como envío de cadenas, descarga de archivos de gran tamaño, fotos personales, música, entre otros.
V. La información confidencial o restringida que sea trasmitida por correo o por algún aplicativo de la organización, deberá viajar cifrada y en la medida en que sea posible el usuario emisor y receptor o en su defecto Cliente/Servidor, deberán incluir certificados digitales.
VI. Ningún colaborador está autorizado para utilizar cuentas de correo asignadas a otra persona; en el caso de requerirse por ausencias, vacaciones, licencias, entre otros, se deben usar mecanismos de redirección de mensajes de acuerdo con lo establecido en el manual de inducción corporativa.
VII. Los colaboradores deberán estar en la capacidad de identificar archivos adjuntos maliciosos y contenidos sugestivos (pornografía, publicidad, cadenas, entre otros). En caso tal de recibir este tipo de información, se debe informar al responsable de Seguridad de la Información, para tomar las medidas de control necesarias.
VIII. Él envió de información únicamente se puede realizar por los canales y medios autorizados los cuales son SharePoint, OneDrive, Teams, Correo Corporativo y demás herramientas que se consideran y autoricen por parte del Área de Seguridad de la Información.
IX. Toda la información generada que se requiera transmitir por correo electrónico corporativo deberá ser enviada de manera cifrada.

Para reportar cualquier caso deberá enviar un correo a seguridad.info@sophossolutions.com

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