TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el presente documento se establecen las Políticas de Seguridad de la Información para la organización ADA S.A.S Y LAPOINT, determinando las mejores prácticas de uso y administración de la información a tal punto que se pueda definir el uso adecuado de sus activos correspondientes, estableciendo responsabilidades y funciones de cumplimiento en cada criterio de los procesos de la organización.

La seguridad de la información es un proceso que se realiza con todos los actores de la compañía, los cuales se comprometen a seguirlas y cumplirlas adecuadamente, determinando los niveles de riesgos más importantes en cada subproceso manejado y el tratamiento correspondiente a éstos.

Es responsabilidad de todos los empleados velar por el cumplimiento de estas políticas y reportar sus violaciones.

.

2. ALCANCE

El Sistema de Gestión de Seguridad de la Información (SGSI) de ADA S.A.S. y LAPOINT ICT S.A.S. aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación definidos por la organización, relacionados con el diseño, desarrollo, implementación, soporte y mantenimiento de soluciones de software, la prestación de servicios de infraestructura tecnológica y datacenter, así como la gestión de la información utilizada para la operación y prestación de dichos servicios.

El alcance incluye:

- El personal de ADA S.A.S. y LAPOINT ICT S.A.S., independientemente de su modalidad de contratación.
- Los contratistas, proveedores y terceros que tengan acceso a información o activos de información de la organización.
- Los activos de información físicos y digitales.
- La infraestructura tecnológica, redes de comunicación, servidores, bases de datos, aplicaciones, servicios en la nube y equipos de usuario administrados por la organización.
- Las sedes de Medellín y Bogotá, así como los servicios tecnológicos operados desde el Datacenter de LAPOINT ICT S.A.S.
- La información procesada, almacenada o transmitida durante la ejecución de los procesos organizacionales.

La definición del alcance se basa en:

- El análisis del contexto de la organización (Cláusula 4.1).
- La identificación de las partes interesadas y sus requisitos (Cláusula 4.2).
- La evaluación de riesgos y oportunidades de seguridad de la información.
- Las interfaces y dependencias existentes con proveedores, clientes, contratistas y demás partes interesadas relacionadas con la prestación de los servicios.

No se establecen exclusiones dentro del alcance del SGSI.

3. OBJETIVOS

- Mantener la Información íntegra, disponible y con niveles de confidencialidad adecuados.
- Garantizar un manejo confiable de la información de ADA S.A.S Y LAPOINT junto con su plataforma tecnológica, frente a amenazas internas o externas.
- Velar por el cumplimiento de las políticas de seguridad de la información.
- Minimizar, evitar o transferir los riesgos más importantes, relacionados al tratamiento de la información.
- Revisar y valorar la Política de Seguridad de la Información a intervalos planificados, o cuando se produzcan cambios que afecten los activos de información, de tal forma que permanezca actualizada, operativa y auditada asegurando su nivel de eficiencia y eficacia.

4. POLÍTICA GENERAL SGSI

La información es un recurso valioso para la organización ADA S.A.S Y LAPOINT, la cual, apoyada en su misión, visión y objetivos estratégicos, expresa su compromiso en la minimización de los riesgos a los cuales está expuesta la información, impulsando una cultura de seguridad, gestionando los incidentes de seguridad, con el fin de garantizar la continuidad de los procesos principales y la mejora continua.

Todos los empleados y personal contratista garantizan la protección de la información, a la cual tenga acceso para evitar pérdida, daño o uso no autorizado, el incumplimiento de los controles y política de seguridad será reportada y se realizará seguimiento.

5. COMPROMISO DE LA DIRECCION

La Alta Dirección de ADA S.A.S Y LAPOINT. se compromete a:

- Integrar la seguridad de la información en los procesos estratégicos y operativos de la organización

- Asegurar la asignación de recursos humanos, técnicos y financieros necesarios para el funcionamiento eficaz del SGSI
- Promover la mejora continua del sistema a través de revisiones periódicas, auditorias y análisis de desempeño
- Cumplir con los requisitos legales, reglamentarios, contractuales y normativos aplicables.

6. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN

5.1 Estructura de seguridad

ADA S.A.S Y LAPOINT., bajo la dirección del Gerente General, asigna al Área de Gestión de Calidad la responsabilidad de coordinar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

El Área de Tecnología de la Información será responsable de la implementación y operación de los controles técnicos de seguridad de la información. Igualmente, se asignan responsabilidades de seguridad de la información a todos los colaboradores de acuerdo con el proceso, cargo o rol desempeñado dentro de la organización.

5.2 Contacto con autoridades y grupos de interés

ADA S.A.S Y LAPOINT conoce, identifica y establece contacto con las autoridades (Policía Judicial en temas de informática forense, CSIRT de la Policía Nacional y equipo de coordinación de incidentes de seguridad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones) y grupos especializados en seguridad de la información, para gestionar los incidentes de seguridad de la información minimizando la exposición de sus efectos.

5.3 Partes Interesadas

Esta política considera las expectativas y necesidades de todas las partes interesadas relevantes, incluyendo clientes, empleados, proveedores, entes reguladores y socios comerciales, con el fin de asegurar la confianza en los servicios ofrecidos por ADA S.A.S Y LAPOINT.

5.4 Política para dispositivos móviles

Los dispositivos móviles institucionales tales como celulares, tabletas entre otros y personales que hagan uso de los servicios de la plataforma tecnológica de ADA S.A.S Y LAPOINT, deben tener un uso responsable, ético, sin poner en riesgo la seguridad de la información de la compañía y seguir los lineamientos del área de TI en cuanto a configuración, métodos de bloqueo, instalación de aplicaciones y copias de seguridad.

Los empleados deben evitar el uso de dispositivos móviles en lugares donde estén expuestos a robos, daño o pérdida, garantizando en todo momento que se utiliza solo por personal autorizado y con las medidas de seguridad apropiadas.

En lo posible no conectar los dispositivos móviles institucionales a redes inalámbricas públicas de baja seguridad y sin contraseña de ingreso, como, por ejemplo: hoteles, centros comerciales, aeropuertos, entre otros y de igual manera solo activar las conexiones wifi y bluetooth sólo en el momento de ser utilizada. Los dispositivos móviles no se deben conectar por puerto USB a computadores de uso público.

En caso de robo o pérdida, se deberá reportar lo más pronto posible al jefe inmediato e instaurar la respectiva denuncia ante la autoridad competente.
.

5.5 Teletrabajo

En relación con este ítem, la Compañía ha definido una política de conexión laboral en pro de establecer y aplicar aquellas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada y almacenada en los lugares en que se realiza teletrabajo.

El documento al que se hace referencia tiene como nombre" Política de Conexión Laboral" , el cual se encuentra almacenado en el synology de la empresa

5.6 Inteligencia sobre Amenazas

La inteligencia de amenazas es la disciplina de obtener y analizar información sobre quienes podrían hacernos daño en el ciberespacio, con el fin de entender cómo hacer que nuestras defensas sean lo más efectivas posible. La recopilación, el procesamiento y la presentación de informes de inteligencia de amenazas son

vitales para la capacidad de ADA SAS de evaluar el riesgo y reaccionar ante las amenazas que enfrenta a su seguridad de la información.

ADA SAS se compromete a garantizar que se empleen métodos efectivos para asegurar la precisión, integridad y puntualidad de la inteligencia de amenazas que utiliza.

La compañía ha definido una política de inteligencia de amenazas la cual se encuentra almacenada en el synology de la empresa.

7. SEGURIDAD DE LOS RECURSOS HUMANOS

6.1 Selección

ADA S.A.S Y LAPOINT establece los criterios de selección de personal para los cargos, definiendo perfiles para el cargo respectivo en cuanto a experiencia, formación y educación. Igualmente, confirma las referencias personales y laborales del aspirante y la veracidad de la información colocada en la hoja de vida.

Para los contratos de prestación de servicios profesionales y de apoyo a la gestión, la selección del contratista se realizará teniendo en cuenta los requisitos de idoneidad y experiencia para la prestación del servicio

6.2 Responsabilidades de los empleados

ADA S.A.S Y LAPOINT, con el fin de crear un ambiente laboral que garantice un adecuado manejo de los activos de información, establece que todos los empleados y contratistas son responsables de conocer y aplicar las políticas de seguridad de la información.

Todos los empleados deben velar por la protección y buen uso de los activos de información de la compañía, informando oportunamente los eventos de seguridad que la puedan poner en riesgo.

ADA S.A.S Y LAPOINT tiene definidas y claras las funciones y responsabilidades de los cargos de la compañía.

6.3 Formación y concienciación sobre la seguridad de la información

Los empleados, y de ser necesario el personal contratista, recibirán formación adecuada, para el cumplimiento de sus funciones y responsabilidades con el Sistema de Gestión de Seguridad de la Información.

Esta formación deberá contemplar los requisitos de seguridad, responsabilidades legales, el correcto uso de los recursos, entre otros.

6.4 Proceso disciplinario

En el momento de presentarse un incidente de seguridad de la información, se iniciaría la correspondiente indagación preliminar a fin de establecer la veracidad de los hechos y definir las acciones a que haya lugar, teniendo en cuenta la gravedad del incidente y su impacto en la compañía.

6.5 Terminación o cambio de relación laboral

ADA S.A.S Y LAPOINT al terminar la relación laboral con el funcionario, o al cambiar sus funciones debe entregar sus proyectos al debido encargado o líder de su área, requiriendo esa transferencia de manera documentada o a través de la capacitación a la persona que lo reemplaza.

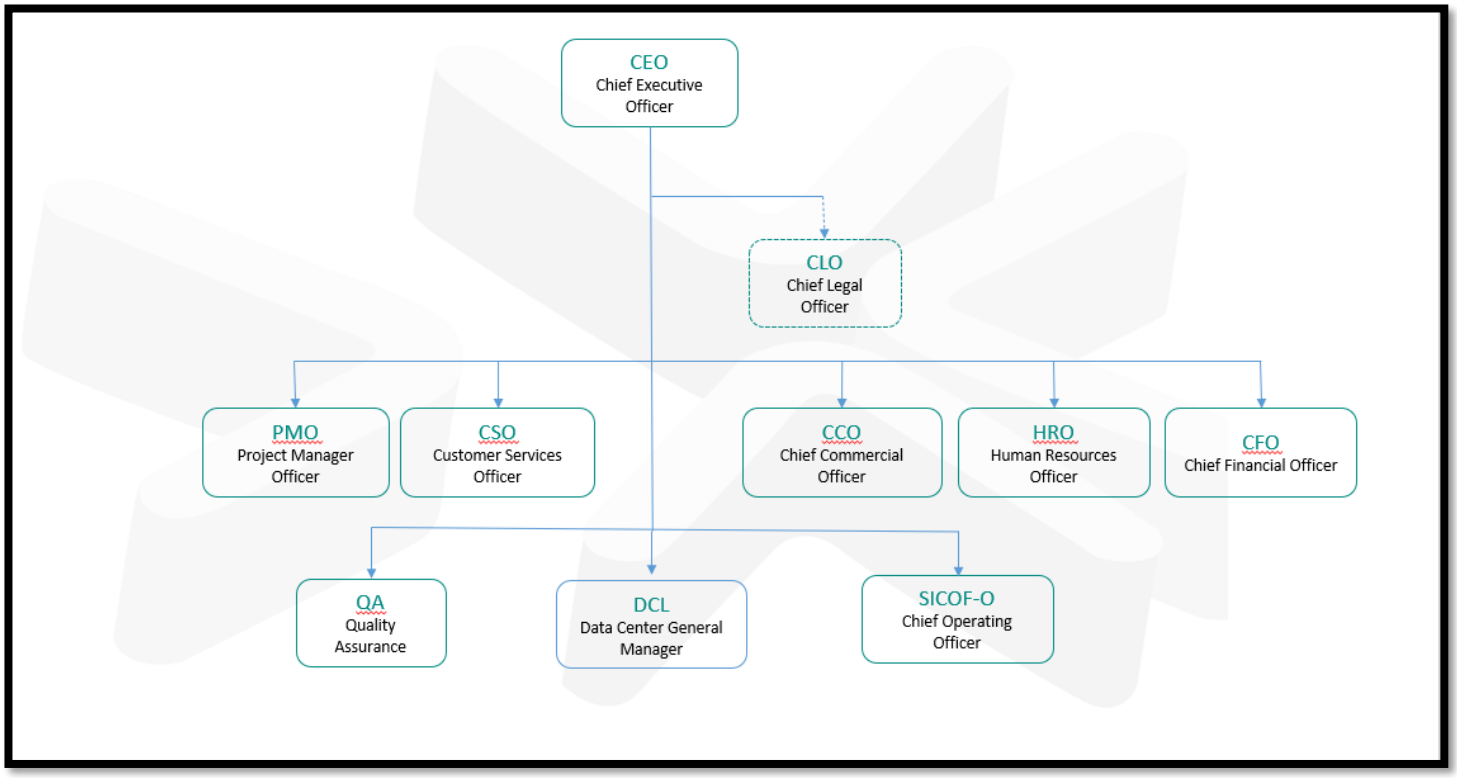
La compañía garantiza que todos sus activos de información sean devueltos y descargados del archivo de activos, retirando los accesos físicos y lógicos, como requisito para la firma de paz y salvos.

8. GESTION DE ACTIVOS

7.1 Inventario de activos

El conocimiento, uso y propiedad de los activos de información en la organización, permite generar valor agregado efectuando control y protección a sus procesos, contando con el pleno conocimiento de lo que la compañía posee para el desarrollo de su misión y visión y evitando así incumplimiento de responsabilidades, violación a los derechos de autor y responsabilidades derivadas por la pérdida o daño de los mismos. La compañía ha designado un responsable en cada área para clasificar, elaborar y mantener actualizado un inventario de activos de información, con el fin de garantizar la disponibilidad, integridad y confidencialidad de estos. De igual forma, que permita al activo de información ser identificado, teniendo un dueño o propietario que establezca permisos para su acceso, esta información es debidamente protegida con esquema de seguridad de directorios y archivos bajo esquema de lista control accesos.

7.1.1 Estructura organizacional de ADA S.A.S Y LAPOINT



7.1.2 Responsable VS activos Información acorde a la estructura organizacional.

Rol	Activo información
CEO	\\nas-002\gestion interna \gestion interna\Gerencia
Quality Manager	\\nas-002\gestion interna \gestion interna\
Development Sr. Manager	\\nas-002\gestion interna \fabrica
PMO Sr. Manager	\\nas-002/Gestión Interna/007_Proyectos
Jurídica	\\nas-002\gestion interna \jurídica

Rol	Activo información
Calidad	\\nas-002/Gestión Interna/002_Calidad
Dirección de Servicios	\\nas-002\gestion interna \gestión Servicios
Dirección Comercial	\\nas-002\gestion interna \comercial
Dirección Administrativa y Financiera	\\nas-002\gestion interna \administrativo
Dirección Recursos Humano	\\nas-002\gestion interna \recursos humanos

7.2 Uso aceptable de los activos

Los activos de información de ADA S.A.S Y LAPOINT, tales como hardware, software, aplicaciones, servicios, información (bases de datos, archivos de datos, contratos, acuerdos, planes, entre otros) son para uso exclusivo del cumplimiento de los objetivos misionales y debe dársele un uso ético, racional y responsable.

Para realizar consultas de documentos que reposan en las oficinas de la compañía y en el Data Center se permitirá en días y horas laborales, con la presencia del empleado responsable o custodio de la información, en caso de la información digital esta va acorde a los permisos asignados en la unidad de almacenamiento y/o dispositivo.

Los activos asignados deben ser devueltos una vez se termine la relación laboral con ADA S.A.S Y LAPOINT.

7.3 Devolución de activos

Todo empleado es responsable de devolver todos los activos pertenecientes a ADA S.A.S Y LAPOINT y que se encuentren en su poder como consecuencia bien sea de la finalización del contrato o acuerdo.

Si un funcionario posee conocimiento que es importante para las operaciones en curso, es su responsabilidad documentar dicha información y transferirla a la empresa.

El área de Talento Humano es responsable de informar la desvinculación de funciones de uno o más empleados, enviando un comunicado a quienes estime pertinentes.

Adicionalmente, deberá informar la desvinculación del empleado al área de TI para gestionar la devolución de equipos, dentro de los cuales se pueden encontrar, pantalla, teclado, portátil, cables USB, mouse y demás.
.

Igualmente es responsabilidad del líder del proceso a cargo o del área de TI eliminar los derechos de acceso a los sistemas de información, bases de datos, en cuanto a los correos electrónicos dichas cuentas son deshabilitadas.

Así mismo se debe realizar con la desvinculación de empleados para mantener los registros actualizados de los accesos activos, esto debe ser debidamente informado vía correo electrónico y/o mediante ticket en la aplicación Zoho Desk.

7.4 Clasificación de la información

La información es uno de los activos más importantes que tiene la organización.

Clasificar la información, permite consolidar su buen nombre con proveedores y clientes, por el manejo seguro que le hace a su información, ya que le permite demostrar el cumplimiento de regulaciones internas y gubernamentales. La información se clasifica de acuerdo con su nivel de confidencialidad.

ADA S.A.S Y LAPOINT, con el fin de proteger su información que hace parte del patrimonio de la compañía, ha establecido los siguientes niveles de clasificación y responsabilidad en el manejo de la información:

Publica: Se denomina a toda la información que al ser divulgada no resulte perjudicial para la comunidad o la compañía y que no requiera ningún nivel de seguridad y/o que provenga de registros o fuentes de acceso público, o a alguna normatividad que así lo estipule.

De uso interno: Se denomina a toda la información de uso interno de ADA S.A.S Y LAPOINT para el desarrollo de sus actividades, que no puede ser conocida por terceros sin la autorización de su propietario. Si llegara a ser conocida por terceros que no se encuentren autorizados para ello, afectaría levemente a las actividades, procesos, sistemas o decisiones de la Administración.

Confidencial: Se denomina a toda la información que es utilizada para el cumplimiento de las actividades, pero que solo puede ser conocida por un grupo de empleados. Si llegara a conocerse sin la debida autorización del propietario, afectaría de manera grave las actividades, procesos, Sistemas o decisiones de la Administración.

Los propietarios de los activos son los responsables de identificar y relacionar el nivel de clasificación de cada activo acorde a los criterios establecidos e informados los cuales van acorde a los permisos asignados en la unidad de almacenamiento y/o dispositivo cumpliendo así con los niveles definidos.

7.5 Manejo de medios

La utilización de medios de almacenamiento removibles tales como memorias USB, discos duros externos, celulares, iPad,, entre otros en la infraestructura tecnológica de ADA S.A.S Y LAPOINT, deberá estar autorizada por cada uno de los líderes de procesos, para aquellos empleados que lo requieran de acuerdo con el cumplimiento de sus funciones.

Corresponde al área de TI establecer los controles necesarios a fin de evitar la divulgación, modificación, retiro o destrucción de activos no autorizada y la interrupción en las actividades, tales como:

- Antivirus actualizados.
- Sensibilización a los empleados.
- Capacitación a los usuarios.
- Uso adecuado de los niveles de clasificación de información.
- Uso aceptable de los activos.
- Bloqueo de puertos cuando se requiera.

De igual forma los empleados deben asegurar física y lógicamente los dispositivos con el fin de no poner en riesgo la disponibilidad, integridad, y confidencialidad de la información.

Los empleados contratistas y terceros que utilicen los recursos de la plataforma tecnológica de la compañía, deben acoger los lineamientos de uso de medios removibles impartidos por el área de TI

Cuando ya no se requieran los medios removibles, debe realizarse borrado seguro o destrucción si esta inservible.

9. POLÍTICA DE CONTROL DE ACCESO

El acceso a los servicios de la plataforma tecnológica, tales como acceso a correo electrónico, aplicaciones de gestión de la compañía se realizará a través de una cuenta de usuario debidamente autorizada por el jefe inmediato, señalando los permisos a los cuales tiene derecho de acuerdo a las funciones desempeñadas.

El acceso a través de redes inalámbricas institucionales de uso privado, debe hacerse con la debida autorización del Jefe inmediato.

8.1 Instalación de programas o utilitarios

La instalación y configuración de software y hardware está a cargo del área de TI. Los usuarios no se encuentran facultados para realizar este tipo de actividades.

Los usuarios no deben tener acceso a usuarios administradores en sus equipos, de requerirse deben estar autorizados por el área de TI, quien es la encargada de establecer los protocolos y mejores prácticas de seguridad.

10. POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS

La información confidencial que requiera ser enviada debe ser encriptada para su correcta distribución y/o transmisión, con el fin de garantizar la confidencialidad e integridad de la información, el área de TI dará los lineamientos para ello.

NOTA: Para mayor claridad sobre el uso de los controles criptográficos, consulte el documento:

POLITICA_USO_DE_CONTROLES_CRIPTOGRAFICOS_ADA_S.A.S

Ruta de ubicación del documento en el repositorio:

/GESTION INTERNA/CALIDAD/Aseguramiento de la Calidad/Sistema_Integrado_De_Gestion/SGSI/2021/ADA/Politicas/

11. SEGURIDAD FÍSICA Y AMBIENTAL

10.1 Política de áreas seguras

ADA S.A.S Y LAPOINT, con el fin de proteger su información sensible, define áreas de acceso restringido donde se procesa información vital para la compañía.

El centro de datos cuenta con dispositivos de control de acceso físico, y el software de administración de estos dispositivos lleva una bitácora detallada del ingreso del personal autorizado por el área de TI. Además, se registra el ingreso mediante captura en video a través de sistemas de circuito cerrado de televisión (CCTV).

Adicionalmente, el centro de datos cuenta con sistemas de alimentación de energía ininterrumpida (UPS) y planta eléctrica, permitiendo así prevenir daños e interrupciones en las operaciones críticas.

Considerando los riesgos derivados del **cambio climático**, ADA S.A.S Y LAPOINT. realiza análisis periódicos para evaluar la vulnerabilidad de sus instalaciones frente a eventos climáticos extremos, como inundaciones, altas temperaturas, tormentas eléctricas y otros fenómenos relacionados. Como resultado, se han implementado medidas específicas tales como sistemas adicionales de climatización redundante, ubicación estratégica de equipos críticos en zonas menos vulnerables y planes de respuesta ante emergencias ambientales, garantizando así la continuidad operativa y la protección efectiva de los activos de información ante situaciones climáticas adversas.

El área de TI será responsable de asegurar que todos los mantenimientos preventivos y correctivos sean realizados oportunamente por personal idóneo, autorizado y capacitado en la gestión efectiva de estos riesgos ambientales y climáticos.

10.2 Seguridad de los equipos

Los equipos que pertenecen a la infraestructura de tecnología de Información de ADA S.A.S Y LAPOINT tales como computadores, servidores, equipos de comunicaciones, cableado de energía eléctrica y comunicaciones, UPS, subestaciones eléctricas, planta telefónica, CCTV, dispositivos de almacenamiento, aire acondicionado, dispositivos móviles y demás que sirvan como soporte de la información de la compañía, deben ser protegidos y ubicados de tal forma que se minimicen los riesgos de pérdida, daño, robo, accesos no autorizados o interrupción de las actividades.

En ese orden de ideas, la organización también debe asegurarse contra amenazas físicas y ambientales tales como las producidas por agua, fuego, explosivos, polvo, interferencia electromagnética, errores humanos, vandalismo, entre otros.

La compañía debe asegurar que la infraestructura de servicios de TI esté protegida contra fallas en el suministro de energía y demás anomalías relacionadas con esta, implementando un sistema de alimentación ininterrumpida (UPS), aire acondicionado y planta eléctrica, que garanticen el funcionamiento continuo de los sistemas computacionales que así lo requiera.

Por otro lado, no está permitido consumir alimentos, beber o fumar en el puesto de trabajo.

La compañía asegura un sistema de protección contra descargas eléctricas, protegiendo los sistemas de información de amenazas naturales.

10.3 Seguridad de los equipos por fuera de las instalaciones de la compañía y retiro de activos

Los equipos o software no se retiran de las instalaciones de la compañía sin previa autorización de su jefe inmediato, informando sus fines y razones de salida, teniendo en cuenta que estos no pueden quedar desatendidos en lugares públicos, deben tener las medidas de seguridad necesarias para ser transportados.

La persona responsable del retiro de equipos asegura que en todo momento estos están continuamente vigilados, controlados y manipulados por personal autorizado, manteniendo las medidas de seguridad necesarias para ser transportados evitando robo y daño.

En caso de robo o pérdida, se deberá reportar la compañía y a al área de TI e instaurar la respectiva denuncia ante la autoridad competente.

Los equipos portátiles se deben llevar como equipaje de mano y camuflado cuando sea posible, durante los viajes y con todas las precauciones necesarias a fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

En caso de dar de baja un equipo, se debe asegurar que se haya realizado borrado seguro de información y software licenciado en los medios de almacenamiento.

10.4 Política de escritorio y pantalla limpia

Para ADA S.A.S Y LAPOINT es muy importante el buen manejo de la información tanto digital como física y teniendo en cuenta que las dependencias son visitadas frecuentemente por personal de la comunidad, empresas, personal de aseo, y personal de otras áreas, se requiere tener especial cuidado y atención con la información de carácter confidencial y de uso interno.

Es responsabilidad de los empleados y personal contratista que tengan a cargo un equipo de cómputo, bloquear la sesión de su equipo cuando se ausente de su puesto de trabajo y se reactivará ingresando la contraseña del usuario.

Al terminar la jornada laboral se deben cerrar las aplicaciones y apagar los equipos de cómputo de manera adecuada.

La información sensible que se encuentre en papel o en medios magnéticos debe ser protegida y no dejar a la vista, especialmente cuando no se esté utilizando, para lo cual debe asegurarse bajo llave en gabinetes u otros sitios seguros.

Los documentos confidenciales que se envíen a las impresoras, deben retirarse inmediatamente

12. GESTIÓN DE LAS OPERACIONES

11.1 Documentación de los procedimientos de operación

Los procedimientos operativos relacionados con los servicios de comunicaciones y procesamiento de la información, se mantendrán documentados, actualizados y disponibles con el fin de garantizar el correcto funcionamiento de la plataforma tecnológica. Sus cambios serán autorizados por el jefe del área de TI y las Comunicaciones de ADA S.A.S Y LAPOINT.

El área de TI posee mecanismos para hacer realizar monitoreo y el seguimiento al uso de recursos de la plataforma tecnológica, para asegurar el óptimo desempeño del sistema.

11.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

La compañía protege su plataforma tecnológica de códigos maliciosos, tomando las precauciones necesarias en materia de tecnología, tales como herramientas de software de seguridad como antivirus, antimalware y demás que permitan contrarrestar estas amenazas, así como la concientización de los empleados.

El área de TI es la encargada de autorizar el uso de estas herramientas y garantizar que estas no sean deshabilitadas, al igual que su actualización permanente.

No está permitido sin la autorización del área de TI, desinstalar o deshabilitar las herramientas de seguridad que provee la compañía.

Los usuarios deben ejecutar las herramientas de seguridad sobre los archivos que sean abiertos por primera vez especialmente los que provienen de medios removibles o correo electrónico.

Los usuarios que detecten una infección por código malicioso, deberán reportarla inmediatamente al área de TI, para tomar los correctivos necesarios.

11.3 Copias de respaldo

ADA S.A.S Y LAPOINT debe garantizar que la información definida como vital para el desarrollo de las actividades de la compañía, contenida en medios tecnológicos, será almacenada periódicamente de forma que se asegure su identificación, protección, integridad y disponibilidad. Igualmente deberá contar con un plan de recuperación de copias de seguridad, que permite actuar en caso de que ocurra alguna falla o error.

El personal contratista deberá entregar copia de seguridad de la información generada en la realización de sus funciones en la compañía como requisito para la liquidación de su contrato y es función del interventor(es) o supervisores su verificación teniendo en cuenta medios, contenidos y etiquetado.

Igualmente, los empleados que se retiren de la compañía deberán hacer entrega de las copias de seguridad de la información correspondiente a las funciones desempeñadas, como requisito para la firma de paz y salvos.

11.4 Registro de eventos y seguimiento

La compañía debe garantizar el registro de eventos de las aplicaciones que hacen parte de la plataforma tecnológica, con el fin de identificar usos no autorizados e incidentes de seguridad de la información. El monitoreo y revisión de estos logs deben estar disponibles en el momento que sea requerido y estos son verificados por demanda por empleados única y exclusivamente autorizados para ello bajo modalidad de ticket y/o correo

11.5 Gestión de vulnerabilidades técnicas

La compañía tiene establecida una periodicidad semestral donde se define el desarrollo de pruebas de vulnerabilidad con el fin de establecer fallos en la seguridad de la plataforma tecnológica y tomar las medidas necesarias para su minimización

13. SEGURIDAD DE LAS COMUNICACIONES

El acceso remoto de los equipos de trabajo, empleados y/o contratistas se establece mediante redes privadas virtuales, así mismo las publicaciones web y servicios prestados mundo externo están debidamente contralados por los dispositivos de seguridad perimetral los cuales el área TI establece los controles pertinentes.

12.1 Uso de internet

ADA S.A.S Y LAPOINT proporciona a sus empleados el servicio de Internet, con el fin de mejorar el rendimiento y eficiencia en las actividades que se realizan, encaminadas al cumplimiento de la misión y la visión institucional. El uso de esta herramienta debe hacerse de manera responsable, ética, no abusiva, sin afectar la productividad de la compañía, sin atentar contra las leyes vigentes y sin poner en riesgo la confidencialidad,

integridad y disponibilidad de la plataforma tecnológica. No está permitido desde la red interna el acceso a páginas con contenido que atente contra los lineamientos de seguridad y la normatividad vigente.

El servicio de internet es para fines laborales, haciendo buen uso del mismo, por lo cual no se permite el ingreso a páginas poco fiables, redes sociales, descargas de juegos, música, videos, aplicaciones, programas y demás que afecte el ancho de banda; la velocidad y perjudique la gestión de las redes que podría verse afectada por malware (virus, troyanos, programas espías, entre otros).

12.2 Uso del correo interno

El correo electrónico es una herramienta que agiliza los trámites, cuida el medio ambiente, elimina la papelería utilizada para fines de distribución, conocimiento y asegura su confidencialidad, integridad y disponibilidad, permitiendo almacenar los testigos de recibido y lectura, asegurando que las personas de interés estén informadas a un mínimo costo.

ADA S.A.S Y LAPOINT proporciona a sus empleados, cuentas de correo electrónico con el fin de consolidar la imagen corporativa el sentido de pertenencia. Para lo cual debe dársele un uso racional, responsable, ético y acorde con las funciones desempeñadas.

El envío de información de ADA S.A.S Y LAPOINT, debe realizarse única y exclusivamente desde cuentas de correo institucional, no está permitido realizar envío de información institucional desde cuentas de correo personales.

La cuenta de correo institucional solo podrá ser utilizada para fines laborales, y de ninguna manera para el envío de correo masivo o individual de mensajes con contenido religioso, político, propagandístico o que afecte la sensibilidad o reputación de las personas y quede entredicho el buen nombre de la compañía, queda prohibido y se hará la respectiva investigación a que diera lugar.

Los mensajes que se envíen de cuentas de correo institucionales, deben incluir información legal relacionada con la protección de la confidencialidad.

12.3 Mensajería electrónica

El correo electrónico en ADA S.A.S Y LAPOINT debe ser tratado como un activo más de información donde se apliquen controles apropiados para mantener la confidencialidad, Integridad y disponibilidad de la información. Dentro de la mensajería electrónica también deberemos incluir los mensajes de chat electrónico, así como redes sociales. Los controles aplicables a la mensajería electrónica serian:

- Protección ante acceso no autorizado.
- Utilización de mensajería encriptada en caso de ser necesario.

- Control de envió masivo de correo.
- Asegurar el correcto direccionamiento y transporte de los mensajes.
- Confiabilidad y disponibilidad del servicio.
- Consideraciones legales (firmas digitales).

12.4 Política de transferencia de información

ADA S.A.S Y LAPOINT firmará acuerdos de no divulgación de la información clasificada como confidencial, que por requerirse deba ser entregada o transferida a personal contratista, o terceras partes.

Los empleados velarán por la protección de la información, aplicando los controles adecuados para la exposición de los medios de almacenamiento fuera de las instalaciones de la compañía, igualmente evitando divulgar información confidencial de la compañía, en lugares públicos o sitios donde se pueda poner en riesgo la confidencialidad, integridad y disponibilidad de la información.

La información contenida en medios digitales clasificada como confidencial, cuando se requiera ser transferida puede ser enviada de modo encriptado si el grado de confidencialidad lo amerita y es responsabilidad del empleado aplicar esta mejor practica en caso de ser necesario.

Este punto, el área Jurídica deberá velar porque se dispongan de los acuerdos de confidencialidad por cada cliente y/o proveedor e informar donde se guardan dichos acuerdos para tener acceso de solo lectura.

14. ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS

Cuando la compañía requiera nuevos productos tecnológicos o actualizaciones para la plataforma tecnológica, deberá evaluar las características técnicas que cumplan con los requisitos de seguridad de la información, protegiendo la información de actividades fraudulentas o usos no autorizados al pasar por redes de comunicación públicas, definir acuerdos sobre licencias de uso, propiedad de los códigos y derechos de propiedad intelectual. Antes de poner en funcionamiento las aplicaciones, se realizan pruebas para detectar fallos que puedan atentar contra la seguridad de la información de la Compañía.

15. POLÍTICAS PARA RELACIONES CON CONTRATISTAS

La compañía, a través de las dependencias que tengan responsabilidades directas con contratistas (supervisores), deben comunicar las políticas de seguridad de la información y hacer énfasis en su cumplimiento e, igualmente, firmar acuerdos de confidencialidad cuando se requiera poner en conocimiento información de la compañía clasificada como confidencial.

Los contratistas que requieran acceso a la red privada de la compañía (RED LAN), deben solicitarlo al supervisor y el área de TI deberá establecer mecanismos que permitan la comunicación con la plataforma tecnológica de la compañía.

Los supervisores deberán hacer seguimiento a los cambios en los servicios suministrados por contratistas al área de TI, de tal forma que no afecten la seguridad de la información y que los nuevos riesgos sean mitigados oportunamente.

16. POLITICA SERVICIO DE SEGURIDAD EN LA NUBE

La compañía requerirá de servicios en la nube lo cual se realizará después de evaluar exhaustivamente el cumplimiento del proveedor con estándares internacionales de seguridad, análisis detallado de riesgos y validación técnica. Además, asegurará la inclusión en los contratos de cláusulas sobre confidencialidad, gestión de incidentes, auditorías periódicas y estrategias claras para la salida segura del servicio.

El uso de estos servicios se administrará bajo estrictas medidas de control de acceso, monitoreo constante, capacitación periódica y auditorías frecuentes, siendo el área de TI la responsable directa del seguimiento y cumplimiento de esta política.

17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Un evento de seguridad son aquellas situaciones donde se presentan posibles fallas en el cumplimiento de las políticas y controles de la seguridad de la información, pero que no afectan el desarrollo de las actividades de la Compañía y puede tratarse con una acción correctiva.

Un incidente de seguridad es aquel que pone en riesgo la seguridad de la información, ya sea de forma intencional o no y ocasiona interrupciones en el desarrollo de las actividades de la Compañía.

Es deber de todos los empleados y contratistas, reportar el área de TI toda situación que genere un evento o incidente de seguridad de la información, que atente contra el normal desarrollo de las actividades de ADA S.A.S Y LAPOINT. El área de TI deberá crear bancos de conocimiento con el tratamiento de incidentes presentados, a fin de resolver incidentes futuros de manera eficiente y eficaz. Los incidentes de seguridad serán evaluados por del área de TI o designará el personal idóneo para realizar estas funciones, quien entregará los resultados para dar el tratamiento requerido.

Para el desarrollo de estas labores puede requerirse el apoyo de otras dependencias de la compañía y/o de empresas o entidades externas.

El CEO de ADA S.A.S Y LAPOINT, es la persona encargada de reportar situaciones ante las autoridades competentes cuando haya implicaciones legales ya sean penales o civiles.

18. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La compañía contará con un plan de continuidad de las actividades más críticas en tecnología, que permita reanudar sus actividades ante la presencia de interrupciones prolongadas en la prestación de los servicios, ya sea por fallos o desastres naturales.

De acuerdo con el análisis de riesgos, se identificarán los eventos con alto impacto en la plataforma tecnológica de la compañía, probabilidad de ocurrencia y sus consecuencias.

Es indispensable implementar planes de mejora acordes a los resultados de las auditorías en pro de obtener las mejoras en el sistema que garanticen la continuidad del negocio. Los planes deberán estar documentados, probados, actualizados de acuerdo con las características de la compañía y deben ser de conocimiento de los empleados, de tal manera que sean conscientes de sus roles y responsabilidades.

La compañía debe establecer mecanismos que permitan tener una continuidad de la operación a fin de reanudar actividades cuando se presente un fallo.

19. CUMPLIMIENTO

La compañía debe cumplir con el marco normativo colombiano y para ello deberá identificar los requerimientos normativos aplicables y contractuales pertinentes para los sistemas de información.

La compañía debe cumplir los derechos de propiedad intelectual sobre el uso de productos de software patentados y realizará revisiones periódicas a fin de que se aplique esta reglamentación.

El área de TI es la dependencia responsable de la correcta aplicación y control de las licencias de productos de software y hardware, así como el número de usuarios permitidos. Está prohibido el uso de productos ilegales o sin licencia.

La compañía tiene definidos acuerdos contractuales con los proveedores que realizan desarrollos de software, donde se señalan los acuerdos de protección de la propiedad intelectual.

Es deber de todos los empleados y contratistas velar por el buen manejo y protección de los datos e información personal, de la cual puedan tener conocimiento por el ejercicio de sus funciones.

Las dependencias que procesen datos personales de beneficiarios, proveedores, empleados y demás terceros, deben garantizar que están autorizados para ello y son responsables de su uso, almacenamiento, distribución y actualización.

ADA S.A.S Y LAPOINT tiene establecida la divulgación de estas políticas y su actualización cuando considere necesario.

Estas políticas están disponibles para la consulta del personal y otras partes interesadas.

FIRMA APROBATORIA DE ESTE DOCUMENTO

Cesar Augusto Echeverri Perez
CEO
Agosto 26 de 2026