1. OBJETIVO

Establecer las políticas y estándares de CIBERSEGURIDAD que son de obligatorio cumplimiento para los colaboradores, usuarios finales y partes interesadas que tengan relación o hagan uso de los sistemas de información de la Organización. La Organización está conformada por las siguientes compañías: NAVES S.A.S., identificada con NIT 860.532.426-7; Compañía Logística Colombiana S.A.S. – CLC S.A.S., identificada con NIT 811.022.799-2; ULOG S.A.S., identificada con NIT 900.160.943-0; GDK S.A.S., identificada con NIT 901.825.461-1; e Inversiones Poseidón S.A.S., identificada con NIT 800.203.705-8, en adelante “la Organización”.

También se establecen las directrices para el uso adecuado de los recursos informáticos y de telecomunicaciones, con el fin de proteger de manera integral los ACTIVOS TECNOLÓGICOS y la información de la Organización.

Esta política establece los principios y lineamientos para gestionar de manera efectiva la CIBERSEGURIDAD de acuerdo con el Estándar Internacional de seguridad BASC en su versión 6 y el Framework CIS Controls v. 7.1.

2. ALCANCE

Esta política aplica a todos los activos de información y tecnológicos de la organización y es de aplicación obligatoria para todas las partes interesadas, usuarios finales y colaboradores de la organización que interactúen con los sistemas de información.

3. DEFINICIONES:

Para la correcta interpretación de esta política y los diversos conceptos que la misma regula e incluye, deberá ceñirse a las definiciones que se describen a continuación:

ACTIVO TECNOLÓGICO: cualquier dispositivo, equipo, software o recurso digital utilizado por la organización para facilitar, mejorar o respaldar sus operaciones y procesos comerciales. Estos activos incluyen hardware (como computadoras, servidores, dispositivos móviles), software (aplicaciones, sistemas operativos), redes de comunicaciones y datos almacenados, entre otros componentes tecnológicos críticos para el funcionamiento de las operaciones de la organización**.**

CIBERSEGURIDAD: se refiere al conjunto de prácticas, procesos, técnicas y tecnologías diseñadas para proteger sistemas informáticos, redes, dispositivos y datos contra amenazas cibernéticas. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información en entornos digitales, mitigando riesgos y protegiendo activos frente a ataques maliciosos y actividades no autorizadas**.**

CLIENTE: se refiere a una persona, empresa u entidad externa que utiliza los servicios ofrecidos por la Organización. Un CLIENTE es alguien que realiza transacciones comerciales con nuestra Organización, ya sea contratando sus servicios o interactuando de alguna manera comercial.

COLABORADOR: un individuo que trabaja en conjunto con otros miembros del equipo para lograr los objetivos y metas de la Organización.

COMITÉ DE GERENCIA: es un grupo colaboradores de la Organización que se reúnen regularmente para tomar decisiones estratégicas y supervisar el funcionamiento general de la organización.

CONTRASEÑA: secuencia de caracteres y símbolos utilizados para determinar que un USUARIO específico requiere acceso a una computadora personal, sistema de información, aplicación o red en particular.

DATOS PERSONALES: toda aquella información asociada a una persona y que permite su identificación o puede hacerlo identificable. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.

DATOS SENSIBLES: son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

DIRECTORIO ACTIVO: servicio de directorio desarrollado por Microsoft que se utiliza principalmente en entornos de redes informáticas basadas en Windows. Su función principal es proporcionar un servicio centralizado de administración de identidades, autenticación y control de acceso para USUARIOS, equipos, aplicaciones y otros recursos en un entorno de red.

HURTO: tomar o retener bienes ajenos contra la voluntad de su dueño, sin intimidación en las personas ni fuerza en las cosas.

INFORMACIÓN CONFIDENCIAL: toda aquella información susceptible de ser tutelada por los derechos humanos a la privacidad, intimidad, honor y dignidad, que se encuentra en posesión de alguno de los sujetos obligados y sobre la que no puede realizarse ningún acto o hecho sin la autorización debida de los titulares o sus representantes legales.

INCIDENTE DE CIBERSEGURIDAD: es un evento o serie de eventos inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio; provocando una pérdida o uso indebido de información, interrupción parcial o total de los Sistemas.

ORGANIZACIÓN: la Organización está conformado por las siguientes compañías, NAVES S.A.S. identificada con NIT 860.532.426-7, Compañía Logística Colombiana S.A.S. – CLC S.A.S. identificada con NIT 811.022.799-2, ULOG S.A.S. identificada con NIT 900.160.943-

0, GDK S.A.S. identificada con NIT 901.825.461-1 e Inversiones Poseidón S.A.S., identificada con NIT 800.203.705-8, en adelante “Organización”.

MAL USO DE ACTIVO TECNOLÓGICO: uso inapropiado de un ACTIVO TECNOLÓGICO, que está siendo utilizado de una manera que no está de acuerdo con su propósito.

MFA: es un proceso de registro en varios pasos que requiere que los USUARIOS ingresen algo más de información que simplemente una CONTRASEÑA.

OFFICE 365: es una solución integral y basada en la nube que combina aplicaciones familiares de Microsoft Office con servicios de colaboración y productividad en línea, permitiendo a las organizaciones mejorar la eficiencia, flexibilidad y seguridad en sus procesos empresariales.

PARTES INTERESADAS: una parte interesada es una persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad de la Organización, dentro de estos: accionistas/propietarios, colaboradores/colaborador, clientes, proveedores y asociados de negocio.

PROVEEDORES DE TECNOLOGIA: un proveedor de tecnología es un socio comercial que ayuda a la Organización a adquirir, implementar y mantener soluciones tecnológicas que les permitan mejorar sus operaciones, aumentar su eficiencia y alcanzar sus objetivos comerciales.

PROVEEDOR DE INFRAESTRUCTURA TI COMO SERVICIO (BACKUP, COPIAS BAJO DEMANDA Y SERVIDORES ALQUILADOS): proveedor que suministra servicios de infraestructura tecnológica a la Organización, incluyendo respaldo de información, copias bajo demanda y servidores alquilados, garantizando la seguridad, disponibilidad e integridad de los datos y activos gestionados, así como el cumplimiento de normas y estándares de seguridad.

PROVEEDORES DE LICENCIAS ON-PREMISE (SOFTWARE INSTALADO EN SERVIDORES DE LA EMPRESA): Proveedores que suministran licencias de software que se instala en los servidores o infraestructura de la organización.

PROVEEDOR O DISTRIBUIDOR DE LICENCIAS DE SOFTWARE INSTALADO EN PCS O ENDPOINTS: Proveedores que suministran software que se instala directamente en computadores de escritorio, portátiles u otros dispositivos del usuario final.

PROVEEDOR DE SERVICIOS EN LA NUBE / HOSTING / SAAS: Provee plataforma / aplicaciones en cloud (pública, privada, híbrida) o software como servicio.

PROVEEDOR DE COMUNICACIONES Y CONECTIVIDAD: Red de telecomunicaciones, enlaces de datos, conectividad entre sedes, IoT, sensores en flota/puerto.

PROVEEDOR DE CONSULTORÍA / INTEGRACIÓN / DESARROLLO A MEDIDA: Ayudan a analizar, adaptar, integrar tecnologías, realizar desarrollos personalizados, vincular sistemas existentes.

PROVEEDOR DE CONSULTORÍA DE CIBERSEGURIDAD: Un proveedor de consultoría de ciberseguridad es una empresa o profesional especializado que ofrece servicios expertos para ayudar a las organizaciones a proteger sus activos digitales, redes, sistemas y datos frente a amenazas cibernéticas.Entre sus principales servicios destacan la evaluación de riesgos, el diseño de estrategias de protección, el cumplimiento normativo, la respuesta a incidentes y la realización de pruebas de hacking ético, que permiten detectar vulnerabilidades mediante simulaciones controladas de ciberataques, fortaleciendo así la seguridad de la organización.

PROVEEDOR SERVICIOS DE IMPRESIÓN: Suministrar, administrar y da soporte a servicios de impresión, copiado y digitalización de documentos, mediante el uso de impresoras, equipos multifuncionales o soluciones de impresión gestionada, ya sean propios o arrendados, utilizados por la organización para el manejo de información física y digital.

PROVEEDOR MANTENIMIENTO DE HARDWARE: especializado en la prestación de servicios de mantenimiento preventivo, correctivo y evolutivo sobre equipos de cómputo, servidores físicos y/o virtuales y componentes asociados de la infraestructura tecnológica, incluyendo diagnóstico, actualización, reparación y soporte técnico presencial o remoto, con el objetivo de asegurar su disponibilidad, rendimiento y estabilidad operativa.

PROVEEDOR DE SUMINISTRO Y COMERCIALIZACIÓN DE EQUIPOS DE CÓMPUTO E INFRAESTRUCTURA TECNOLÓGICA: Proveedor responsable de la venta y suministro de equipos de cómputo, servidores, dispositivos periféricos, accesorios, cables y demás componentes de infraestructura tecnológica, destinados a soportar la operación y las necesidades tecnológicas de la organización.

PROVEEDOR DE ARRENDAMIENTO DE ACTIVOS TECNOLÓGICOS: Proveedor que suministra a la organización activos tecnológicos bajo la modalidad de arrendamiento, sin que exista transferencia de la propiedad de dichos activos en ningún momento de la relación contractual. Este tipo de proveedor pone a disposición de la organización una amplia gama de activos tecnológicos, que pueden incluir, entre otros, equipos de cómputo, servidores, dispositivos de red, equipos de telecomunicaciones, dispositivos de almacenamiento, periféricos, dispositivos móviles, equipos de seguridad, infraestructura tecnológica y cualquier otro activo tecnológico requerido para la operación del negocio. Los activos son entregados para su uso temporal por parte de la organización durante un período definido contractualmente, bajo condiciones específicas de uso, soporte, mantenimiento, actualización, renovación y devolución, según lo establecido en el contrato de arrendamiento.

PROVEEDOR DE SERVICIOS PROFESIONALES: Persona natural o jurídica que, mediante contrato de prestación de servicios, brinda apoyo técnico o consultoría en TIC. Puede requerir accesos temporales a los activos de la organización y debe cumplir los lineamientos de seguridad de la información, ciberseguridad, confidencialidad, mínimo privilegio y la normativa legal vigente.

ROBO: quitar o tomar un elemento con violencia o con fuerza.

TI: tecnologías de la información.

USUARIO: es un identificador, el cual es asignado a una persona para el acceso y uso de la computadora, sistemas, aplicaciones, red, etc.

USUARIO FINAL: la persona designada responsable de utilizar y aprovechar el ACTIVO TECNOLÓGICO para llevar a cabo sus actividades laborales. Esta persona es responsable de mantener el ACTIVO TECNOLÓGICO en condiciones óptimas, siguiendo las políticas y procedimientos establecidos por la Organización, y velando por su seguridad e integridad en el contexto de su trabajo diario.

VPN: es una tecnología que establece una conexión segura y encriptada entre un dispositivo y una red privada a través de Internet. Actúa como un túnel virtual que protege la privacidad y la seguridad de los datos transmitidos.

VULNERABILIDAD: se refiere a una debilidad o fallo en un sistema informático, red, aplicación o dispositivo que podría ser explotado por un atacante para comprometer la seguridad de dicho sistema y realizar acciones no autorizadas. Las vulnerabilidades pueden existir en diferentes componentes de un sistema, incluyendo software, hardware, configuraciones, protocolos de red y prácticas de seguridad.

4. DISPOSICIONES GENERALES

- El área de TI de la Organización es responsable y única área autorizada para gestionar la asignación, modificación e inactivación de USUARIOS en los sistemas de información de la Organización.

- El área de TI de la Organización es responsable y única área autorizada para gestionar la asignación y modificación de roles y permisos en los sistemas de información de la Organización.

- El área de TI de la Organización es la encargada de generar y asignar CONTRASEÑAS iniciales para los USUARIOS del sistema de información, el USUARIO debe realizar el cambio de dichas CONTRASEÑAS lo más pronto posible después de la entrega.

- Los USUARIOS y CONTRASEÑAS son de uso personal e intransferible, está prohibido compartir estos datos con otros colaboradores u USUARIOS FINALES, salvo algunos casos excepcionales y controlados en los que podrán compartir estos datos únicamente con el área de TI de la Organización.

- La CIBERSEGURIDAD hace parte fundamental de los servicios prestados por el área de TI de la Organización, se definirá a través de roles y responsabilidades las tareas y funciones que tendrán LOS COLABORADORES de esta área en relación con CIBERSEGURIDAD, esto con el objetivo de reforzar y validar todos los aspectos asociados a CIBERSEGURIDAD. Los temas críticos de CIBERSEGURIDAD serán tratados dentro del COMITÉ DE GERENCIA.

- El área de TI de la Organización establece y gestiona una serie de controles enfocados en evitar qué riesgos asociados a CIBERSEGURIDAD se materialicen.

- Un componente fundamental que da sustento a esta política es la matriz de riesgos SQE-FOR-014-004 MATRIZ BASC.

- Dentro de los temas tratados en el COMITÉ DE GERENCIA se revisarán los ajustes que se puedan dar a esta política, así como los controles establecidos para la CIBERSEGURIDAD, cuando sea necesario, se realizará la actualización y divulgación de este documento. Se realizará revisión de esta política por lo menos una vez al año.

- El incumplimiento de cualquiera de las normas establecidas en esta política será sancionado de acuerdo con lo establecido en el reglamento interno de trabajo o contrato de servicios firmado entre las partes y de acuerdo con la gravedad de la falta.

- La Organización realizará auditorías periódicas para verificar el cumplimiento de esta política y de los controles establecidos. Se llevarán registros de incidentes de ciberseguridad y se tomarán medidas correctivas en caso de violaciones o incumplimientos.

5. DESCRIPCIÓN

La CIBERSEGURIDAD se refiere a la práctica de proteger los sistemas informáticos, las redes, los programas y los datos de amenazas cibernéticas, como el acceso no autorizado, el ROBO de información, la interrupción del servicio y el daño a la integridad de los sistemas.

El objetivo de la CIBERSEGURIDAD es salvaguardar la confidencialidad, la integridad y la disponibilidad de los datos y los recursos tecnológicos. Esto implica la implementación de medidas preventivas, de detección y de respuesta para proteger los sistemas y minimizar los riesgos de ataques cibernéticos.

Las PARTES INTERESADAS que manejen información de nuestro sistema, deben leer, entender y cumplir con esta política. El incumplimiento de esta política puede resultar en medidas disciplinarias o legales, según corresponda, de acuerdo con lo establecido en reglamentos, contratos comerciales y legislación vigente.

5.1. RESPONSABILIDADES Y CRITICIDAD

Con el fin de fortalecer la gestión de la ciberseguridad, la organización identifica y clasifica de manera general sus partes interesadas, tanto internas como externas, que interactúan directa o indirectamente con los sistemas de información y los activos tecnológicos.

A continuación, se describen dichas partes interesadas, junto con sus responsabilidades y su nivel de criticidad.

5.1.1. LA GERENCIA GENERAL DE LA ORGANIZACIÓN ES RESPONSABLE DE: (CRITICIDAD: ALTA)

a. Establecer y mantener un marco de CIBERSEGURIDAD.
b. Proporcionar los recursos necesarios para implementar y mantener la CIBERSEGURIDAD.

5.1.2. ÁREA DE TI DE LA ORGANIZACIÓN, ES RESPONSABLE DE: (CRITICIDAD: MUY ALTA)

a. Coordinar y supervisar la implementación de las medidas de CIBERSEGURIDAD.
b. Realizar evaluaciones periódicas de riesgos y establecer controles adecuados.
c. Mantener políticas y procedimientos actualizados.
d. Promover la conciencia y la capacitación en CIBERSEGURIDAD.
e. Reportar incidentes de ciberseguridad a la gerencia general y al área legal de la Organización (incluyendo violaciones a lo establecido en esta política).

5.1.3. COMITÉ DE GERENCIA (CRITICIDAD: ALTA)

a. Reunirse periódicamente para reportar, recolectar y analizar situaciones e información asociada a CIBERSEGURIDAD.
b. Tomar decisiones frente a la normatividad, los controles y violaciones asociadas a CIBERSEGURIDAD.
c. Promover la conciencia en CIBERSEGURIDAD.

5.1.4. ÁREA LEGAL DE LA ORGANIZACIÓN (CRITICIDAD: MEDIA)

a. Evaluar y tomar medidas legales (preventivas/correctivas) de acuerdo con lo reportado por TI.

5.1.5. COLABORADORES DE LA ORGANIZACIÓN (EMPLEADOS) (CRITICIDAD ALTA)

Son responsables de cumplir de manera integral con los lineamientos de ciberseguridad definidos en la presente política y sus documentos asociados. En este sentido, deberán:

a. Cumplir con las políticas, normas y procedimientos establecidos en materia de ciberseguridad y seguridad de la información.
b. Hacer uso adecuado, responsable y seguro de los activos de información y recursos tecnológicos de la organización.
c. Proteger la confidencialidad, integridad y disponibilidad de la información a la que tengan acceso, en función de sus roles y responsabilidades.
d. Gestionar de manera segura sus credenciales de acceso, evitando su divulgación o uso indebido.

e. Reportar de forma oportuna cualquier incidente de ciberseguridad o evento sospechoso que pueda afectar a la organización.
f. Actuar conforme a las buenas prácticas de seguridad de la información en el desarrollo de sus actividades diarias.
g. Cumplir con los lineamientos definidos para el acceso, uso y protección de la información, así como con las medidas de control establecidas en los diferentes dominios de esta política.
h. Participar obligatoriamente en las actividades de capacitación, sensibilización y concienciación en ciberseguridad definidas por la organización, así como aplicar los conocimientos adquiridos en el desarrollo de sus funciones.

5.1.6. PROVEEDOR DE INFRAESTRUCTURA TI COMO SERVICIO (BACKUP, COPIAS BAJO DEMANDA Y SERVIDORES ALQUILADOS):
(CRITICIDAD: CRITICO)

a. Plan de copias de seguridad y respaldo.
b. Cifrado de los datos respaldados en reposo y en tránsito.
c. Plan de continuidad y contingencia (disponibilidad del servicio y recuperación).
d. Cumplimiento de Acuerdos de Nivel de Servicio (ANS).
e. Notificación inmediata de incidentes de seguridad.
f. Cumplimiento de normas de protección de datos y seguridad de la información.
g. Eliminación segura de información y activos al finalizar el contrato.
h. Contar con un Plan de Respuesta a Incidentes de Ciberseguridad
i. Documentación necesaria para auditorías y respaldos.
j. El proveedor debe entregar únicamente la documentación técnica necesaria para auditorías de seguridad y procesos de respaldo.
k. Garantizar la seguridad del tráfico de red de la infraestructura alquilada, mediante la implementación, administración y correcta configuración de los controles de firewall, así como la aplicación de las políticas de autorización, segmentación y bloqueo de accesos de acuerdo con lo establecido contractualmente.
l. Garantizar la segregación lógica de la infraestructura virtualizada, asegurando el aislamiento adecuado entre clientes, máquinas virtuales y entornos compartidos, con el fin de prevenir accesos no autorizados, fugas de información o interferencias entre servicios.
m. En caso de que el proveedor cuente con certificaciones, estándares o evaluaciones de seguridad, deberá suministrar a la Organización la evidencia documental correspondiente, incluyendo alcance y vigencia, cuando esta información sea requerida.

5.1.7. PROVEEDORES DE LICENCIAS ON-PREMISE (SOFTWARE INSTALADO EN SERVIDORES DE LA EMPRESA):
(CRITICIDAD: ALTO)

a. Garantizar que el software suministrado cuenta con licencias legales, vigentes y acordes al uso contratado.
b. Entregar el software libre de malware, backdoors o componentes no autorizados, y aplicar configuraciones seguras recomendadas por el fabricante.

c. Proveer parches y actualizaciones de seguridad durante la vigencia del contrato o licenciamiento.
d. Informar oportunamente sobre vulnerabilidades críticas del software y apoyar su corrección.
e. Entregar la documentación mínima necesaria para la instalación, operación y administración segura del software.

5.1.8. PROVEEDOR O DISTRIBUIDOR DE LICENCIAS DE SOFTWARE INSTALADO EN PCS O ENDPOINTS:
(CRITICIDAD: ALTO)

a. Garantizar que las licencias suministradas sean legales, vigentes y acordes al uso contratado.
b. Entregar el software libre de malware, backdoors o componentes no autorizados.
c. Proveer parches y actualizaciones de seguridad del software durante la vigencia de la licencia.
d. Suministrar la documentación básica para instalación, uso y configuración segura del software y ANS de servicio del fabricante.

5.1.9. PROVEEDOR DE SERVICIOS EN LA NUBE / HOSTING / SAAS DE LA ORGANIZACIÓN, SON RESPONSABLES DE:
(CRITICIDAD: MUY ALTA)

a. Asegurar cumplimiento de normativas locales (por ejemplo, Habeas Data, Ley 1581 en Colombia)
b. El almacenamiento y procesamiento de los datos personales y datos operativos deberá realizarse en infraestructuras que estén alineadas con las políticas, normas o certificaciones de protección de datos y seguridad de la información vigentes en el lugar donde dichos datos sean alojados, garantizando su confidencialidad, integridad, disponibilidad y uso adecuado.
c. Cifrar datos en tránsito y en reposo- Ofrecer mecanismos de control de accesos sólidos (MFA para administradores, roles RBAC, segregación de ambientes).
d. Notificar al cliente de manera oportuna cualquier incidente de seguridad o brecha que afecte la confidencialidad, integridad o disponibilidad de los datos.
e. En caso de que el proveedor declare contar con certificaciones, estándares o evaluaciones de seguridad, deberá suministrar a la Organización la documentación oficial que respalde dichas certificaciones, incluyendo informes, alcances y vigencia, cuando aplique.
f. Permitir la realización de auditorías, evaluaciones de seguridad o revisiones técnicas por parte de la Organización o de un tercero designado por esta, cuando dichas actividades se encuentren establecidas contractualmente o cuando la criticidad del servicio así lo requiera.
g. Garantizar la disponibilidad del servicio conforme a los Acuerdos de Nivel de Servicio (ANS) definidos, incluyendo mecanismos de alta disponibilidad y tolerancia a fallos.
h. Implementar y mantener planes de continuidad del negocio y recuperación ante desastres (BCP/DRP), con pruebas periódicas y tiempos de recuperación acordes a la criticidad del servicio.

i. Asegurar la segregación lógica y/o física de los entornos del cliente frente a otros clientes, cuando se trate de infraestructuras compartidas.
j. Proveer mecanismos de respaldo y recuperación de la información, garantizando la integridad, confidencialidad y disponibilidad de los datos.
k. Notificar previamente cambios relevantes en la infraestructura, plataforma o servicio que puedan impactar la seguridad o la operación del negocio.
l. Restringir y auditar los accesos administrativos a la infraestructura y plataformas, aplicando el principio de mínimo privilegio.
m. Asegurar la entrega íntegra de la información de la Organización y la posterior eliminación segura, completa y verificable de la misma al finalizar la relación contractual.
n. Entregar de manera obligatoria la documentación técnica y los lineamientos de seguridad del servicio contratado. Cuando aplique, deberá definirse y formalizarse el modelo de responsabilidades compartidas entre las partes, conforme a lo establecido contractualmente.

5.1.10. PROVEEDOR DE COMUNICACIONES Y CONECTIVIDAD DE LA ORGANIZACIÓN, SON RESPONSABLES DE: (CRITICIDAD:MUY ALTA)

a. Garantizar canales seguros de transmisión de datos.
b. Asegurar disponibilidad de comunicaciones y tolerancia a fallos.
c. Notificar de manera inmediata a la organización cualquier incidente de seguridad, indisponibilidad significativa o evento que pueda afectar la confidencialidad, integridad o disponibilidad de las comunicaciones.
d. Cumplir con la normativa legal y regulatoria aplicable en materia de telecomunicaciones y protección de datos personales (por ejemplo, Habeas Data y Ley 1581 de 2012 en Colombia).
e. Garantizar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos, incluyendo tiempos de disponibilidad, latencia, recuperación y soporte.
f. Implementar planes de continuidad del servicio y recuperación ante fallos de conectividad, con pruebas periódicas acorde a la criticidad del servicio.
g. En caso de que el proveedor declare contar con certificaciones, estándares o evaluaciones de seguridad, deberá suministrar a la Organización la documentación oficial que respalde dichas certificaciones, incluyendo informes, alcances y vigencia, cuando aplique.

5.1.11. PROVEEDOR DE CONSULTORÍA / INTEGRACIÓN / DESARROLLO A MEDIDA SON RESPONSABLES DE: (CRITICIDAD: ALTA)

a. Cumplir con los requisitos de ciberseguridad exigidos por la organización.
b. Aplicar estándares seguros para desarrollo de software e integración de APIs.
c. Documentar todas las dependencias técnicas y componentes usados.

d. Garantizar que no exista exposición innecesaria de información ni conexiones externas no autorizadas o no previamente validadas.
e. Participar en pruebas de seguridad del software antes de pasar a producción.
f. Garantizar la transferencia de conocimiento a los equipos internos de la organización, incluyendo documentación funcional, técnica y de seguridad.
g. Dar cumplimiento a los procedimientos de gestión de cambios y control de versiones definidos por la organización durante el desarrollo, mantenimiento o integración de software, asegurando el conocimiento y la aplicación de la Política de Desarrollo de Software y del instructivos desarrollo y modificación de software.
h. Asegurar que el código desarrollado sea entregado sin credenciales embebidas, puertas traseras, cuentas genéricas o componentes no autorizados.
i. El proveedor será responsable de garantizar que cualquier tercero o subcontratista que contrate para la ejecución del servicio cumpla con el principio de mínimo privilegio en los accesos temporales que se le otorguen, así como de asegurar la revocación inmediata de dichos accesos una vez finalizado el servicio o alcanzado el objetivo autorizado.
j. Garantizar la entrega del código fuente, scripts, configuraciones y artefactos desarrollados, de acuerdo con lo establecido contractualmente.
k. El proveedor debe contar con un Plan de Respuesta a Incidentes de Ciberseguridad debidamente documentado y aprobado por su Gerencia General, el cual deberá estar disponible para verificación cuando la organización lo requiera.
l. Garantizar la corrección o mitigación oportuna de las vulnerabilidades de seguridad identificadas en el software desarrollado, ya sea durante pruebas, auditorías o en operación, de acuerdo con su nivel de criticidad, asegurando la aplicación de parches, ajustes de código o controles compensatorios antes de su paso a producción o en los plazos acordados con la organización.

5.1.12. PROVEEDOR DE CONSULTORÍA DE CIBERSEGURIDAD DE LA ORGANIZACIÓN, SON RESPONSABLES DE:
(CRITICIDAD: MUY ALTA)

a. Realizar todas las pruebas técnicas (pentesting, red team, ethical hacking) exclusivamente sobre activos autorizados en el documento de alcance Firmar acuerdos de confidencialidad (NDA) y comprometerse al manejo seguro de evidencias
b. Evitar la interrupción de operaciones o generación de fallas sin planificación previa (seguridad operativa)
c. No explotar, manipular ni acceder a datos sensibles de usuarios, sistemas de producción o entornos OT (Operational Technology) fuera de entornos de prueba controlados y autorizados.
d. Garantizar el almacenamiento seguro de reportes, capturas y credenciales temporales.
e. Destruir o devolver toda la evidencia al finalizar el contrato (según cláusulas acordadas).
f. Mantener registro detallado de cada prueba realizada y permitir su trazabilidad técnica- Participar en validación de remediaciones (retest) y asesorar al cliente en priorización de hallazgos.

g. Definir y acordar formalmente el alcance, reglas de compromiso (Rules of Engagement), ventanas de ejecución y responsables técnicos antes de iniciar cualquier actividad.
h. Garantizar que el personal asignado cuente con las competencias, certificaciones y experiencia necesarias para la ejecución de las pruebas.
i. Utilizar únicamente herramientas, técnicas y metodologías reconocidas, evitando el uso de software malicioso no controlado o técnicas que excedan el alcance autorizado.
j. Clasificar los hallazgos de seguridad según su criticidad, impacto y probabilidad, proporcionando recomendaciones claras y accionables para su remediación.
k. Notificar de manera inmediata hallazgos críticos que representen un riesgo inminente para la organización, sin esperar la entrega del informe final.
l. Garantizar la independencia y objetividad de los resultados, evitando conflictos de interés durante la prestación del servicio.
m. Custodiar de forma segura las credenciales temporales, tokens o accesos otorgados, asegurando su revocación inmediata al finalizar las pruebas.

5.1.13. PROVEEDOR SERVICIOS DE IMPRESIÓN, SON RESPONSABLES DE: (CRITICIDAD: ALTA)

a. Apoyar en la configuración segura de los equipos suministrados, asegurando que los dispositivos de impresión, copiado y digitalización cuenten con configuraciones de seguridad adecuadas, incluyendo controles de acceso, autenticación de usuarios y la desactivación de servicios innecesarios.
b. Restringir y controlar el acceso del personal técnico, contratistas o subcontratistas a los equipos y a la información.
c. Garantizar que, al finalizar el contrato, realizar mantenimiento mayor o retirar los equipos, la información almacenada sea eliminada de forma segura, completa y verificable.
d. Cumplir con los compromisos de mantenimiento preventivo y correctivo adquiridos contractualmente, asegurando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).
e. Colaborar en la investigación de incidentes de ciberseguridad en los que alguno de los equipos suministrados se encuentre involucrado.
f. Suministrar los insumos de impresión que apliquen dentro de los plazos acordados contractualmente, así como recolectar los desechos generados y garantizar su disposición final adecuada.
g. Suministrar los certificados de disposición final a la organización.

5.1.14. PROVEEDOR MANTENIMIENTO DE HARDWARE, SON RESPONSABLES DE: (CRITICIDAD: ALTA)

a. Ejecutar actividades de mantenimiento preventivo y correctivo sobre equipos de cómputo, servidores y componentes de infraestructura tecnológica, de acuerdo con los lineamientos técnicos.
b. Garantizar que las labores de mantenimiento no comprometan la confidencialidad,

integridad o disponibilidad de la información almacenada o procesada en los equipos intervenidos.
c. Restringir y controlar el acceso del personal técnico, contratistas o subcontratistas a los equipos y a la información.
d. Proteger la información y configuraciones de los equipos durante las actividades de mantenimiento, evitando la copia, extracción o alteración no autorizada de datos.
e. Notificar de manera oportuna a la organización cualquier incidente de seguridad, anomalía o vulnerabilidad detectada durante las labores de mantenimiento.
f. Cumplir con la normativa legal y regulatoria aplicable en materia de protección de datos personales y seguridad de la información, así como con las políticas internas de la organización.
g. Garantizar que, al finalizar el servicio o retirar equipos para reparación externa, no se conserve información, accesos, credenciales o configuraciones pertenecientes a la organización.
h. Asegurar que cualquier tercero o subcontratista involucrado en la prestación del servicio cumpla con las mismas obligaciones de seguridad y confidencialidad establecidas para el proveedor principal.

5.1.15. PROVEEDOR DE SUMINISTRO Y COMERCIALIZACIÓN DE EQUIPOS DE CÓMPUTO E INFRAESTRUCTURA TECNOLÓGICA, SON RESPONSABLES DE:
(CRITICIDAD: ALTA)

a. Suministrar equipos, dispositivos y componentes tecnológicos nuevos u homologados, que cumplan con las especificaciones técnicas, de seguridad y calidad definidas por la organización.
b. Garantizar que los equipos entregados no incorporen software malicioso, componentes alterados o configuraciones que representen un riesgo para la seguridad de la información.
c. Entregar los equipos con configuraciones base seguras o en estado de fábrica, conforme a los lineamientos establecidos por la organización.
d. Proveer la documentación técnica, manuales y garantías correspondientes a los equipos y componentes suministrados.
e. Cumplir con la normativa legal y regulatoria aplicable, así como con las políticas internas de la organización, en lo relacionado con el suministro de tecnología.
f. Garantizar la confidencialidad de la información a la que pueda tener acceso de manera incidental durante los procesos de suministro, transporte o entrega.

5.1.16. PROVEEDOR DE ARRENDAMIENTO DE ACTIVOS TECNOLÓGICOS: SON RESPONSABLES DE:
(CRITICIDAD: ALTA)

a. Respetar la confidencialidad de la información a la que pueda tener acceso durante actividades de entrega, mantenimiento, reemplazo o retiro de los equipos.
b. Cumplir con la normativa legal y regulatoria aplicable, así como con las políticas internas de seguridad de la información y ciberseguridad de la organización.

c. Garantizar que, al finalizar el contrato de arrendamiento, los equipos sean retirados únicamente una vez la organización haya realizado el borrado seguro de la información, o asegurar la eliminación segura, completa y verificable de la información cuando dicho proceso sea responsabilidad del proveedor.

5.1.17. PROVEEDOR DE SERVICIOS PROFESIONALES TI: (CRITICIDAD: ALTA)

a. Cumplir los lineamientos de seguridad de la información y ciberseguridad definidos por la organización.
b. Utilizar únicamente los accesos, credenciales y permisos expresamente autorizados.
c. Mantener la confidencialidad de la información a la que tenga acceso durante la prestación del servicio.
d. Usar los accesos otorgados solo para el alcance y tiempo definido contractualmente.
e. Notificar de manera inmediata cualquier incidente de seguridad, pérdida de información o uso indebido de accesos.
f. Cumplir la normativa legal aplicable en materia de protección de datos personales y confidencialidad de la información.
g. Garantizar la eliminación o devolución de la información y credenciales al finalizar el servicio.
h. No instalar software, herramientas o configuraciones no autorizadas en los activos de la organización.
i. Participar en la investigación de incidentes de ciberseguridad si sus acciones pudieran haber estado relacionadas con el incidente.

El área de TI es responsable de identificar y gestionar las partes interesadas asociadas a cada sistema de información de la organización. Para ello, se debe diligenciar adicionalmente, una matriz que incluya, como mínimo, la siguiente información: el sistema de información correspondiente, la parte interesada, su clasificación (interna o externa), sus necesidades específicas, el nivel de acceso requerido (alto, medio, bajo o nulo) y el impacto en la operación ante una eventual falla del sistema (alto, medio o bajo).

Esta información permitirá analizar la criticidad de cada parte interesada y facilitar la toma de decisiones en materia de gestión de infraestructura tecnológica y ciberseguridad.

5.2. GESTIÓN DE ACCESOS LÓGICOS

a. El área de TI de la Organización es responsable de administrar de forma segura un inventario de cuentas con privilegios administrativos.
b. El área de TI de la Organización será responsable de garantizar la disponibilidad de las credenciales de super usuarios, con el objetivo de asegurar la continuidad de las operaciones de los sistemas de información, incluyendo servidores, equipos de red y aplicaciones críticas. Estas credenciales deberán ser compartidas de manera segura únicamente entre los miembros autorizados del área de TI de la Organización, responsables del acceso y administración de los sistemas mencionados. La transmisión y almacenamiento de dichas credenciales deberá realizarse siguiendo estrictos protocolos de seguridad, como el uso de

herramientas de gestión de contraseñas seguras y la implementación de mecanismos de cifrado, para prevenir accesos no autorizados o compromisos de seguridad.

c. El área de TI de la Organización es responsable de mantener un inventario detallado y actualizado de los sistemas de autenticación y las cuentas de USUARIOS, registrando su nivel de criticidad y accesos autorizados, este debe ser actualizado periódicamente.
d. El área de TI de la Organización es responsable de administrar el control de accesos a los sistemas de información de la Organización, solo las personas autorizadas tendrán acceso a la información.

e. El área de TI de la Organización es responsable de eliminar o inactivar cuentas administrativas que vienen por defecto habilitadas por los fabricantes en los sistemas y activos tecnológicos.
f. El área de TI de la Organización es responsable de garantizar que los colaboradores con roles de administración en Directorio Activo y Office 365 cuenten con dos cuentas diferenciadas: una cuenta con privilegios elevados, destinada exclusivamente a tareas administrativas, y una cuenta estándar para el desarrollo de sus actividades cotidianas.
g. El área de TI de la Organización es responsable de definir y configurar la vigencia máxima de las CONTRASEÑAS de las cuentas de USUARIOS de los sistemas de información de la Organización.

h. Es responsabilidad de los USUARIOS generar CONTRASEÑAS seguras para el acceso a los sistemas de información de la Organización, estas deben cumplir con los siguientes parámetros como mínimo:

- Longitud mínima: Se requiere que la CONTRASEÑA tenga una longitud mínima de 8 caracteres.
- Diversidad de caracteres: La CONTRASEÑA debe tener una combinación de caracteres alfanuméricos (letras y números) y caracteres especiales (por ejemplo, @, #, $, %), además, la inclusión de letras tanto en mayúscula como en minúscula.
- No utilizar información personal, como nombres propios, fechas de nacimiento, números de cédula o teléfono.
- No utilizar palabras comunes: Se recomienda evitar el uso de palabras comunes y secuencias obvias, ya que pueden ser vulnerables a ataques de fuerza bruta.
- Cambio periódico: es obligatorio cambiar la CONTRASEÑA, por lo menos, cada 90 días por parte del USUARIO FINAL.
- Se recomienda para mayor seguridad, si el sistema lo permite, no usar palabras sino frases para la generación de estas CONTRASEÑAS.
- No se deben de reutilizar contraseñas, siempre deben ser diferentes.

i. Está completamente prohibido guardar las contraseñas de acceso a los sistemas de información de la organización y las contraseñas personales en los navegadores web autorizados por el área de TI. De igual manera, el área de TI debe implementar controles que restrinjan esta opción al usuario final en los activos tecnológicos de la organización.

j. Herramientas de secuencia de comando como, por ejemplo: Microsoft PowerShell y Python estarán habilitadas en los equipos de la Organización únicamente para personas que ejerzan un rol administrador.
k. El área de TI de la Organización es responsable de garantizar que todo proceso de autenticación debe ser transmitido a través de canales seguros (cifrados).
l. El área de TI de la Organización es responsable de la gestión de cuentas para el acceso a los sistemas de información del Organización, por tanto, todo inicio o terminación de un vínculo laboral o contractual que involucre USUARIOS de cualquier sistema de información debe ser reportado al área de TI por parte del área de personas del Organización.
m. Es responsabilidad del área de Personas de la Organización comunicar al área de TI de la Organización oportunamente los ingresos, cambios y retiros de COLABORADORES, indicando los datos necesarios para poder asignar o retirar los roles acordes a sus funciones, para los contratos a término fijo se debe confirmar la fecha de terminación de contrato con el objetivo de programar caducidad en las cuentas.
n. En caso de que un PROVEEDOR, CLIENTE o asociado de negocio requiera acceso a cualquier sistema de información digital de la Organización, por naturaleza del negocio, la Unidad de Negocio debe escalar el requerimiento al área de TI con los datos básicos de identificación de la persona y la empresa (nombre completo, tipo y número de identificación, correo electrónico, número de contacto, nombre de empresa, NIT de empresa y rol) con el objetivo de poder crear y asignar las credenciales. Es también responsabilidad de la Unidad de Negocio reportar al área de TI la terminación del vínculo contractual con el Organización para que el área de TI de la Organización pueda proceder con la inactivación de la cuenta.
o. Con el objetivo de proteger la seguridad y la privacidad de la información, todos los usuarios están obligados a bloquear la sesión de sus activos tecnológicos al levantarse de su puesto de trabajo.
p. El área de TI de la Organización es responsable de definir y configurar un tiempo máximo de inactividad para el bloqueo automático de pantalla, estableciendo estos parámetros con base en buenas prácticas de ciberseguridad.
q. El personal del área de TI está autorizado para tomar medidas de seguridad ante el hallazgo de un equipo desatendido que represente un incumplimiento a la política de ciberseguridad. Estas acciones pueden incluir el bloqueo de la sesión del equipo y el registro del incumplimiento mediante evidencia fotográfica. Asimismo, se notificará al responsable de ciberseguridad.
r. El área de TI de la Organización es responsable de habilitar modos de autenticación para el acceso seguro a las aplicaciones de la Organización, en lo posible habilitando métodos de MFA y/o VPN.
s. Todo sistema de información que soporte la opción de doble autenticación (MFA) debe tenerla habilitada de forma obligatoria para todos los usuarios.
t. El área de TI de la Organización realiza revisiones periódicas y aleatorias de logs de acceso en las diferentes aplicaciones que componen los sistemas de información críticos, estos logs se activaran en los sistemas que soporten este tipo de registro.
u. No está permitido el acceso remoto a equipos de cómputo para los colaboradores, este proceso es exclusivo del área de TI de la Organización para la prestación de soporte técnico de forma remota. Las excepciones aplicadas a este numeral

deberán autorizarse por la Gerencia General y formalizarse por medio de la plataforma de soporte de mesa de ayuda.

v. Los accesos remotos a equipos de cómputo y servidores están protegidos mediante autenticación segura y conexiones cifradas.

5.3. PROTECCIÓN DE DATOS

a. El área de TI de la Organización gestionará el acceso o bloqueo de proveedores de correo electrónico o almacenamiento en nube, de acuerdo con las listas blancas de software.
b. En la Organización utilizamos tecnologías y procesos de cifrado para el almacenamiento seguro de dispositivos móviles.
c. El área de TI de la Organización es responsable de implementar controles para proteger los DATOS PERSONALES, DATOS SENSIBLES e INFORMACIÓN CONFIDENCIAL de accesos no autorizados.
d. Todo tratamiento de datos personales debe estar alineado con la Política de Tratamiento de Datos de la organización y cumplir con la normativa vigente.
e. La organización dispone de sistemas de videovigilancia (CCTV) y grabación de audio mediante los cuales se recolecta información, debidamente informada a través de avisos visibles al ingreso a las instalaciones. En consecuencia, toda solicitud de acceso consulta o suministro de la información almacenada deberá contar con la autorización previa y expresa del área legal de la organización.
f. No se debe acceder, copiar, modificar o divulgar DATOS PERSONALES, DATOS SENSIBLES o INFORMACIÓN CONFIDENCIAL sin la debida autorización. El acceso a la información de la Organización debe ser autorizado únicamente a aquellos USUARIOS que requieran dicha información para llevar a cabo sus labores.
g. El área de TI de la Organización establecerá procesos de clasificación de datos para determinar el tipo de dato y el nivel adecuado de protección.
h. El área de TI de la Organización administra los dispositivos de almacenamiento externo que se pueden utilizar en los equipos de cómputo de la Organización, tanto para lectura como para escritura.
i. Las PARTES INTERESADAS deberán ceñirse a las obligaciones y compromisos asociados al tratamiento de DATOS PERSONALES contenidas, sin limitarse a este y según le aplique, en la POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES, contratos suscritos con la Organización y el reglamento Interno de Trabajo.
j. El área de TI es responsable de administrar los permisos para la carga de imágenes en las cuentas corporativas. Esto incluye otorgar los permisos necesarios para que los usuarios puedan subir fotos a su perfil en Office 365 u otras herramientas corporativas, garantizando un control adecuado sobre esta información personal y evitando la exposición de datos de exempleados o cualquier inconveniente relacionado con la privacidad y el tratamiento de datos personales.

5.4. GESTIÓN DE ACTIVOS TECNOLÓGICOS.

a. El área de TI de la Organización es responsable del control de todos los ACTIVOS TECNOLÓGICOS de la Organización, mediante un inventario detallado y actualizado.
b. El área de TI de la Organización es responsable de dar disposición final a los ACTIVOS TECNOLÓGICOS y accesorios relacionados para su correcto funcionamiento (cable de poder, adaptador de voltaje, teclado, mouse, cable red), que hayan cumplido su ciclo de vida útil, de acuerdo con lo estipulado en el plan de Gestión Ambiental SQE-PLN-001**.**
c. Es responsabilidad del área de TI de la Organización, de forma periódica realizar un escaneo de red en búsqueda de dispositivos no autorizados y tomar las medidas de control necesarias para su respectiva eliminación.
d. Para solicitar soporte técnico o requerimientos para los ACTIVOS TECNOLÓGICOS, los USUARIOS deben ceñirse a lo establecido en el Procedimiento Mesa de Ayuda ITE-PRO-001**.**
e. Para solicitud de asignación de ACTIVOS TECNOLÓGICOS, los colaboradores deben ceñirse a lo establecido en el procedimiento Para El Aprovisionamiento De Servicios De TI ITE-PRO-002, en donde se indica como proceder para asignación de ACTIVOS TECNOLÓGICOS.
f. Para solicitud de recolección de ACTIVOS TECNOLÓGICOS para COLABORADORES por desvinculación laboral, ya sea por terminación de contrato o renuncia voluntaria, se debe seguir lo establecido en el documento procedimiento para el **aprovisionamiento de servicios de TI ITE-PRO-002,** el cual indica como se realiza el proceso de devolución de ACTIVOS TECNOLÓGICOS de la Organización por parte del COLABORADOR saliente de la organización.
g. Cuando una persona natural termine su contrato laboral o acuerdo de servicios con alguna empresa de LA ORGANIZACIÓN, debe entregar en horario laboral y el mismo día de la terminación, los ACTIVOS TECNOLÓGICOS que LA ORGANIZACIÓN le asignó. Estos deben entregarse en la oficina en la cual estaba vinculada la persona, si es en Bogotá directamente al área de TI de LA ORGANIZACIÓN, si es en alguna de las sucursales al jefe inmediato o en su defecto la persona de administración de dicha oficina (quien será guiada por TI para la recolección de los ACTIVOS TECNOLÓGICOS).
h. El USUARIO FINAL debe proteger y mantener en buen estado los ACTIVOS TECNOLÓGICOS asignados. Esto incluye no realizar modificaciones o alteraciones no autorizadas en el hardware o software (no está permitido pegar sticker o calcomanías en los ACTIVOS TECNOLÓGICOS), así como reportar cualquier daño, pérdida o ROBO de los equipos de inmediato al área de TI de la Organización.
i. Los daños causados por MAL USO DEL ACTIVO TECNOLÓGICO deberán ser asumidos por el USUARIO FINAL, para esto el área de TI de la Organización gestionará la reparación del ACTIVO TECNOLÓGICO, el 100 % del costo de reparación será descontado por nómina al COLABORADOR, las siguientes acciones son consideradas como MAL USO DE ACTIVO TECNOLÓGICO:

- Caídas y golpes del ACTIVO TECNOLÓGICO.
- Presión excesiva en pantalla o teclado del ACTIVO TECNOLÓGICO.
- Uso inadecuado del cargador de voltaje del ACTIVO TECNOLÓGICO.

- Manipulación brusca de puertos y conectores del ACTIVO TECNOLÓGICO.
- Exposición a temperaturas extremas del ACTIVO TECNOLÓGICO.
- Derrames de líquidos, sobre el ACTIVO TECNOLÓGICO.
- Daños ocasionados por el consumo de alimentos sobre o frente al ACTIVO TECNOLÓGICO.
- No transportar los ACTIVOS TECNOLÓGICOS de forma segura.
- Pegar sticker o calcomanías en los ACTIVOS TECNOLÓGICOS.

j. En caso de existir ambigüedad sobre las causas del daño del ACTIVO TECNOLÓGICO, se debe recurrir a un proceso de diagnóstico con un tercero y, si aplica, descargos con el apoyo del área de Personas de la Organización, para aclarar las causas del daño. Si como resultado del proceso de investigación se logra concluir que la responsabilidad sobre el daño del ACTIVO TECNOLÓGICO es parcial, se descontara al COLABORADOR el 50% del valor de la reparación o reposición.

k. Para el traslado de ACTIVOS TECNOLÓGICOS fuera de las instalaciones de la Organización es imperativo que el COLABORADOR cumpla con las medidas de seguridad que se describen a continuación:

- **Para computadores portátiles:**
  Estos equipos solamente deben transportarse fuera de las instalaciones de la Organización cuando las funciones del COLABORADOR así lo demanden o para hacer uso del beneficio de Home Office, de acuerdo con las políticas establecidas por el área de Personas de la Organización para este beneficio. Para esto cada COLABORADOR debe tomar las siguientes medidas de seguridad:
  - Transportarlo cuando sea estrictamente necesario y para poder dar cumplimiento al desarrollo de sus labores.
  - En caso de transportarlo en un vehículo personal o corporativo, es imperativo ubicar el vehículo en lugares seguros (parqueaderos que cuenten con seguridad, donde se genere un pago por el almacenamiento y cuidado del vehículo), está prohibido dejar computadores portátiles almacenados dentro de vehículos que el COLABORADOR haya dejado abandonado en un lugar público (bahías, calles, parques o similar).
  - Si el computador se almacena dentro de un vehículo, se debe dejar el computador dentro del baúl del vehículo con el baúl asegurado y portar las llaves, esto para mayor seguridad y que no sea fácilmente visible desde el exterior del vehículo, si el COLABORADOR se dirige a una zona segura (Ejemplo: instalaciones de otra empresa, Centro comercial, Restaurante o similar) preferiblemente llevar consigo el computador dentro del maletín que le suministró la empresa, para disminuir el riesgo de ROBO.
  - Siempre que requiera transportar el computador, fuera de las instalaciones de la Organización, este se debe almacenar en el maletín o morral que le suministró la Organización.

- **Teléfonos móviles:**
  Para estos ACTIVOS TECNOLÓGICOS se definen las siguientes medidas de cuidado:
  - Transportarlos dentro del maletín o morral asignado por el Organización, en su defecto en algún bolsillo seguro de las prendas del COLABORADOR.
  - En caso de movilizarse en servicio público o estar en medio de una multitud de personas, tomar medidas adicionales para disminuir el riesgo de ROBO o perdida (por ejemplo: ubicar el maletín frente al cuerpo del COLABORADOR, almacénelo e los bolsillos más seguros y menos propensos a la modalidad de cosquilleo, entro otros).
  - Evite al máximo exponer a la vista de los demás el teléfono en lugares públicos que se identifiquen como inseguros (transporte público, en lugares solos, en la calle a altas horas de la noche, frente a personas sospechas, en ubicaciones que tengan altos índices de HURTO e inseguridad).
  - No abandonar el teléfono móvil en lugares públicos.

- **Impresoras portátiles:**
  Estos equipos solamente deben transportarse fuera de las instalaciones de la Organización cuando las funciones del COLABORADOR así lo demanden. Para esto es importante que cada COLABORADOR tome las siguientes medidas de seguridad:
  - Transportarlo cuando sea estrictamente necesario y para poder dar cumplimiento al desarrollo de sus labores.
  - En caso de transportarlo en un vehículo personal o corporativo, es imperativo ubicar el vehículo en lugares seguros (parqueaderos que cuenten con seguridad, donde se genere un pago por el almacenamiento y cuidado del vehículo), está prohibido dejar impresoras portátiles almacenadas dentro de vehículos que el COLABORADOR haya dejado abandonado en un lugar público (bahías, calles, parques o similar).
  - Si la impresora se almacena dentro de un vehículo, se debe dejar la impresora dentro del baúl del vehículo con el baúl asegurado y portar las llaves, esto para mayor seguridad y que no sea fácilmente visible desde el exterior del vehículo, si el COLABORADOR se dirige a una zona segura (Ejemplo: instalaciones de otra empresa, Centro comercial, Restaurante o similar) preferiblemente llevar consigo la impresora dentro del maletín que le suministró la empresa, para disminuir el riesgo de ROBO.
  - Siempre que requiera transportar la impresora, fuera de las instalaciones de la Organización, este se debe almacenar en el maletín o morral que le suministró la Organización.

- **Otros ACTIVOS TECNOLÓGICOS:**
  - En caso de que el COLABORADOR requiera, estrictamente para el cumplimiento de sus funciones, transportar otro tipo de ACTIVOS

TECNOLÓGICOS, almacenar estos en el morral o maletín suministrado por la Organización.
- Aplicar las mismas medidas establecidas para computadores portátiles.

En caso de presentarse HURTO, ROBO o pérdida de cualquier ACTIVO TECNOLÓGICO y se evidencie que el COLABORADOR no tomó estás medidas (para situaciones en las cuales exista ambigüedad sobre los hechos reportados, se aplicará un proceso de descargos conducido por el área de Personas de la Organización), el valor del ACTIVO TECNOLÓGICO será descontado de nómina a la persona responsable del mismo, el valor a descontar se establecerá de acuerdo con la depreciación del ACTIVO TECNOLÓGICO establecido por el área de Contabilidad de la Organización.

l. En caso de ROBO o pérdida de un ACTIVO TECNOLÓGICO, el COLABORADOR debe seguir el siguiente proceso:
   - Reportar de forma inmediata la novedad al área de TI de la Organización, de acuerdo con lo establecido en el procedimiento “Mesa de ayuda”, indicando los siguientes datos: Tipo de ACTIVO TECNOLÓGICO, fecha y hora del evento, lugar y clasificación: ROBO con violencia, HURTO o pérdida.
   - Interponer denuncia ante fiscalía del ROBO o pérdida del ACTIVO TECNOLÓGICO y enviar soporte con número de denuncia al área de TI de la Organización.

m. Los ACTIVOS TECNOLÓGICOS proporcionados deben ser utilizados exclusivamente para fines relacionados con las actividades laborales y en cumplimiento de las políticas establecidas.

n. El área de TI de la Organización es responsable de mantener un inventario detallado del software autorizado en los ACTIVOS TECNOLÓGICOS de la Organización.

o. El área de TI de la Organización es la única autorizada para realizar instalación o desinstalación de software en los ACTIVOS TECNOLÓGICOS de la Organización. Esta completamente prohibida la instalación de software por parte de USUARIOS FINALES en los ACTIVOS TECNOLÓGICOS de la Organización

p. El área de TI de la Organización es responsable de definir una lista blanca de Software que contiene las aplicaciones autorizadas y las características técnicas para su uso en los ACTIVOS TECNOLÓGICOS de la Organización.

q. El área de TI de la Organización definirá los procedimientos para la configuración segura del software y SO en los ACTIVOS TECNOLÓGICOS.

r. El área de TI de la Organización es responsable de mantener un repositorio centralizado que almacene únicamente los instaladores de software previamente validados por el responsable de ciberseguridad, con el fin de proporcionar una capa adicional de protección al software que será instalado en los activos tecnológicos de la Organización.

s. El área de TI de la Organización es la responsable de velar por la integridad de la información que se almacene en los ACTIVOS TECNOLÓGICOS de la Organización.

t. Únicamente LOS COLABORADORES del área de TI de la Organización pueden tener privilegios administrativos sobre ACTIVOS TECNOLÓGICOS, si se requiere

alguna excepción a esta regla, debe ser autorizada por gerencia, estas excepciones se documentarán.

u. El área de TI de la Organización es responsable de la seguridad física y lógica de los ACTIVOS TECNOLÓGICOS bajo su custodia (equipos disponibles, centro de datos o en proceso de baja).
v. Toda la información almacenada en los ACTIVOS TECNOLÓGICOS de la Organización será considerada propiedad de esta, el área de TI de la Organización tiene un monitoreo constante y acceso total a estos activos y a la información allí almacenada, por tal motivo los COLABORADORES deben abstenerse de almacenar en estos equipos información personal.
w. Ningún colaborador deberá almacenar información personal sensible en los activos tecnológicos de la organización, incluyendo, pero no limitándose a computadores, dispositivos móviles, correo electrónico y servicios de nube corporativa. Esto abarca datos como fotografías íntimas, conversaciones privadas, historial de navegación, resultados o exámenes médicos, información financiera, credenciales personales, orientación sexual y cualquier otro dato personal sensible. El objetivo es proteger la integridad de los colaboradores y reducir el riesgo de filtración, uso indebido o divulgación no autorizada de dicha información.
x. Está prohibido conectar equipos personales y elementos periféricos no autorizados a la infraestructura tecnológica de la Organización, para casos puntuales en los que un CLIENTE, PROVEEDOR o asociado requiera conexión con internet en nuestras instalaciones, se habilitarán redes aisladas para invitados.
y. El área de TI de la Organización es responsable por garantizar que todos los ACTIVOS TECNOLÓGICOS críticos de la Organización tengan instalado un sistema de protección contra malware, que este sistema de protección contra malware actualice sus firmas y base de datos de amenazas, que realice un análisis antimalware de los medios extraíbles cuando un USUARIO lo inserte o conecten al ACTIVO TECNOLÓGICO, que controle la ejecución automática de software desde medios extraíbles.

5.5. GESTIÓN DE CONTINUIDAD

a. El área de TI de la Organización es responsable de identificar y gestionar las VULNERABILIDADES de seguridad existentes en la red corporativa e infraestructura de la Organización.
b. El área de TI de la Organización es responsable de velar porque el software utilizado en los ACTIVOS TECNOLÓGICOS cuente con soporte de fabricante, actualizaciones y licenciamiento, pueden existir excepciones de software de uso gratuito empresarial que estén autorizados por el fabricante y suministren el soporte de actualizaciones de seguridad como mínimo, además el uso de software de código abierto implementadas bajo el control del área de TI de la Organización.
c. El área de TI de la Organización es responsable de velar porque que todos los sistemas operativos y aplicaciones de terceros cuenten con las ultimas actualizaciones de seguridad proporcionadas por el fabricante.
d. Todos los ACTIVOS TECNOLÓGICOS con capacidad de registrar eventos del sistema deberán tener activados logs mínimos de seguridad, con el fin de facilitar auditorías e investigaciones, se deben almacenar y revisar con regularidad.

e. El área de TI de la Organización cuenta con un plan de copias de seguridad regular para proteger los datos y sistemas críticos. Se realizarán copias de seguridad periódicas y estas serán almacenadas en ubicaciones seguras.
f. El área de TI de la Organización tiene la responsabilidad de asegurar la integridad, confidencialidad y disponibilidad de las copias de seguridad.
g. El área de TI de la Organización establecerá un plan de respuesta para abordar y gestionar de manera efectiva los INCIDENTES DE CIBERSEGURIDAD.
h. Se establece que únicamente el área de TI de la Organización está autorizada para manejar y entregar información relacionada con INCIDENTES DE CIBERSEGURIDAD. Los demás COLABORADORES deben abstenerse de divulgar o compartir cualquier detalle sobre este tipo de incidentes con personas ajenas al área de TI de la Organización.
i. El área de TI de la Organización es responsable de reportar al COMITÉ DE GERENCIA y al área Legal de la Organización los INCIDENTES DE CIBERSEGURIDAD que se presenten en la Organización.
j. El área de TI de la Organización realizará simulacros relacionados con CIBERSEGURIDAD para determinar la efectividad de los controles establecidos en el grupo y la cultura de seguridad de los USUARIOS del sistema de información.
k. El área de TI de la Organizaciónes la responsable de implementar un programa de pruebas de penetración que incluya una gama completa de ataques combinados, como ataques inalámbricos, basados en clientes y de aplicaciones web.
l. El área de TI de la Organización establecerá y actualizará periódicamente una Matriz de Riesgos de CIBERSEGURIDAD, la cual contempla: probabilidad, impacto y controles.
m. El área de TI de la Organización realizará evaluaciones periódicas de riesgos y se establecerán controles para mitigarlos.

5.6. GESTIÓN DE SEGURIDAD EN LA OPERACIÓN

a. El área de TI de la Organización es responsable por garantizar el uso de navegadores y cliente de correo electrónico con soporte.
b. Está prohibido el uso de navegadores web y/o complementos de navegadores que no estén autorizados por la Organización, El área de TI de la Organización velará porque esto se cumpla.
c. Está prohibido el acceso a clientes de correo electrónico no autorizados. El área de TI es responsable de permitir, controlar o bloquear el acceso a los clientes de correo electrónico utilizados dentro de la organización.
d. Está prohibido el acceso a sistemas de almacenamiento y compartición de información en la nube que no estén autorizados por el área de TI. El área de TI es responsable de autorizar, controlar o bloquear el acceso a estos servicios dentro de la organización.
e. La opción de compartir información en la nube con usuarios externos debe estar restringida. Solo debe estar habilitada la compartición de información con usuarios de la misma organización o con tenants de confianza previamente autorizados.
f. Está prohibida la navegación en internet en sitios de ocio que no sean inherentes a las labores que desempeñan los COLABORADORES de la Organización, el área de TI de la Organización es responsable de aplicar restricciones de navegación dentro y fuera de la red.

g. El área de TI de la Organización es responsable de velar porque las URL y DNS que se consuman en los recursos corporativos sean seguras y estén alineadas con la naturaleza del negocio.
h. El área de TI de la Organización es responsable de garantizar la seguridad del servicio de correo electrónico, con el objetivo de reducir la posibilidad de correos electrónicos falsificados o modificaciones de dominios válidos, debe tener implementado un estándar de autenticación de correo electrónico diseñado para combatir el phishing y la suplantación de identidad en los correos electrónicos.
i. El área de TI de la Organización es responsable de definir, filtrar y bloquear en el servicio de correo electrónico extensiones de archivos que sean potencialmente inseguras y que no estén alineadas con la naturaleza del negocio.
j. El área de TI de la Organización es responsable de garantizar que todos los PC y servidores de la Organización tengan instalado un software de protección antimalware (**EDR)**, el cual debe ser gestionado desde un panel de control centralizado para facilitar su administración y detención de amenazas.
k. El área de TI de la Organizaciónes la responsable de velar porque el software de seguridad antimalware **(EDR)** actualice su motor de análisis y su base de datos de firmas de acuerdo con lo disponible por el fabricante.
l. El área de TI de la Organización es responsable de garantizar que el software **EDR**, realice análisis antimalware de forma automática y periódica a los medios de almacenamiento locales y extraíbles, además de bloquear la ejecución automática de contenido.
m. La Organización tiene la responsabilidad de asignar los recursos económicos necesarios y acordes a las posibilidades del negocio para realizar una administración de la CIBERSEGURIDAD en línea con esta política.
n. El área de TI de la Organización es responsable por solicitar los recursos necesarios a la Organización con el objetivo de mantener hardware y software licenciados y actualizados para proteger la infraestructura de TI.
o. El área de TI de la Organización es responsable de comunicar a las PARTES INTERESADAS las amenazas potenciales para la CIBERSEGURIDAD, así como los INCIDENTES DE CIBERSEGURIDAD que se materialicen, según la afectación que estas puedan tener en las diferentes partes.

5.7. GESTIÓN DE LAS TELECOMUNICACIONES

a. El área de TI de la Organización tiene la responsabilidad de administrar reglas de firewall y filtrado de puertos de comunicación del Organización.
b. El área de TI de la Organización es responsable de garantizar una adecuada operación y seguridad de los equipos de comunicaciones de red de la Organización, esta responsabilidad abarca la actualización de firmware, parches de seguridad y configuraciones necesarias para mantener la integridad y eficiencia de la infraestructura de red.
c. El área de TI de la Organización es responsable de generar un control para la denegación de comunicaciones con direcciones IP de Internet no utilizadas o maliciosas conocidas, también es responsable de la denegación de comunicación sobre puertos de comunicaciones no autorizados.
d. El área de TI de la Organización es responsable por mantener un inventario detallado y actualizado de todos los ACTIVOS TECNOLÓGICOS de acceso inalámbrico a la red de la Organización.
e. Es responsabilidad de todos los USUARIOS FINALES de la Organización deshabilitar el sistema de acceso a la red inalámbrica (Wi-Fi) cuando no se esté utilizando esta red, los dispositivos como lo son las computadoras portátiles, teléfono móvil, tablet, etc., el objetivo es asegurar la red de la Organización, la eficiencia energética y la reducción de interferencias electromagnéticas.
f. Es responsabilidad del área de TI de la Organización inhabilitar la conexión inalámbrica en los dispositivos que no lo requieran, de áreas compartidas o publicas dentro de la Organización.
g. El área de TI de la Organización es responsable por asegurar que las comunicaciones inalámbricas de la Organización cuenten con un sistema de seguridad de cifrado de datos.
h. El área de TI de la Organización es responsable de administrar las redes inalámbricas de la Organización, debe garantizar la segmentación de la red inalámbrica para equipos confiables y no confiables.

5.8. ENTRENAMIENTO EN CIBERSEGURIDAD

El área de TI de la Organización es responsable de diseñar e implementar un programa de capacitación y concienciación en ciberseguridad, el cual deberá mantenerse actualizado conforme a las tendencias, amenazas, políticas y tecnologías vigentes.

La participación en las actividades de capacitación definidas en este programa es de carácter obligatorio para todos los colaboradores. En este sentido:

a. La inasistencia reiterada e injustificada a los espacios de capacitación será considerada una falta grave y será gestionada conforme a lo establecido en el Reglamento Interno de Trabajo (RIT).
b. El área de TI podrá evaluar y recomendar la restricción parcial o total del acceso a herramientas tecnológicas para aquellos colaboradores que incumplan de manera reiterada con estas obligaciones, en función del riesgo que representen para la organización.

c. Los colaboradores que de manera reiterada no superen satisfactoriamente los simulacros de ciberseguridad, o que se vean involucrados en incidentes derivados de error humano o incumplimiento de los controles de seguridad, estarán sujetos a las medidas disciplinarias definidas en el RIT.

5.9. DESARROLLO DE SOFTWARE

El área de TI de la Organización ha establecido una política específica para todo lo relacionado con desarrollo de software la cual se debe cumplir por todas las PARTES INTERESADAS involucradas en estos procesos, la política se encuentra publicada en el sistema integrado de gestión de la Organización y tiene el nombre POLÍTICA DE DESARROLLO DE SOFTWARE ITE-POL-005.

6. SANCIONES

Cualquier incumplimiento de esta política o de los documentos de control asociados será evaluado de acuerdo con su naturaleza, impacto y recurrencia. En función de ello, podrá dar lugar a medidas correctivas o disciplinarias, conforme a lo establecido en el Reglamento Interno de Trabajo y demás normas aplicables de la Organización.

CONTROL DE CAMBIOS

No.	Fecha	Versión	Modificación	Elaboró	Revisó	Aprobó
1	02-Feb-19	.003	• Cambio de Logo • Actualización de código por Listado Maestro • Adición del cuadro de control de cambios			Victor Abril **JEFE DE TI**
2	21-Jul-23	.004	• Cambio de nombre de la política • Actualización general de la política			Jorge Blanco **Gerente A&F**
3	05-May-24	.005	• Actualización general de la política			Catalina Viancos **Gerente General**
4	20-Ago-24	.006	• Inclusión de firma de gerente general como constancia de aprobación			Francisco Páez **Gerente General**
5	29-Abr-26	.007	• Actualización de objetivo y alcance del documento. • Incorporación de nuevas definiciones, incluyendo la clasificación de tipos de proveedores. • Se establece la denominación general de las empresas como “La Organización”. • Ampliación de la categorización de los proveedores de TI y se detallan sus responsabilidades según el tipo. • Incorporación de cláusulas en el numeral 5.2 y actualización de conceptos. • Incorporación de cláusulas en el numeral 5.3. • Incorporación de cláusulas en el numeral 5.4. • Actualización numeral 5.8.	William Maldonado **Auxiliar TI**	Andersson Montaño **Jefe TI**	Sandra Perafán **Gerente A&F**