Lineamientos de Ciberseguridad

OD-TI-002

ODINSA

CONTENIDO

AUDIENCIA

Estos lineamientos aplican a todos los colaboradores de Odinsa, Odinsa Gestor Profesional, Odinsa Vías y Odinsa Aeropuertos, contratistas y terceros que tengan acceso a los recursos tecnológicos de la Compañía.

1. CONTEXTO DEL DOCUMENTO

Este documento hace parte del modelo de ciberseguridad, el cual contempla entre otros los siguientes elementos:

Ilustración 1 – Elementos del modelo de ciberseguridad

Política de ciberseguridad: La política de ciberseguridad es un documento de alto nivel que denota el compromiso de la dirección con la ciberseguridad, y por lo cual establece el marco de actuación que orienta las pautas de comportamiento de colaboradores y terceros involucrados en el manejo de la información y de las operaciones; así como las medidas de protección a nivel de seguridad de las tecnologías que habilitan los negocios.

Lineamientos / Normas: Hace referencia al conjunto de órdenes, directrices, principios, o reglas específicas sobre determinado tema asociado a la seguridad, y deben estar alineados con la política de ciberseguridad.

Anexos técnicos: Documentos técnicos correspondientes a guías[1], procedimientos[2], estándares[3] para la implementación de las políticas de ciberseguridad.

2. DEFINICIONES

Activos de información: Conjunto de datos recolectados y transformados que tienen un valor para el negocio de tipo estratégico, operativo, económico, técnico, jurídico o normativo; por ende, su necesidad de protegerlos.

Ciber activos: Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.

Comité de ciberseguridad: Es un grupo multidisciplinario liderado por el área de ciberseguridad el cual garantiza la implementación de las acciones para asegurar el cumplimiento de la política de ciberseguridad.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. ISO/IEC 27002:2013

Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. ISO/IEC 27002:2013

Evento de ciberseguridad: es la presencia identificada de un estado del sistema, o un servicio que indica un incumplimiento posible a la política de ciberseguridad, una falla de los controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Fraude: Cualquier acto u omisión intencionada, diseñada para engañar a los demás; llevado a cabo por una o más personas con el fin de apropiarse, aprovecharse o, hacerse de un bien ajeno, sea material o intangible, de forma indebida, en perjuicio de otra y generalmente por la falta de conocimiento o malicia del afectado.

Incidente de ciberseguridad: está indicado por un solo evento o una serie de eventos inesperados o no deseados de ciberseguridad que tienen una probabilidad significativa de poner en peligro las operaciones del negocio y amenazar la seguridad de la

[1] **Guías**: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas y lineamientos. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
[2] **Procedimientos**: Definen específicamente como las políticas, estándares, mejores prácticas y guías serán implementadas en una situación dada. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible.
[3] **Estándar**: Es un documento establecido por consenso que sirve de patrón, modelo o guía que se usa de manera repetitiva. Los estándares de seguridad suelen ser actualizados periódicamente ya que dependen directamente de la tecnología.

información.

Integridad: Propiedad de la información relativa a su exactitud y completitud. ISO/IEC 27002:2013

Plan de continuidad del negocio: Plan documentado y probado con el fin de responder ante una emergencia en los procesos de negocio de manera adecuada, logrando así el mínimo impacto a la operación del negocio.

Propietario: Es el responsable del activo de información a ser protegido.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Sistemas de información: Se entiende como el conjunto de tecnologías, procesos, aplicaciones de negocios y software disponibles para las personas dentro de una organización.

Terceros: Se entiende por terceros los clientes, contratistas, empresas de outsourcing y temporales.

Usuario: Es el que utiliza la información para llevar a cabo las funciones de sus trabajos.

3. OBJETIVO

Establecer el conjunto de lineamientos, normas, principios, directrices, y reglas para garantizar la ciberseguridad de la Compañía, de acuerdo con lo establecido en la política de ciberseguridad y asegurando el cumplimiento de los objetivos y de las obligaciones legales conforme al ordenamiento jurídico vigente en la Compañía.

4. ORGANIZACIÓN PARA LA CIBERSEGURIDAD

La Compañía establece la estructura para gestionar la ciberseguridad con instancias y responsabilidades claramente definidas, con el fin de asegurar un adecuado funcionamiento del programa de seguridad de las tecnologías de información y operaciones.

4.1. Estructura para la ciberseguridad

La estructura para la ciberseguridad estará compuesta por:

4.1.1. Junta directiva

Responsable por la adopción y adecuada implementación de las políticas y normas de la ciberseguridad, el establecimiento de una estructura organizacional que proporcione guía y dirección para la gestión de la ciberseguridad, otorgar los recursos necesarios para la implementación de medidas en pro de la ciberseguridad, y ejercer frente a sus

colaboradores el liderazgo apropiado para disminuir los riesgos digitales.

4.1.2. Comité Estratégico de Ciberseguridad:

- Aprobar la estrategia organizacional que proporciona la dirección en la gestión de la ciberseguridad.
- Aprobar la política de ciberseguridad y sus lineamientos.
- Gestionar el mapa de riesgo de ciberseguridad y evaluar la efectividad de las medidas de tratamiento adoptadas.
- Verificar la adopción de recomendaciones emitidas por entes de control, auditores, compañías de seguros, áreas de riesgos, entre otras.
- Reportar a la junta directiva y la alta dirección.

4.1.3. Comité táctico de ciberseguridad

- Proponer lineamientos para materializar la política de ciberseguridad.
- Identificar riesgos y vulnerabilidades del entorno, monitoreando constantemente el ambiente cibernético.
- Supervisar la implementación de medidas de seguridad.
- Proponer el programa de pruebas de intrusión y de simulacros ante ataques cibernéticos.
- Ajustar el programa de capacitación y conciencia para todos los miembros de la organización.
- Diseñar e implementar programas de comunicación y capacitación ampliados para fortalecer la cultura y las capacidades del sistema de gestión de la ciberseguridad.
- Comunicar y reportar el estado de la ciberseguridad de la organización a la alta gerencia y a otros miembros clave de la organización.

4.1.4. Comité operativo de Ciberseguridad

Responsable por la operación del programa de seguridad de las tecnologías de información y operaciones de la Compañía (Equipo de Tecnología). Debe contar con la presencia de personal idóneo y claramente definido, con el objeto de cumplir y soportar las actividades de ciberseguridad. Sus responsabilidades incluyen:

- Liderar la implementación del programa de seguridad de las tecnologías de información y operaciones en la Compañía.
- Liderar el desarrollo de proyectos e iniciativas de ciberseguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos que sean consistentes con las metas y objetivos de la Compañía.
- Recomendar roles y responsabilidades específicos que se relacionen con la ciberseguridad.
- Aprobar el uso de metodologías, herramientas y procesos específicos para la ciberseguridad.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos de ciberseguridad.
- Poner en conocimiento los documentos generados al interior del comité táctico de

ciberseguridad que impacten de manera transversal a la Compañía.

- Velar por que en la Compañía se estén tomando las acciones necesarias para el tratamiento del riesgo sobre los activos de información.
- Promover la difusión y sensibilización de la ciberseguridad dentro de la Compañía.
- Realizar seguimiento de incidentes de seguridad reportados por el área de seguridad.

4.1.5. Oficial de seguridad de la información y la ciberseguridad de la Compañía – Líder de la ciberseguridad

Responsable del programa de seguridad de las tecnologías de información y operación de la Compañía, reportando al nivel directivo asignado o en su defecto al comité táctico de ciberseguridad sobre las políticas, los objetivos y su cumplimiento. La Compañía es propietaria de los activos de información. La tenencia y manejo de la información es delegada al Equipo de Tecnología*, quien es responsable de la custodia y seguridad de la información que la Compañía genera, considerando su propósito y uso. Sus responsabilidades incluyen:

- Desarrollar, implementar y administrar un programa de seguridad de las tecnologías de información y operación.
- Velar por que las implementaciones de controles de ciberseguridad a través de los procesos sean adecuadas.
- Coordinar que el compromiso de educación de ciberseguridad y concientización sea soportado y promovido efectivamente a través de la Compañía.
- Garantizar que los incidentes de ciberseguridad de la Compañía sean monitoreados y revisados, identificando acciones preventivas y correctivas apropiadas.
- Asesorar a la Compañía sobre como incluir la ciberseguridad en las fases de inicio de todos los proyectos de tecnología de la información.
- Revisar las políticas, normas, procedimientos y especificaciones según lo estipulado y presentar los cambios para la aprobación a las instancias correspondientes.
- Participar en la definición de los controles de ciberseguridad para la plataforma tecnológica de la Compañía.
- Evaluar, realizar el seguimiento y reportar al comité, los incidentes de ciberseguridad relevantes.
- Asegurar que los planes de respuesta ante incidentes de ciberseguridad o interrupciones en la tecnología de información y comunicaciones sean desarrollados, mantenidos y probados regularmente para su funcionamiento.
- Asegurar que los controles de acceso de cada sistema de información u operación estén de acuerdo con el nivel de riesgo evaluado.
- Verificar que las herramientas para controlar el acceso a la información funcionen de acuerdo con las normas y guías de clasificación de la información.
- Definir y aprobar el plan de concientización en ciberseguridad para el personal interno o externo.
- Realizar evaluaciones periódicas de seguridad de la plataforma tecnológica.
- Reportar al comité táctico de ciberseguridad los avances sobre los proyectos e iniciativas de seguridad.
- Evaluar cambios significativos de la exposición de los activos de información y ciber activos a las amenazas de seguridad.

4.1.6. Propietarios de activos de información y ciber activos – Líderes de áreas

Responsables de los activos de información que le sean asignados, así como de la clasificación, control y monitoreo del uso y gestión de los mismos. Sus responsabilidades incluyen:

- Monitorear las prácticas de los colaboradores y terceros bajo su control y tomar las acciones necesarias para asegurar el cumplimiento de las políticas y procedimientos de ciberseguridad.
- Asegurar que los incidentes de seguridad del personal a cargo sean reportados.
- Mantener actualizado el inventario de los activos de información y ciber activos de los procesos a su cargo.
- Determinar el nivel de clasificación de cada uno de los activos de información y ciber activos de los cuales es responsable, de acuerdo con su impacto para el negocio y sus objetivos estratégicos.
- Asegurar que los controles de seguridad están de acuerdo con la clasificación de la información o criticidad de la infraestructura de operación.
- Definir criterios de acceso y respaldo de los activos de su propiedad.
- Ejecutar o delegar la aprobación de los requerimientos de acceso, y el respaldo de la información o la asignación de las tareas al responsable de la información.
- Aprobar los acuerdos de confidencialidad de la información con terceros.
- Determinar los requerimientos de disponibilidad de la información.
- Evaluar el riesgo de la información.
- Asegurar que los contratos con terceros que acceden a la plataforma tecnológica incluyan cláusulas de cumplimiento de políticas, procedimientos y especificaciones de seguridad de la información y la ciberseguridad de la Compañía, requerimientos de cuentas de usuario a servicios y aplicaciones, y sanciones en caso de incumplimiento.
- Identificar los requerimientos del tiempo que los activos de información deben ser salvaguardados.
- Monitorear los niveles de acceso de colaboradores y terceros a sus activos de información para garantizar la confidencialidad e integridad de la información almacenada, resguardada o procesada en los mismos.
- Cuando haya retiros o cambios de cargos de colaboradores, debe asegurar que la información que se entrega y recibe este acorde a los lineamientos de almacenamiento de información corporativa.

4.1.7. Custodios de activos de información y ciber activos

Responsables dentro de la compañía de custodiar el activo de información y ciber activo, haciendo efectivas las restricciones y clasificaciones de acceso dadas por el propietario. El custodio puede ser cualquier colaborador, proveedor, contratista, u otra persona autorizada. Sus responsabilidades incluyen:

- Implementar y documentar los controles de ciberseguridad.
- Administrar el acceso a la información de acuerdo con los criterios definidos por los dueños.

- Participar en la definición de los controles de seguridad de los activos a cargo.
- Identificar, investigar y reportar los incidentes de ciberseguridad.
-

4.1.8. Usuarios

Cualquier colaborador, proveedor, contratista, u otra persona autorizada que utiliza la información de la Compañía en la ejecución de las actividades de su trabajo diario. Sus responsabilidades incluyen:

- Usar la información y los recursos informáticos de la Compañía únicamente para el desarrollo de su trabajo.
- La información de la compañía no puede ser usada para fines personales.
- Reportar los incidentes de ciberseguridad.
- Cumplir con las políticas, normas y procedimientos de ciberseguridad.
- Asistir a las capacitaciones y evaluaciones de ciberseguridad.
- Hacer buen uso de la infraestructura de las operaciones y velar por su disponibilidad.
- Clasificar la información y la infraestructura de operación de acuerdo con su importancia.

Cumplir con todo lo descrito en el numeral 17 (Documentación relacionada).

4.1.9. Área de tecnología

Responsables de la gestión de las medidas necesarias para mitigar los riesgos asociados a la ciberseguridad y reportaran al comité táctico de ciberseguridad cualquier evento asociado.

4.1.10. Gerencia de Talento Humano

-
- Informar al área de tecnología de forma permanente y oportuna los ingresos, retiros, y licencias de colaboradores.
- Entrenar en aspectos relacionados con la ciberseguridad a los colaboradores como parte del proceso de inducción.
- Realizar el proceso de selección de acuerdo con el procedimiento definido.
- Incluir las cláusulas de confidencialidad de la información en los contratos de los colaboradores de la Compañía y terceros junto con el área jurídica.
- Definir el proceso disciplinario para el incumplimiento de las políticas de seguridad y ciberseguridad.
- Incluir dentro del paz y salvo en el retiro del colaborador de la Compañía, la devolución de recursos informáticos y activos de información bajo su custodia.
- Realizar evaluaciones sobre el conocimiento de ciberseguridad de los colaboradores de la Compañía.

4.1.11. Gerencias jurídicas

- Identificar e incluir en los contratos con los terceros los requerimientos legales y

contractuales asociados a la seguridad de la información y la ciberseguridad.

- Colaborar en el proceso de la administración de respuesta a incidentes cuando sea necesario debido a un pleito legal o solicitudes de entidades competentes.
- Mantener contacto con las autoridades y grupos de interés para estar al corriente en cambios de normativas de gobierno en los países de influencia.

4.1.12. Área de auditoría y entes de control

- Implementar y ejecutar un plan de auditoría de ciberseguridad con apoyo del equipo de Tecnología* y/o especialistas externos. Este plan debe estar enfocado hacia la revisión de todos los requerimientos (políticas y procedimientos) de seguridad. Los resultados deben generar un programa, que incluya como mínimo: acciones a realizar, tablas de tiempo y responsables. El programa debe ser aprobado por el comité táctico de ciberseguridad.

4.1.13. Mesa de Servicio

- Atender y soportar o escalar a un segundo y tercer nivel los incidentes de ciberseguridad.

5. SEGURIDAD EN RECURSO HUMANO

El área de gestión humana de la Compañía, o la empresa que estas deleguen para gestionar su talento humano, deben notificar al área de tecnología todas las novedades del personal directo e indirecto tales como ingresos, traslados, retiros y vacaciones, así como deben asegurar que los colaboradores, contratistas y usuarios de terceras partes entiendan y cumplan sus responsabilidades en ciberseguridad.

5.1. Seguridad previa a la contratación del personal

Para toda persona que ingrese a la Compañía, debe tener una adecuada descripción del cargo y en los términos y condiciones de la contratación.

Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deben seleccionar adecuadamente (si se requiere hacer su respectivo estudio de seguridad), especialmente para los trabajos que requieren acceso a información sensible, confidencial o reservada, por lo cual se debe asegurar que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el colaborador a contratar. Este mismo tratamiento se debe implementar a los candidatos que administran y operan ciber activos en las operaciones de la Compañía.

Los colaboradores, contratistas y usuarios de terceras partes de las tecnologías de información y operación deberán firmar un acuerdo sobre sus funciones y responsabilidades con relación a la ciberseguridad.

5.2. Seguridad durante la contratación del personal

En conjunto con el área de tecnología de la información de la Compañía, o la empresa que esta delegue para gestionar su tecnología de información, el área de Procesos y el área de gestión humana de la Compañía, se debe desarrollar un programa efectivo y continuo de concientización de protección de la información para todo el personal. También se debe definir y desplegar la capacitación específica en administración de riesgos tecnológicos para aquellos individuos que están a cargo de responsabilidades especiales de protección y los conceptos básicos con que debe cumplir todo colaborador.

Es responsabilidad y deber de cada colaborador de la Compañía asistir a los cursos de concientización en ciberseguridad que la empresa programe y aplicar la seguridad según las políticas y los procedimientos establecidos por la Compañía.

Cualquier colaborador que sea encontrado violando las políticas y procedimientos de ciberseguridad, dará origen a una investigación administrativa que establezca las circunstancias y los motivos que lo produjeron. Con las conclusiones de esta investigación se adelantan las acciones administrativas, reglamentarias y legales pertinentes.

El contrato laboral debe contener un parágrafo que acote esta responsabilidad.

5.3. Seguridad en la finalización o cambio de contrato

El área de gestión humana de la Compañía debe asegurar que todos los colaboradores, consultores, contratistas, terceras partes, que salgan de la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que la Compañía lo consideren conveniente, incluso después de la finalización del puesto de trabajo o del contrato.

El área de gestión humana de la Compañía se debe asegurar que la salida o movilidad de los colaboradores, contratistas o terceros sea gestionada hasta la completa devolución de todos los activos y retirada de los derechos de acceso.

El líder del área donde pertenece el colaborador que se retira, debe asegurar la entrega de los activos que le serán retornados para su administración.

Se bloquearán los derechos de acceso y cuentas de usuario a todos los colaboradores, contratistas y terceros, una vez se haya dado por finalizado las relaciones establecidas para prevenir los accesos posteriores a los procesos y sistemas de la organización.

A todos los funcionarios que cambien de rol, se les debe revisar el acceso a los sistemas, eliminándolo si es necesario. La información almacenada, procesada o transmitida por

estos funcionarios en repositorios distintos a los oficiales de la Compañía será borrada (Esto incluye la información almacenada en computadores personales, dispositivos móviles, sistemas de correo y colaboración).

El único impedimento para la destrucción de información es de orden legal y/o jurídico, el cual determinará el periodo mínimo de almacenamiento de la información (periodo de retención).

6. GESTIÓN DE ACTIVOS DE INFORMACIÓN Y CIBER ACTIVOS

La Compañía debe tener un conocimiento preciso sobre los activos de información y ciber activos que posee como parte fundamental en la administración de riesgos de ciberseguridad, por lo cual deberán disponer de:

- Un inventario de activos de información y ciber activos, con sus respectivos riesgos, amenazas, vulnerabilidades y controles.
- La asignación de propietarios de los activos de información y ciber activos con la responsabilidad de controlar el desarrollo, mantenimiento, tratamiento, clasificación y seguridad de los mismos.
- La clasificación de los activos de información y los ciber activos teniendo en cuenta su valor para el negocio, y de acuerdo a los criterios de confidencialidad, integridad y disponibilidad, para lo cual la Compañía deberán establecer los criterios de clasificación que incluyan al menos estas tres variables claves en la seguridad.
- El manejo de los soportes de almacenamiento para proteger la información, e identificar si es necesario el uso de mecanismos de cifrado con el fin de proteger su confidencialidad.

7. CONTROL DE ACCESOS

El área de tecnología de la información de la Compañía, o la empresa que esta delegue para gestionar su tecnología de información, debe implementar las medidas de control de acceso aplicables según el caso, conforme la clasificación de los activos de información y los ciber activos, con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento.

El control de acceso de datos e información sensible se debe basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido. Adicional, se deben cumplir con los siguientes requerimientos:

- Garantizar que los usuarios únicamente se les asignen los privilegios y derechos necesarios para el desarrollo de sus funciones.
- Documentar los perfiles y los derechos de acceso.
- Registrar los hechos en caso de requerir una auditoria.
- La Compañía deberá definir procedimientos, guías y estándares para:
- Gestionar el acceso a los usuarios que den cubrimiento a todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del

registro a quienes no necesiten el acceso, incluyendo los niveles y responsabilidades de autorización.
- Revisar los derechos de acceso a los usuarios.
- Definir las responsabilidades de los usuarios frente a los equipos y el acceso a los activos digitales.
- Control de acceso a los sistemas de información y plataformas, incluyendo las restricciones de acceso a la información, el uso de herramientas de administración de sistemas, y la gestión de contraseñas de usuario.
- Para los recursos como carpetas compartidas, los accesos y gestión de permisos son responsabilidad del propietario del activo, quien se encarga de la asignación o retiro de los accesos a terceros, según la necesidad.
- Control de acceso a terceros.

8. CRIPTOGRAFÍA

El área de tecnología de la información de la Compañía, o la empresa que esta delegue para gestionar su tecnología de información, debe establecer el uso de sistemas y técnicas criptográficas para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización, de forma tal que se asegure su confidencialidad e integridad.

La compañía asegurará la información de los activos a través de cifrado de los equipos portátiles de su propiedad y medios removibles sobre los cuales se tiene información corporativa.

En caso de que un colaborador o un tercero haga uso de medios portátiles ajenos a la compañía, estos podrán ser leídos y tendrán una restricción para descargar información de la compañía, la cual puede ser levantada con una autorización expresa del dueño del activo de la información.

9. SEGURIDAD FÍSICA Y DEL ENTORNO

La Compañía debe minimizar los riesgos de daños e interferencias a la información y a sus operaciones mediante el establecimiento de áreas seguras y perímetros de seguridad que permitan la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados.

Igualmente, deberán proteger los equipos contra amenazas físicas y ambientales para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

10. SEGURIDAD EN LAS OPERACIONES DE INFRAESTRUCTURA

El área de tecnología de la información de la Compañía, o la empresa que esta delegue para gestionar su tecnología de información, debe proveer el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación, a través de una gestión adecuada, efectiva y eficiente de la tecnología de información y comunicaciones, que incluya aspectos asociados a:

- Copias de seguridad.
- Verificación de cintas.
- Recuperación de datos y reversión de cambios.
- Gestión de cambios.
- Administración de sistemas de antivirus.
- Administración de usuarios y contraseñas.
- Administración de acceso a los recursos.
- Administración de acceso remoto.
- Medición de desempeño.
- Gestión de capacidad y disponibilidad de los recursos de TI.
- Gestión de pistas de auditoría y sistemas de registro de información.
- Aseguramiento de plataformas.
- Separación de entornos de desarrollo, prueba y producción.
- Segregación de funciones.
- Protección contra código malicioso.
- Control del software en explotación
- Gestión de la vulnerabilidad técnica

11. SEGURIDAD EN LAS REDES Y TELECOMUNICACIONES

El área de tecnología de la información de la Compañía, o la empresa que esta delegue para gestionar su tecnología de información, debe asegurar la protección de la información que se comunica por redes de voz y datos, y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección, por lo cual deberá:

- Garantizar que los proveedores de servicios de red implementan medidas en cumplimiento con las características de seguridad.
- Incorporar controles especiales para salvaguardar la integridad y confidencialidad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectadas. Igualmente se debe garantizar la disponibilidad de los servicios de red y computadores conectados.
- Asegurar que los intercambios de información por parte de la Compañía se deben basar en una política, procedimientos y controles formales de intercambio y en línea con los acuerdos de intercambio, y deben cumplir con cualquier legislación relevante.

12. SEGURIDAD EN LA GESTION DE SISTEMAS

El área de tecnología de la información de la Compañía, o la empresa que esta delegue

para gestionar su tecnología de información, debe proveer las medidas de seguridad en sistemas de información desde la fase de requerimientos, y deben ser incorporados en las etapas de desarrollo, implementación y mantenimiento, lo cual incluye:

- La definición de los requisitos relacionados con la ciberseguridad que deben cumplir los sistemas de información.
- Los requisitos relacionados con la ciberseguridad se deben incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes, al igual que justificar, acordar y documentarse, como parte de todo el proyecto del sistema de información.
- El aseguramiento de los entornos de desarrollo, así como el acceso al sistema de archivos y al código fuente.
- El aseguramiento del control de cambio a los sistemas, la revisión técnica de los sistemas tras efectuar cambios en el sistema operativo.
- La incorporación de las políticas de seguridad de la información en procesos de externalización del desarrollo de software.
- El uso adecuado de los datos de prueba.

13. RELACIÓN CON PROVEEDORES

La Compañía debe mantener un nivel apropiado de ciberseguridad en sus relaciones con terceros, garantizando la protección de los activos de información que son accesibles por los mismos. Se debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras partes. La Compañía deberá establecer y acordar todos los requisitos de ciberseguridad pertinentes a cada proveedor que acceda, procesa, almacene, comunique o proporcione componentes de infraestructura de TI que dan soporte a la información de la organización. Para tales efectos el área legal debe suministrar las clausulas que regulen la relación con los proveedores para los temas de ciberseguridad mencionados en este documento.

Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de ciberseguridad asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

La Compañía debe verificar la implementación de los acuerdos asociados a la ciberseguridad, el monitoreo de su cumplimiento y la gestión de los cambios con el fin de asegurar que los servicios que se prestan cumplen con todos los requerimientos acordados.

14. GESTIÓN DE LOS INCIDENTES DE CIBERSEGURIDAD

Todos los colaboradores o terceras partes deben comunicar si han observado o sospechan que exista un evento de ciberseguridad comunicar al personal de tecnología.

El área de tecnología de la información de la Compañía, o la empresa que esta delegue

para gestionar su tecnología de información, debe definir los procedimientos, guías y estándares para la gestión de los incidentes de ciberseguridad, y los cuales deberán incluir:

- El aseguramiento de la notificación oportuna de eventos y debilidades de ciberseguridad, para emprender las acciones correctivas.
- El escalamiento, valoración y respuesta a los incidentes de ciberseguridad reportados.
- La recopilación adecuada de evidencias para investigaciones y futuras acciones legales.
- La gestión adecuada del conocimiento adquirido en la respuesta a incidentes de seguridad de la información y ciberseguridad como fuente de aprendizaje para análisis y resolución de incidentes futuros.

15. SEGURIDAD EN LA CONTINUIDAD DE NEGOCIO

La Compañía debe contar con un programa de continuidad de negocio en el cual se debe incluir la ciberseguridad como un elemento primordial en todas las fases del programa: la identificación de escenarios y riesgos; análisis de impacto al negocio; identificación, definición e implementación de estrategias de continuidad y recuperación; documentación e implementación de planes de respuesta, incluyendo planes de continuidad de negocio, recuperación ante desastres, y manejo de crisis; así como en las respectivas pruebas de estrategias y planes.

La Compañía debe preservar la ciberseguridad durante las fases de activación, evaluación, y puesta en operación de procedimientos y planes para la continuidad de negocio, así como en el retorno a la normalidad. Se debe integrar dentro de la continuidad de los procesos críticos de negocio, aquellos requisitos de gestión de la ciberseguridad con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

16. CUMPLIMIENTO CON REQUERIMIENTOS LEGALES Y CONTRACTUALES

Toda solución de servicios o infraestructura tecnológica debe garantizar que su selección está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la organización.

16.1. Cumplimiento de los requisitos legales y contractuales

El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales, por lo cual deberán ser advertidos por los asesores legales de la organización o por profesionales

adecuadamente cualificados.

16.1.1. Identificación de la legislación aplicable

Todos los requerimientos contractuales y legales que puedan afectar los sistemas de información de la Compañía deben definirse previamente y documentarse de acuerdo con las guías o metodologías empleadas por la Compañía. Los controles específicos, medidas de protección y responsabilidades individuales que cumplan con los requerimientos, deben así mismo definirse y documentarse. El área legal y/o jurídica de la Compañía debe ser participe en la identificación de legislación aplicable.

16.1.2. Derechos de Propiedad intelectual

Se protegerá adecuadamente la propiedad intelectual de la Compañía, tanto propias como la de terceros (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.
Se debe incluir dentro de los contratos de trabajo cláusulas que indiquen a todos colaboradores las responsabilidades de tipo legal con relación a los derechos de autor, con el fin de evitar posibles violaciones a la legislación.

Para el cumplimiento del licenciamiento de software se establece lo siguiente:

- Se debe tener una herramienta o procedimiento que permita controlar las licencias vigentes del software utilizado oficialmente por la Compañía.
- Se debe mantener evidencia de las licencias que son propiedad de la Compañía, manuales o discos maestros.
- No se excede el número de usuarios permitidos por una licencia determinada.
- Se debe realizar al menos una revisión anual, que garantice que sólo se tiene software licenciado.
- Antes de enviar información por correo electrónico, usar información disponible en Internet, música o usar información de algún tipo de documento, se debe tener la respectiva aprobación o pago al dueño de los derechos de autor.

16.1.3. Protección de los registros de información

Para los registros de información asociados a registros de contabilidad, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, se debe tener definido los periodos de retención y los tipos de medio de almacenamiento como papel, microfichas, medios magnéticos, ópticos, etc. Adicional se deben proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

16.1.4. Protección de datos y privacidad de la información personal

La Compañía debe garantizar la privacidad y la protección de la información personal identificable según requiere lo establece la legislación y las normativas pertinentes aplicables que correspondan. Los estándares de seguridad son de obligatorio cumplimiento para los colaboradores con acceso a los datos de carácter personal y a los sistemas de información.

16.1.5. Controles sobre la implementación de técnicas criptográficas

El uso de licencias de software de cifrado debe cumplir con los acuerdos, las leyes y los reglamentos pertinentes.

16.2. Revisiones de la ciberseguridad

La Compañía debe realizar revisiones regulares de la seguridad de los sistemas de información. Las revisiones se deben realizar según las políticas de seguridad apropiadas, y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados.

16.2.1. Cumplimiento de políticas y normas de seguridad

Los directivos de la Compañía se deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión con auditoria.

16.2.2. Comprobación de cumplimiento

Se debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad. Se deben realizar auditorías periódicas con ayuda de herramientas automatizadas y se deben generar informes técnicos que reflejen la evaluación de riesgos de ciberseguridad, las vulnerabilidades y su grado de exposición al riesgo.

16.2.3. Consideraciones sobre auditorias de sistemas de información

Para el desarrollo de auditorías internas o de tercera parte se cumplen los siguientes aspectos:

- Las actividades relacionadas con procesos de auditorías deben contar con aprobación del líder de seguridad y el propietario de la información.
- Se debe determinar con anterioridad el alcance, su concertación y control durante todo el proceso.
- Se debe preservar la integridad de la información durante todo el proceso.
- Los recursos necesarios para realizar la auditoria deben ser explícitamente definidos.
- Los requerimientos de procesamiento adicional deben ser identificados con anterioridad.
- Todos los accesos deben ser monitoreados y almacenados para producir un registro de las actividades realizadas durante el proceso.
- Todos los procedimientos, requerimientos y responsabilidades deben ser formalmente documentados.
- Las herramientas de auditoría deben ser protegidas de uso indebido.

17. DOCUMENTACIÓN RELACIONADA

- Política de ciberseguridad
- Política de protección de datos personales
- Guía de buen uso de recursos informáticos
- Guía de seguridad para la clasificación de activos de información
- Especificaciones de Seguridad de la Información - Usuarios Finales
- Estándar de Seguridad de la Información - Aceptación de Aplicaciones

BIBLIOGRAFÍA

ISO International Organization for Standardization. (2013). *ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls.*

HISTORIAL DEL DOCUMENTO

CONTROL DE VERSIÓN

Número	Fecha	Descripción del cambio o modificación
1	16/11/2016	Emisión inicial
2	11/04/2022	Ajustes oportunidades de mejora en Auditoria del proceso de Ciberseguridad
3	30/08/2023	Instancia de aprobación Comité estratégico de ciberseguridad