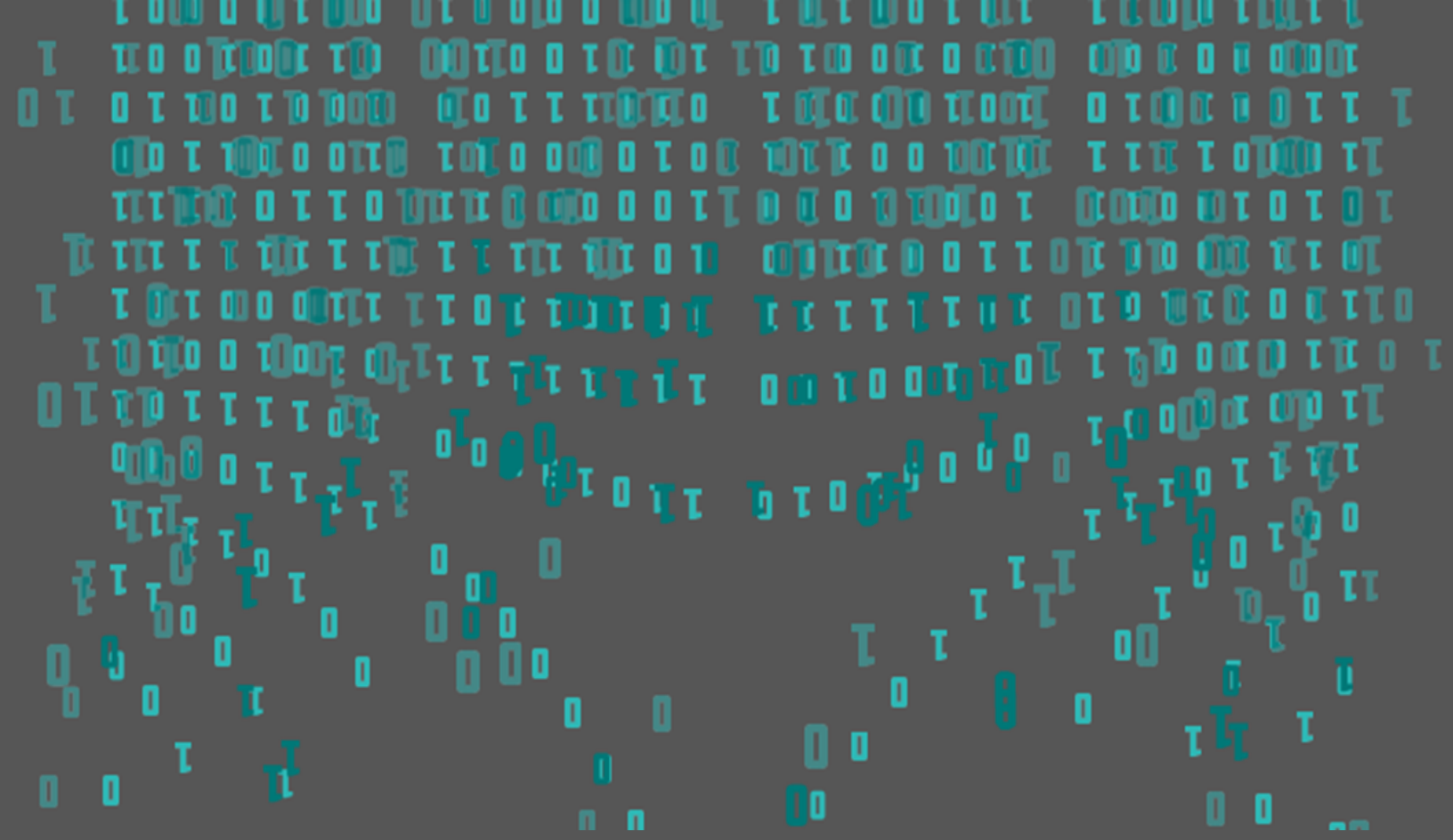


OPEN LATINOAMERICA

Políticas de Seguridad de la Información y Ciberseguridad

1. Introducción

2. Objeto

3. Alcance

4. Descripción

4.1. Política General De Seguridad De La Información Y Ciberseguridad

4.1.1. Cumplimiento De La Política General De La Seguridad De La Información Y Ciberseguridad

4.1.2. Declaración De La Política General De Seguridad De La Información Y Ciberseguridad

4.1.3. Ámbito De Seguridad De La Información Y Ciberseguridad

4.1.4. Política De Seguridad De Información Y Ciberseguridad

4.1.5. Revisión De La Política General De Seguridad De La Información Y Ciberseguridad

5. Organización De La Seguridad De La Información Y Ciberseguridad

5.1. Compromiso De Openlatinoamerica S.A.S.

5.2. Establecer El Sistema De Gestión De Seguridad De La Información Y Ciberseguridad

5.3. Confidencialidad De La Información

5.4. Partes Externas (Intermediarios Y Vinculados)

6. Gestión De Activos

6.1. Responsabilidad De Los Activos

6.2. Clasificación De La Información

7. Seguridad De Los Recursos Humanos

7.1. Antes De La Contratación Laboral

7.2. Seguridad Durante La Vigencia De La Contratación
7.3. Terminación O Cambio De La Contratación Laboral
8. Seguridad Física Y Del Entorno
9. Gestión De Comunicaciones Y Operaciones
9.1. Procedimientos Y Responsabilidades De Operación
9.2. Gestión De La Prestación Del Servicio Por Terceras Partes
9.3. Planificación Y Aceptación De Sistemas
9.4. Protección Contra Códigos Maliciosos
9.5. Respaldo
9.6. Gestión De La Seguridad De Las Redes
9.7. Manejo De Medios De Almacenamiento De Información
9.8. Intercambio De Información
9.9. Monitoreo
10. Control De Acceso
10.1. Requisito Del Negocio Para El Control De Acceso
10.2. Gestión Del Acceso De Usuarios
10.3. Registro De Usuarios
10.4. Administración De Privilegios
10.5. Administración De Contraseñas Para Usuario
10.6. Responsabilidades De Los Propietarios De Activos De Información
10.7. Control Del Acceso A Las Redes
10.8. Control De Acceso Al Sistema Operativo
10.9. Control De Acceso A Las Aplicaciones
10.10. Computación Móvil Y Trabajo Remoto

11. Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información

11.1. Requisitos De Seguridad De Los Sistemas De Información

11.2. Procesamiento Correcto De Las Aplicaciones Del Sistema

11.3. Controles Criptográficos

11.4. Seguridad De Los Archivos Del Sistema

11.5. Seguridad En Los Procesos De Desarrollo Y Soporte

11.6. Gestión De La Vulnerabilidad Técnica

12. Gestión De Los Incidentes De La Seguridad De La Información Y Ciberseguridad

12.1. Reporte Sobre Los Eventos Y Las Debilidades De La Seguridad De La Información Y Ciberseguridad.

12.2. Gestión De Incidentes Y Mejoras En La Seguridad De La Información Y Ciberseguridad

13. Gestión De La Continuidad Del Negocio

13.1. Aspectos De Seguridad De La Información Y Ciberseguridad, De La Gestión De La Continuidad Del Negocio

14. Cumplimiento

14.1. Cumplimiento De Los Requisitos Legales

14.2. Cumplimiento De Las Políticas Y Las Normas De Seguridad Y Cumplimiento Técnico

14.3. Consideraciones De La Auditoría De Los Sistemas De Información

15. Aspectos Reglamentarios

16. Indicadores De Cumplimiento

17. Glosario

1. INTRODUCCIÓN

La Política General establece la directriz de la Compañía sobre la seguridad de la información y ciberseguridad, las estructuras organizacionales de soporte y el perfil de los procedimientos que se aplican para proporcionar un adecuado nivel de seguridad.

La política orienta el Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC), con el cual se establece que el diseño, la implantación y el mantenimiento de procesos, los responsables de su ejecución, y las herramientas de tecnología, se realizarán en un marco que considere los principios de Confidencialidad, Integridad y Disponibilidad que proporcionan seguridad a los activos de información que se vinculan con la razón de ser de Openlatinoamerica S.A.S cuando se haga referencia a Openlatinoamerica S.A.S.

El Sistema de Gestión de Seguridad de la Información (SGSIC) tiene un enfoque de mejoramiento continuo PHVA “Planear- Hacer- Verificar- Actuar”.

• **Planear:** Es una fase de diseño del SGSIC, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

• **Hacer:** Es una fase que envuelve la implantación y operación de los controles.

• **Verificar:** Es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSIC.

• **Actuar:** En esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSIC a máximo rendimiento.

2. OBJETO

La presente Política de Seguridad de la Información tiene los siguientes objetivos:

a. Proteger los activos de información de Openlatinoamerica S.A.S (tecnología, información y personas) de posibles riesgos que puedan afectar los principios de la Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad).
b. Proporcionar los lineamientos de seguridad de la información y ciberseguridad, dirigido a los empleados y vinculados de Openlatinoamerica S.A.S para su entendimiento y aplicación.
c. Establecer los fundamentos para la gestión y el funcionamiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad de Openlatinoamerica S.A.S
d. Lograr la concientización y la cultura de la seguridad de la información y ciberseguridad, en los empleados y vinculados.
e. Definir los roles y responsabilidades de los propietarios de la información para promover el cumplimiento del SGSIC.
f. Disminuir los incidentes que afecten la productividad y el buen nombre de la Compañía.

3. ALCANCE

La Política de Seguridad de la Información involucra a todos los directivos, empleados, intermediarios y vinculados a Openlatinoamerica S.A.S que puedan acceder a los activos de información de la Compañía a través de cualquier medio, quienes deben cumplir con la presente política, los lineamientos y mantener un nivel adecuado de protección de la información que tengan bajo su responsabilidad y custodia.

4. DESCRIPCIÓN

4.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

4. 1. 1. CUMPLIMIENTO DE LA POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Todos los empleados, vinculados o externos deben cumplir la presente Política del Sistema de Gestión de Seguridad de la Información y Ciberseguridad. El no cumplirla tendrá la aplicación de las sanciones establecidas en el reglamento Interno de Trabajo y las demás aplicables al Marco Legal Colombiano, conforme a la magnitud y característica del aspecto incumplido.

4. 1. 2. DECLARACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- **Openlatinoamerica S.A.S** reconoce la información como un activo de valor que debe ser protegido.
- **Openlatinoamerica S.A.S** se compromete con la protección de la información y de sus sistemas de información con el objetivo de asegurar la Confidencialidad, Integridad y Disponibilidad.
- **Openlatinoamerica S.A.S** reconoce y soporta el rol de la Unidad de Seguridad de la información y Ciberseguridad, y se compromete con su gestión.

La Política General de Seguridad de la Información y Ciberseguridad define el marco de referencia para el Sistema de Gestión de Seguridad de la Información de Openlatinoamerica S.A.S. el cual debe ser cumplido por todos los empleados y vinculados que tengan relación contractual con la Compañía.

La presente política de Seguridad de la Información y Ciberseguridad está directamente relacionada con los manuales de políticas y procedimientos vigentes de los procesos de la Compañía, los cuales se encuentran sujetos a un proceso constante de actualización y hacen parte integral de este documento.

4. 1. 3. ÁMBITO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El Sistema de Gestión de Seguridad de la Información y Ciberseguridad está basado en las mejores prácticas de acuerdo con lo establecido a las normas ISO/NTC 27001:2013 e ISO/NTC 27032:2012, los cuales proveen un nivel adecuado de aseguramiento para la protección de la Confidencialidad, Integridad y Disponibilidad de los activos de información de Openlatinoamerica S.A.S, los siguientes son los Dominios emanados de la norma que se adoptan por el sistema:

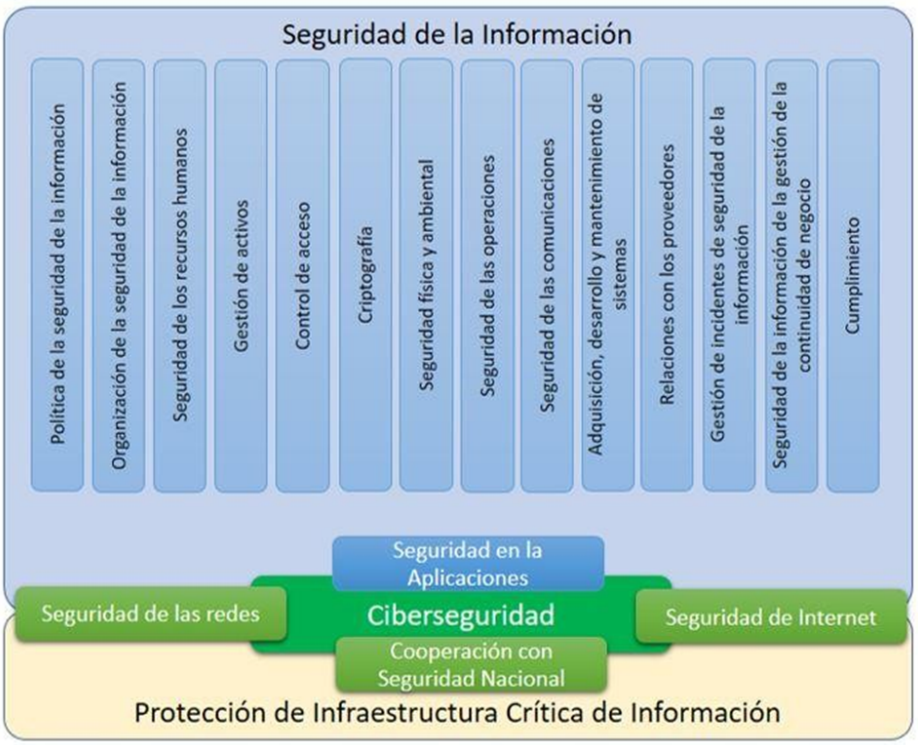


Figura 1. Dominios de Seguridad de la Información y Ciberseguridad

4. 1. 4. POLÍTICA DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD

La presente Política General de Seguridad de la Información y Ciberseguridad está ha sido revisada por el Comité de Seguridad de la Información y ha sido aprobada por la Junta Directiva de la compañía.

4. 1. 5. REVISIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El Comité de Seguridad de la Información es el responsable de la revisión de la presente Política. Todo cambio que se efectúe a la Política deberá consignarse, ser aprobado y divulgado en una nueva versión.

La revisión y actualización de esta política se realizará por lo menos **una vez al año** tomando en consideración lineamientos estratégicos de la alta dirección, análisis de riesgos, nuevas regulaciones y buenas prácticas.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Openlatinoamerica S.A.S. a través de su Sistema de Gestión de la Seguridad de la Información y Ciberseguridad determina las actividades, compromisos, responsabilidades y lineamientos, de empleados y vinculados, que utilizan o acceden a los recursos de la Compañía, para el cumplimiento de los objetivos estratégicos y la gestión adecuada de la información.

La Openlatinoamerica S.A.S cuenta con una unidad responsable de gestionar la Seguridad de la Información y Ciberseguridad, la cual cumple las siguientes funciones:

• Definir el plan estratégico de seguridad de la información y ciberseguridad.

• Identificar los riesgos de seguridad de la información y ciberseguridad con la finalidad de establecer, recomendar y ejecutar los debidos controles.

• Gestionar los activos de información, con la finalidad de identificarlos, clasificarlos, inventariarlos y fomentar la implementación de los controles necesarios para garantizar su confidencialidad, disponibilidad e integridad.

• Detectar y/o gestionar adecuadamente los incidentes de seguridad de la información y ciberseguridad, con el propósito de contenerlos y generar el conocimiento necesario para su prevención.

• Validar y verificar la gestión de las vulnerabilidades que puedan amenazar la plataforma tecnológica y activos de información, para su gestión y mitigación de riesgos asociados.

• Validar y verificar la gestión de accesos lógicos a la plataforma tecnológica.

• Verificar la activación y custodia de logs para determinar la correcta trazabilidad de eventos en la plataforma tecnológicas y sistemas de información que soportan las funciones críticas de la organización.

• Evaluar y supervisar las tecnologías de seguridad de la información y ciberseguridad que sean implementadas en la organización.

• Identificar necesidades de monitoreo de componentes y verificar que éste sea llevado a cabo.

• Definir estándares de seguridad de la información y ciberseguridad que sean necesarios adoptar por la organización y verificar el cumplimiento de éstos.

• Responder ante los requerimientos de cumplimiento sobre seguridad de la información y ciberseguridad, que se presenten en la organización.

• Ejecutar el plan de concientización en seguridad de la información y ciberseguridad de la organización.

• Gestionar proveedores para el cumplimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

• Incorporar controles de seguridad de la información y ciberseguridad en el ciclo de desarrollo del software y verificar su cumplimiento.

• Definir políticas seguras de gestión de cambio para asegurar la continuidad de negocio y verificar su cumplimiento.

• Verificar la ejecución adecuada del esquema de respaldo y recuperación de datos de la organización.

• Identificar e informar a las áreas responsables sobre necesidades de controles de seguridad física que sean necesarios para la protección de los activos de información.

• Efectuar monitoreo sobre el cumplimiento de las políticas de seguridad de la información y ciberseguridad establecidas por las Compañías.

• Garantizar que se cuente con los recursos necesarios para el mantenimiento y aplicación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

5.1. COMPROMISO OPENLATINOAMERICA S.A.S

Openlatinoamerica S.A.S demuestra el apoyo y compromiso manifestado por parte de la Alta Dirección quien promueve el Sistema de Gestión de Seguridad de la Información y Ciberseguridad mediante:

1) Confirmación del cumplimiento de los objetivos y planes de Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC).
2) Definición de las funciones y responsabilidades a cada Propietario de la información.

5.2. ESTABLECER EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

En desarrollo de la presente política, Openlatinoamerica S.A.S apoyado en la estructura de la Seguridad de la Información del numeral 5 del presente documento, designa como líder del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSIC) al Comité de Seguridad de la Información (OSI), para velar por el establecimiento, cumplimiento, mantenimiento, control y gestión del SGSIC.

5.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

Openlatinoamerica S.A.S por medio de la Gerencia de Gestión Humana, exige a sus empleados, vinculados o cualquier ente externo que tenga acceso a los activos de información o a su infraestructura, firmar y cumplir con un acuerdo de confidencialidad definido por la Compañía.

5.4. PARTES EXTERNAS (INTERMEDIARIOS Y VINCULADOS)

- **Openlatinoamerica S.A.S**. gestiona y controla los accesos a los activos de información que se encuentran a cargo de entes externos.
- **Openlatinoamerica S.A.S**. mediante el Comité de Seguridad de la Información, evalúa los riesgos de seguridad de la información, para determinar los requisitos de control y las implicaciones para la seguridad de la información, en caso de aceptarse el riesgo resultante por parte del Líder del Proceso involucrado.

6.GESTIÓN DE ACTIVOS

6.1. RESPONSABILIDAD DE LOS ACTIVOS

Openlatinoamerica S.A.S. por medio de los propietarios de la información, mantiene los controles necesarios para la protección y conservación de la información.

6.2. CLASIFICACIÓN DE LA INFORMACIÓN

A través de la clasificación de activos de información, la Unidad de Seguridad de la Información y Continuidad de Negocio identifica, clasifica y valora la información, con el compromiso y participación activa de cada propietario de los activos de información, para protegerla en todas sus formas o medios en que se encuentre, preservando la Confidencialidad, Integridad y Disponibilidad de acuerdo al nivel de clasificación establecido.

7.SEGURIDAD DE LOS RECURSOS HUMANOS

7.1. ANTES DE LA CONTRATACIÓN LABORAL

Openlatinoamerica S.A.S por medio de la Gerencia de Gestión Humana, verifica los antecedentes del personal que ingresa teniendo en cuenta el tipo y clasificación de la información a la que tendría acceso acorde a la definición de cargos y responsabilidades. Se debe tener en cuenta de acuerdo con el cargo que se vaya a desempeñar, que no todos los procesos de contratación en la Compañía deben ser manejados de igual forma, cada rol y sus responsabilidades deben tener un manejo diferente con relación a la verificación de antecedentes, procedencia, formación, conocimientos y otros.

7.2. SEGURIDAD DURANTE LA VIGENCIA DE LA CONTRATACIÓN

Openlatinoamerica S.A.S por medio de la Gerencia de Gestión Humana busca los mecanismos necesarios para que los empleados y vinculados, den cumplimiento a los acuerdos de Confidencialidad de la información durante el tiempo de permanencia en la Compañía.

7.3. TERMINACIÓN O CAMBIO DE LA CONTRATACIÓN LABORAL

Al finalizar el contrato laboral con Openlatinoamerica S.A.S, los empleados entregan formalmente los activos de información que se encuentren a su cargo al propietario del activo de información y reciben la aprobación por parte de éste, para la entrega del Paz y salvo correspondiente.

8. SEGURIDAD FÍSICA Y DEL ENTORNO

Todos los centros de almacenamiento de información de Openlatinoamerica S.A.S o instalaciones que estén involucrados con los activos de información deben cumplir con las normas de seguridad física y ambiental, para garantizar que la información manejada en estas permanezca siempre protegida de accesos físicos por parte de personal no autorizado o por factores ambientales que le puedan afectar. La Vicepresidencia de Tecnología y Operaciones en conjunto con la Gerencia de Logística y Seguridad serán los responsables de velar por el cumplimiento de estos controles.

La información que manejan los empleados de Openlatinoamerica S.A.S durante los horarios habituales de trabajo o fuera de ellos, dentro o fuera de las instalaciones de la Compañía, es responsabilidad de éstos para la conservación de los controles establecidos para proteger la Confidencialidad, Integridad y Disponibilidad de la información.

9.GESTIÓN DE COMUNICACIONES Y OPERACIONES

9.1. PROCEDIMIENTOS Y RESPONSABILIDADES DE OPERACIÓN

Para la gestión y operación de todos los sistemas y servicios de procesamiento de información, Openlatinoamerica S.A.S establece las actividades y responsabilidades que incluyen el desarrollo de instrucciones adecuadas para la operación y procedimientos de respuesta a incidentes operativos, de seguridad de la información y ciberseguridad.

Para reducir el riesgo de uso no adecuado de los sistemas de información, sin intención, por error o negligencia, el Líder del proceso proporciona al área de Tecnología y Operaciones la información necesaria para propender por la segregación de funciones en los diferentes roles establecidos en Openlatinoamerica S.A.S

9.2. GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR TERCERAS PARTES

Openlatinoamerica S.A.S por medio de la Unidad de Seguridad de la Información y Continuidad de Negocio define los controles de seguridad que garanticen la adecuada y eficiente entrega de servicios por parte de proveedores. Se deben identificar y documentar los riesgos de seguridad de la información, con relación a los servicios que presta el proveedor, para adicionar en el contrato las correspondientes cláusulas de seguridad que ayuden a la mitigación de estos.

Openlatinoamerica S.A.S define “Acuerdos de Niveles de Servicios” (ANS) con respecto a la prestación de servicios establecida, incluyendo controles de cumplimiento y monitoreo, adicionalmente siempre que se involucre uso de información debe adicionar cláusulas de confidencialidad y uso autorizado y borrado seguro de la Información.

9.3. PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

Openlatinoamerica S.A.S establece los requerimientos sobre la planeación de la capacidad de los sistemas o servicios de procesamiento de información, sobre los controles que aplica para la aceptación y desarrollo de actualizaciones o nuevas versiones de los sistemas de información.

Para todas las nuevas actualizaciones a sistemas, versiones y nuevos sistemas de información Openlatinoamerica S.A.S establecerá criterios de aceptación, y deberá realizar planes de pruebas para estos nuevos requerimientos antes de su definitiva aceptación y puesta en producción.

9.4. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Openlatinoamerica S.A.S. por medio de la Unidad de Seguridad de la Información y Continuidad de Negocio, define los controles para prevenir y detectar la introducción de código o software malicioso y realizar las acciones inmediatas en caso de presentarse un incidente. Es responsabilidad del área de Tecnología y Operaciones implementar los controles definidos para la protección contra códigos maliciosos.

9.5. RESPALDO

Openlatinoamerica S.A.S. a través del área de Tecnología y Operaciones, establece normas y procedimientos rutinarios que permiten tener respaldo de la información, planes de pruebas y simulaciones de la recuperación oportuna de los datos, registrando los eventos o fallos y monitoreo de los equipos de recuperación.

9.6. GESTIÓN DE LA SEGURIDAD DE LAS REDES

Openlatinoamerica S.A.S por medio del área de Tecnología y Operaciones establece los controles y medidas específicas para la protección de la red por donde se transmita información, ya sean redes públicas o privadas de la compañía.

Los sistemas por donde se procesa y trasmite la información, deben contar con registros de monitoreo de las actividades realizadas (Ej. Logs).

9.7. MANEJO DE MEDIOS DE ALMACENAMIENTO DE INFORMACIÓN

Para proteger los documentos físicos, soportes de información, como: discos, cintas y otros; Openlatinoamerica S.A.S por medio del propietario del activo de información, debe establecer en conjunto con la Unidad de Seguridad de la Información y Continuidad de Negocio los procedimientos operativos para la protección de los mismos.

9.8. INTERCAMBIO DE INFORMACIÓN

Openlatinoamerica S.A.S a través del área de Tecnología y Operaciones, provee los mecanismos necesarios para que la información, datos y software intercambiado entre las organizaciones permanezcan controlados y cumplan con los principios de Seguridad de la información y ciberseguridad.

Openlatinoamerica S.A.S establece los acuerdos, procedimientos y normas necesarias para el intercambio de información entre organizaciones, considerando las implicaciones relacionadas con interfaces, correo e intercambio electrónico de datos.

9.9. MONITOREO

Openlatinoamerica S.A.S a través de la Unidad de Seguridad de la Información, velará por la protección de los activos de información a través del monitoreo de las actividades que se realizan en los diferentes sistemas de procesamiento de información.

10.CONTROL DE ACCESO

10.1. REQUISITO DEL NEGOCIO PARA EL CONTROL DE ACCESO

El área de Tecnología y Operaciones establece, documenta y revisa por lo menos una vez al año la Política de Control de Acceso Lógico, basado en los requisitos del negocio y de la seguridad para el acceso a los activos y sistemas de información. En esta política deben establecerse las reglas y derechos de cada usuario o grupo de usuarios.

10.2. GESTIÓN DEL ACCESO DE USUARIOS

Todos los usuarios, vinculados, proveedores y/o clientes de servicios de Openlatinoamerica S.A.S que interactúan con los diferentes sistemas de información de la Compañía, son administrados con el fin de evitar el acceso no autorizado.

Openlatinoamerica S.A.S. a través del área de Tecnología y Operaciones controla la asignación de los derechos de acceso a los sistemas y servicios, los cuales abarcan las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de nuevos usuarios hasta su eliminación o desactivación cuando ya no sea requerido dicho acceso a los sistemas de información y servicios de la Compañía.

Para los usuarios que tengan acciones privilegiadas en los sistemas y servicios de información, el área de Tecnología y Operaciones conjuntamente con la Unidad de Seguridad de la Información y Continuidad de Negocio, definirán y establecerán los correspondientes derechos con acceso privilegiado.

10.3. REGISTRO DE USUARIOS

Openlatinoamerica S.A.S provee los elementos necesarios para el registro de usuarios cuando estos acceden a los diferentes sistemas y servicios de información, los cuales deben incluir:

1. Identificador único para cada usuario.

2. Verificación del nivel de acceso asignado.

3. Entregar al usuario la relación escrita de sus derechos de acceso.

4. Mantenimiento de un registro formalizado de usuarios por aplicación.

5. Revocar de acuerdo al tiempo establecido, las autorizaciones de acceso a usuarios que finalizan su contratación o actividades con la Compañía.

10.4. ADMINISTRACIÓN DE PRIVILEGIOS

La asignación y uso de privilegios de acceso a los sistemas y servicios de información de Openlatinoamerica S.A.S. son restringidos, controlados y documentados por Tecnología y Operaciones.

10.5. ADMINISTRACIÓN DE CONTRASEÑAS PARA USUARIO

Openlatinoamerica S.A.S a través del área de Tecnología y Operaciones, realiza la asignación de contraseñas, la cuales son controladas mediante un proceso de gestión formal.

Las contraseñas deben ser almacenadas en un sistema informático con protección de acceso de lectura y escritura.

10.6. RESPONSABILIDADES DE LOS PROPIETARIOS DE ACTIVOS DE INFORMACIÓN

Cada propietario de activos de información es responsable de establecer de manera formal la revisión anual de los derechos de acceso de los usuarios y registrar los resultados, acciones realizadas, y en dado caso los planes de acción efectuados, para apoyar en el mantenimiento de los controles del acceso a datos y servicios de información de Openlatinoamerica S.A.S

10.7. CONTROL DEL ACCESO A LAS REDES

- Los usuarios de Openlatinoamerica S.A.S están autorizados para tener acceso directo a las aplicaciones y sistemas de información, para cuyo uso están específicamente autorizados.
- Todos los accesos de los usuarios a sistemas y aplicaciones de información de la Compañía son controlados por medio de autenticación segura.
- Todas las conexiones remotas que se realicen a los sistemas de información de Openlatinoamerica S.A.S poseen control de autenticación y son monitoreadas para evitar conexiones por personas no autorizadas.
- Openlatinoamerica S.A.S cuenta con los mecanismos para controlar el acceso a los usuarios en la red y en los recursos compartidos de la Compañía.
- El área de Tecnología y Operaciones, aplica controles de enrutamiento para el aseguramiento de las conexiones entre computadores y flujos de información.

10.8. CONTROL DE ACCESO AL SISTEMA OPERATIVO

Todo acceso a los sistemas operativos de Openlatinoamerica S.A.S. está controlado por registros de inicio seguro. Tecnología y Operaciones, define lineamientos para la conexión de los usuarios al sistema informático, para minimizar la posibilidad de accesos no autorizados.

Los procesos de conexión a usuarios deben mostrar el mínimo de información posible, para no exponer nuestros sistemas.

10.9. CONTROL DE ACCESO A LAS APLICACIONES

El acceso lógico al software, a la información y a las funciones de los sistemas de información de Openlatinoamerica S.A.S. es únicamente para usuarios autorizados, de acuerdo con la Política de Control de Acceso Lógico definida por la Unidad de Seguridad de la Información y Continuidad de Negocios.

10.10. COMPUTACIÓN MÓVIL Y TRABAJO REMOTO

Tecnología y Operaciones conjuntamente con la Unidad de Seguridad de la Información y Continuidad de Negocio, antes de proveer los servicios necesarios para el trabajo remoto, considera y evalúa los riesgos asociados a seguridad de la información y ciberseguridad, con el fin de establecer los controles requeridos para la ejecución de sus actividades laborales.

La Unidad de Seguridad de la Información y Continuidad de Negocio, exige a los vinculados la protección de los equipos en el lugar de trabajo remoto, así como la existencia de acuerdos relacionados con el buen uso de los activos de información.

En lugares públicos o áreas desprotegidas que estén fuera del alcance de la seguridad de la Compañía, se deberá tener especial cuidado cuando se utilicen dispositivos móviles (propios o asignados y que tengan acceso a las aplicaciones de la Compañía), se deberán instalar en estos dispositivos protección adecuada contra código o software malicioso para evitar el acceso no autorizado a la divulgación de la información almacenada y procesada en éstos.

11. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

11.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

La Unidad de Seguridad de la Información y Continuidad de Negocio identifica y acuerda con los responsables de los desarrollos, los requerimientos de seguridad que deben contener los sistemas de información durante las etapas iniciales y antes de su implementación. Los requerimientos de Seguridad de la información y ciberseguridad deben estar documentados como parte de la planeación del proyecto.

11.2. PROCESAMIENTO CORRECTO DE LAS APLICACIONES DEL SISTEMA

Para las aplicaciones y sistemas de información de Openlatinoamerica S.A.S. Tecnología y Operaciones implementa medidas de control de seguridad y registros de auditoría o de actividades correspondientes. En el diseño de los controles se incluyen las validaciones de los datos de entrada y de salida y los de procesamiento interno que maneja la aplicación.

11.3. CONTROLES CRIPTOGRÁFICOS

El área de Tecnología y Operaciones provee los mecanismos necesarios para que la información confidencial sea enviada o recibida de forma segura a través de los medios establecidos.

11.4. SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

Todos los accesos otorgados a los archivos de los sistemas y al código fuente de las aplicaciones de Openlatinoamerica S.A.S están controlados y separados, para asegurar que las actividades de soporte y proyectos son llevadas a cabo de forma segura. La separación de los entornos es responsabilidad del área de Tecnología y Operaciones.

El código fuente de las aplicaciones se deberá mantener aislada o por fuera de los sistemas productivos y con los respectivos controles para su custodia.

Los empleados de la Gerencia de Gestión y Calidad de Software y aquellos que estén autorizados por el responsable de la información de acuerdo al rol que desempeñen, son los únicos autorizados para acceder y compilar el código fuente de las aplicaciones, en ambiente de desarrollo.

11.5. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

Tecnología y Operaciones establece los parámetros necesarios para el control de los procesos de desarrollo, soporte en el mantenimiento de la seguridad del software y de la información manejada por las aplicaciones de los sistemas. Cada cambio propuesto para los diferentes sistemas de información es revisado para asegurar que no afecta la seguridad del mismo, bases de datos o del sistema operativo.

11.6. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

Tecnología y Operaciones establecerá normas y remediaciones oportunas a los riesgos resultantes de la explotación de las vulnerabilidades técnicas, priorizando acorde a la criticidad de cada uno. Se realizarán análisis de vulnerabilidades a la red como mínimo dos veces al año con los planes de remediación correspondientes, con el fin de mitigar y minimizar los riesgos de las vulnerabilidades encontrados en los sistemas de procesamiento de información.

12. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

12.1. REPORTE SOBRE LOS EVENTOS Y LAS DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

La Unidad de Seguridad de la Información y Continuidad de Negocio establece mecanismos para que los empleados y vinculados reporten las debilidades detectadas, que permitan el registro oportuno de eventos informáticos que puedan afectar las operaciones de la Compañía, y estos sean mitigados para minimizar el daño causado y facilitar la obtención de cualquier evidencia asociada.

Openlatinoamerica S.A.S establecerá esquemas de comunicación y colaboración con autoridades en el cumplimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

12.2. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Unidad de Seguridad de la Información y Continuidad de Negocio establece los responsables y lineamientos necesarios para la recolección de evidencias y para las remediaciones a los incidentes de seguridad que se presenten en la Compañía.

13.GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

13.1. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD, DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Para llevar a cabo la gestión de Continuidad de Negocio en Openlatinoamerica S.A.S define e implementa un plan para reducir el impacto de la interrupción de la operación causada por desastres naturales, accidentes y fallos de seguridad por medio de la combinación de controles preventivos y de recuperación en cada uno de los procesos de la compañía.

La Unidad de Seguridad de la Información y Continuidad de Negocio fomenta y coordina con los líderes de los procesos tecnológicos y de negocio sobre la creación, pruebas y mantenimiento de los diferentes planes de continuidad.

14. CUMPLIMIENTO

14.1. CUMPLIMIENTO DE LOS REQUISITOS LEGALES

Openlatinoamerica S.A.S debe definir, documentar y mantener actualizados los requisitos estatutarios, reglamentarios, contractuales y la propiedad intelectual, con el fin de definir e implementar los controles, medidas y responsabilidades específicas para su cumplimiento.

14.2. CUMPLIMIENTO DE LAS POLÍTICAS Y LAS NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

Openlatinoamerica S.A.S a través de la Unidad de Seguridad de la Información y Continuidad de Negocio vela por el cumplimiento de las políticas y normas de seguridad estipuladas por la Compañía y entes de control para que se dé el correcto funcionamiento de los procedimientos de Seguridad de la información y ciberseguridad.

14.3. CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Las auditorías realizadas a los sistemas de procesamiento o almacenamiento de información deben ser planificadas evaluando el riesgo al que se encuentre expuesta la información debido a interrupciones, fallas, errores o ajustes.

Las herramientas que sean utilizadas durante el proceso deben estar protegidas contra acceso no autorizado.

15. ASPECTOS REGLAMENTARIOS

Openlatinoamerica S.A.S dentro del Sistema de Gestión de Seguridad de la información y ciberseguridad se apoya en la serie ISO 27000 de la norma para la implementación del sistema y acoge todos los aspectos reglamentarios de ley y sus posteriores actualizaciones que apliquen a la Compañía dentro del marco normativo:

• NTC ISO/IEC 27001:2013 Tecnología de la Información. Sistemas de Gestión de la Seguridad de la Información (SGSI).

• NTC ISO/IEC 27032:2012 Tecnología de la Información. Directrices para la seguridad cibernética.

• Ley 1273 de 2009 de Delitos Informáticos.

• Constitución de la República de Colombia. Artículo 15. Derecho a la intimidad.

• Código Contencioso Administrativo. Artículo 17. Derecho a la Información.

• Constitución de la República de Colombia. Artículo 23. Derecho de petición.

• Constitución de la República de Colombia. Artículo 74. Documentos públicos.

• Circular Básica Jurídica (CE 029/14) - Capítulo I del Título II de la Parte I.

• Ley 1581- 2012 Protección de Datos Personales.

• Decreto 884 - 30 abril de 2012 Ministerio de Trabajo – Teletrabajo.

• Acuerdo 38 de 2002 Archivo General de la Nación.

• Acuerdo 049 de 200 Archivo General de la Nación Conservación de Documentos.

16. INDICADORES DE CUMPLIMIENTO

Los indicadores de cumplimiento del sistema de gestión de Seguridad de la información y Ciberseguridad están relacionados con algunos de los controles establecidos en esta política, los cuales sirven como instrumento de observación e indican el grado de cumplimiento con el sistema.

Estos indicadores hacen parte integral de algunos de los procedimientos establecidos en el sistema. Es responsabilidad de la Unidad de Seguridad de la Información y Continuidad de Negocio la gestión de indicadores del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

17. GLOSARIO

ACTIVO DE INFORMACIÓN: Conocimiento o datos que tienen valor para la entidad o el individuo.

CIBERAMENAZA O AMENAZA CIBERNÉTICA: Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

CIBERATAQUE O ATAQUE CIBERNÉTICO: Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

CIBERESPACIO: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

CIBERSEGURIDAD: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

INCIDENTE DE CIBERSEGURIDAD: Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.

VINCULADO: Hace referencia a entes que tienen relación con la Compañía que prestan un servicio a Seguros del Estado S.A. (Proveedores, Intermediarios, Outsourcing y delegados).

OPEN LATINOAMERICA

Chile:
Apoquindo 4700 - Piso 11 - Oficina 1101
Las Condes - Santiago - Chile
WhatsApp: +56 931973383

Colombia:
Calle 108 Nº 45-30 - El Chicó Bogotá
Móvil: +57 315 6718785

www.openlatinoamerica.com