POLÍTICA DE SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Triple A S.A. E.S.P.

Código: DI-SI-POL-2

Elaborado por:	Revisado por:	Aprobado por:
Yesenia Yance Díaz **Oficial de Ciberseguridad**	Jonas Urbano J. **Subgerente de Sistemas**	Ramón Hemer R. **Gerente General**

Documento aprobado electrónicamente en Software Kawak

REGISTRO DE CAMBIO

Versión No.	Fecha	Resumen de los cambios
01	05/11/2021	Creación de la política
02	17/06/2024	Se modifica el nombre del documento antes “Política de seguridad informática” ahora “Política de seguridad informática y ciberseguridad”. Se agregan los controles pertinentes según estándares de ciberseguridad y buenas prácticas.

1. INTRODUCCION

La dirección de Triple A E.S.P, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación su estrategia de Ciberseguridad buscando establecer un marco de confianza en el ejercicio de sus deberes con los clientes, proveedores y colaboradores, todo enmarcado en el cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para Triple A E.S.P, la protección de los activos de información busca la disminución del impacto generado sobre su operación y los datos relacionados, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

2. OBJETIVO

Proteger, administrar y preservar objetivamente la información y la operación de Triple A E.S.P junto con las tecnologías utilizadas para su procesamiento y disponibilidad, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de minimizar al máximo los riesgos asociados a la seguridad informática y ciberseguridad que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

Establecer las medidas y lineamientos de seguridad informática y ciberseguridad a cumplir por parte de los colaboradores, accionistas, proveedores y terceros, con el fin de proteger los activos de información, contra accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, mal uso o cualquier incidente de seguridad que se pueda producir en forma intencional o accidental.

3. DOCUMENTOS DE REFERENCIA

ISO 27001	Norma internacional de Seguridad de la Información
NIST CSF	Marco de Seguridad Cibernética
OWASP	Open Web Application Security Project

4. ALCANCE

El alcance de la Política de seguridad informática y ciberseguridad aplica a Triple A E.S.P y a todas sus sedes en la región, sus colaboradores, socios, proveedores, y terceros abarcando los activos de información incluidos los datos personales.

5. GLOSARIO DE TERMINOS

TERMINO	DEFINICIÓN
ACL	En seguridad informática, una lista de control de acceso es una lista de permisos asociados con un recurso del sistema. Una ACL especifica a qué usuarios o procesos del sistema se les concede acceso a los recursos, así como qué operaciones están permitidas en determinados recursos.
Activo IT	Es hardware, sistemas de software o información que tienen valor para una organización
Activo OT	Es hardware y software para controlar equipos industriales.
Algoritmo	Un algoritmo informático es un conjunto de instrucciones definidas, ordenadas y acotadas para resolver un problema, realizar un cálculo o desarrollar una tarea. Es decir, un algoritmo es un procedimiento paso a paso para conseguir un fin.
Altos Privilegios	Una cuenta privilegiada es una cuenta de usuario en una organización que tiene privilegios elevados, es decir, permisos y derechos de acceso a sistemas, bases de datos, aplicaciones e infraestructura de red de la organización que la mayoría del resto de usuarios no tiene.
Backup	Una copia de seguridad, respaldo, copia de respaldo o copia de reserva en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
Ciberseguridad	Es el conjunto de recursos, políticas, controles de seguridad, directrices, métodos de gestión del riesgo, formación, buenas prácticas y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

Cifrado	En criptografía, el cifrado es el proceso de codificación de la información. Este proceso convierte la representación original de la información, conocida como texto plano, en una forma alternativa conocida como texto cifrado.
Cloud Computing	La computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo o simplemente «la nube», es el uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software.
Controles criptográficos	La criptografía es una práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas. Los controles criptográficos se pueden utilizar como un control añadido que proporciona confidencialidad, autenticidad, no repudio y autenticación.
Data Center	Un centro de almacenaje de datos y que provee servicios de negocio que entrega de forma segura aplicaciones y datos a usuarios remotos a través de Internet.
Dispositivos IoT	Un dispositivo IoT consiste en un objeto al que se le ha dotado de conexión a Internet y cierta inteligencia, sobre el que se pueden medir parámetros físicos o actuar remotamente. Recopila datos de su entorno, de las entradas de los usuarios o de los patrones de uso y comunica los datos a través de Internet hacia y desde su aplicación de IoT.
DMZ	En seguridad informática, una zona desmilitarizada o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.
EDR	Siglas de Endpoint Detection and Response, también conocida como detección y respuesta de amenazas de puntos finales, es una tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas.
Ethical Hacking	Es la práctica de realizar evaluaciones de seguridad utilizando las mismas técnicas que emplean los hackers, pero con la debida aprobación y autorización de la organización a la que se está hackeando.
Evento	Un evento es algo sospechoso que sucede en un sistema o red y que puede ser una señal de una posible amenaza a la seguridad o un comportamiento inusual.

Firewall - FW	Es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad
HTTPS	El Protocolo seguro de transferencia de hipertexto es un protocolo de aplicación basado en el protocolo http, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de http.
Información sensible	Son un tipo de datos personales que, por su relevancia e importancia para la privacidad, deben ser tratados y almacenados con mayor cuidado y requisitos más estrictos. La información sensible es la que afecta a la intimidad del titular o aquella cuyo uso indebido puede generar discriminación.
ISO 27001	Estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la metodología del Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).
Lineamiento	Los lineamientos describen las etapas, fases, pautas y formatos necesarios para desarrollar actividades o tareas específicas.
Log	En informática, se usa el término registro, log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular. De esta forma constituye una evidencia del comportamiento del sistema.
MFA	La autenticación de múltiples factores, más comúnmente conocida por sus siglas en inglés MFA, es un método de control de acceso informático en el que a un usuario se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser.
NIST CSF	NIST Cybersecurity Framework es un conjunto de pautas para mitigar los riesgos de ciberseguridad organizacional, publicado por el Instituto Nacional de Estándares y Tecnología de EE. UU. basado en estándares, pautas y prácticas existentes.

On premise	En un entorno on-premise, los recursos informáticos (servidores, almacenamiento, redes, etc.) están ubicados físicamente en las instalaciones de la organización, es decir, la empresa tiene su infraestructura en su propio centro de datos o en una sala de servidores dentro de sus instalaciones.
One Drive	OneDrive es el servicio en la nube de Microsoft que te conecta a todos tus archivos. Te permite almacenar y proteger tus archivos, compartirlos con otros usuarios y acceder a ellos desde cualquier lugar.
OWASP	Es una comunidad global de voluntarios y expertos en seguridad informática. Su misión es mejorar la seguridad de las aplicaciones web mediante la concienciación, la educación y la promoción de las mejores prácticas de seguridad.
Parche de seguridad	Un parche de seguridad o actualización de seguridad es una pieza de software que corrige una o más vulnerabilidades de un software. Los fabricantes de software suelen corregir las vulnerabilidades que van descubriendo mediante la publicación de actualizaciones o nuevas versiones.
Plataforma	En informática, plataforma es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible.
Protocolos	En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información.
Puertos	En informática, los puertos son el punto de acoplamiento central del flujo de información desde un programa o Internet a un dispositivo u otro equipo de la red y viceversa.
Puntos finales	Normalmente se refiere a los dispositivos que utilizamos a diario como ordenadores de escritorio, portátiles, servidores, teléfonos inteligentes, tablets o dispositivos de Internet de las cosas (IoT)
Root	El usuario root en GNU/Linux es el usuario que tiene acceso administrativo al sistema. Los usuarios normales no tienen este acceso por razones de seguridad.
Seguridad perimetral	Se considera seguridad perimetral a todo tipo de herramientas y técnicas de protección informática que tienen como propósito defender la tecnología de la información de

	una empresa; relacionada con la red interna y toda la prolongación que forma parte de su entorno.
SFTP	SFTP es la abreviatura de Secure File Transfer Protocol (Protocolo de transferencia segura de archivos). Este protocolo permite transferir datos cifrados entre tu ordenador local y el espacio web del que dispones en tu hosting.
Sistemas de Control Industrial - ICS	Los sistemas de Control industrial o ICS (por sus siglas en inglés: industrial control systems) son de suma importancia para los procesos de fabricación, porque permiten automatizar flujos de trabajo y obtener, en tiempo real, datos exactos y fiables de cada uno de ellos para monitorear la producción de forma eficiente.
SLA / ANS	"Service Level Agreement" o "Acuerdo de Nivel de Servicio". Es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a hacerlo bajo determinadas condiciones y con unas prestaciones mínimas.
SOCLess	Modelo descentralizado de un Centro de Operaciones en Ciberseguridad, con un enfoque más proactivo basado en Inteligencia y cacería de amenazas.
Software Antimalware	El antimalware es un tipo de software diseñado para detectar, prevenir y eliminar software malicioso de los ordenadores.
SSH	SSH es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.
SSL	Secure Sockets Layer son protocolos criptográficos, que proporcionan comunicaciones seguras por una red, comúnmente Internet.
VPN	Una VPN o red privada virtual crea una conexión de red privada entre dispositivos a través de Internet. Las VPN se utilizan para transmitir datos de forma segura y anónima a través de redes públicas.
Vulnerabilidad	En informática, una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.

WAF	Un firewall de aplicaciones web (WAF) es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web. Se diferencia de un firewall normal en que puede filtrar el contenido de aplicaciones web específicas, mientras que un firewall de red protege el tráfico entre los servidores.

6. RESPONSABILIDADES

La Política de Ciberseguridad es de aplicación obligatoria para todo el personal de Triple A E.S.P, cualquiera sea su situación contractual y el nivel de las tareas que desempeñe.

Las directivas institucionales aprueban esta política y son responsables de la autorización de sus modificaciones.

- **Alta Gerencia**
  - ✓ Velar por que la seguridad informática y ciberseguridad se gestione adecuadamente en Triple A E.S.P.
  - ✓ Asignar los recursos necesarios que garanticen la adecuada gestión de la seguridad informática y ciberseguridad.

- **Gerencias**
  - ✓ Garantizar que el personal que laboran bajo su dirección proteja la información de acuerdo con las normas establecidas por la compañía.
  - ✓ Aprobar / revisar periódicamente los accesos de los colaboradores a su cargo.
  - ✓ Determinar para sus colaboradores los niveles de acceso a la información.

- **Oficial de Ciberseguridad**
  - ✓ Documentar y evaluar los riesgos identificados seguridad informática y ciberseguridad y apoyar en las medidas correctivas.
  - ✓ Mantener actualizada a la alta gerencia con los temas relacionados seguridad informática y ciberseguridad que se requieran.
  - ✓ Ejecutar el programa de concientización en temas de Ciberseguridad dirigido a los colaboradores de Triple A E.S.P.
  - ✓ Definir las políticas y procedimientos relacionados a la Ciberseguridad y velar por el cumplimiento de estas.

- ✓ Garantizar la seguridad de los sistemas de información e Infraestructura TI/OT, a través de la supervisión continua de los controles implementados y seguimiento a los planes de acción definidos.
- ✓ Monitorear las plataformas de seguridad, y gestionar los incidentes de ciberseguridad.

- **Subgerencia de Sistemas**
  - ✓ Velar por que se apliquen los controles de seguridad en los sistemas de información, Infraestructuras IT/OT y en los proyectos de tecnología de información.
  - ✓ Convocar al Oficial de Ciberseguridad en los proyectos relacionados a la implementación, modificación de servicios, aplicaciones e infraestructura tecnológicas, de la operación y sistemas de control industrial.

- **Gerencia de Gestión Humana**
  - ✓ Notificar a todo el personal que se vincule contractualmente con Triple A E.S.P, de las obligaciones respecto al cumplimiento de la Política de seguridad informática y Ciberseguridad y de todos los estándares, procesos, procedimientos, prácticas y guías diseñadas.
  - ✓ Incluir en la inducción de nuevos colaboradores la capacitación de seguridad informática y Ciberseguridad.
  - ✓ Definir las acciones disciplinarias en caso de incumplimiento de las políticas de seguridad informática y ciberseguridad.
  - ✓ Definir, notificar y hacer cumplir los compromisos de confidencialidad de la información.

- **Colaboradores**
  - ✓ Conocer, comprender y cumplir la política de seguridad informática y ciberseguridad de Triple A E.S.P.
  - ✓ Mantener la confidencialidad de sus credenciales de acceso a los sistemas de información, servicios y herramientas corporativas a las cual tienen acceso.
  - ✓ Notificar incidentes y riesgos de seguridad informática y ciberseguridad a las áreas encargadas.

- **Terceros y Proveedores de Servicios**
  - ✓ Conocer y cumplir las políticas de seguridad informática y ciberseguridad.
  - ✓ Cumplir con las cláusulas de Ciberseguridad incluidas en los contratos para asegurar seguridad a lo largo de todo el ciclo de vida del servicio o producto suministrado.

- **Área Legal**
  - ✓ Establecer un modelo de contrato para los servicios tercerizados y/o la contratación de personal, que incluyan cláusulas que obliguen a los proveedores y colaboradores a que sus servicios no afecten la confidencialidad, integridad y disponibilidad de la información.

7. POLÍTICA

El área de Ciberseguridad diseña, evalúa e implementa procedimientos de control adecuados que permitan administrar de forma segura los activos de información soportados en plataformas tecnológicas, tomando como referencia las buenas prácticas establecidas en estándares como ISO 27001 y NIST CSF.

8. MODELO DE APLICACIÓN DE LA POLITICA

8.1. GESTION Y ORGANIZACIÓN DE LA CIBERSEGURIDAD

8.1.1. Política de Organización de la Ciberseguridad

Dentro de la estructura de la organización se cuenta con un oficial de Ciberseguridad que depende de la Subgerencia de Sistemas.

El Oficial de Ciberseguridad es responsable de definir, liderar y monitorear la estrategia de Ciberseguridad en Triple A E.S.P, gestionando un plan para la implementación de estrategias que lleven a la organización a un nivel de madurez cada vez mayor y que garanticen la adherencia a la Ciberseguridad como parte de la cultura organizacional, acorde a la gestión y respuesta de áreas involucradas, partes interesadas y a la asignación de recursos necesarios.

8.1.2. Política de gestión de riesgos Cibernéticos

El área de ciberseguridad es responsable de elaborar y gestionar la matriz de riesgos cibernético teniendo como base el inventario de activos, servicios y recursos internos o externos para las operaciones de IT y OT. Dentro de las actividades a tener en cuenta se tienen:

- El nivel y la tolerancia del riesgo debe ser calculado acorde a los lineamientos definidos en la gestión de riesgo corporativo.
- Gestionar la implementación de controles con los responsables, para mitigar los posibles riesgos inherentes y calcular el riesgo residual.
- Monitorear y hacer seguimiento a la implementación de los controles comprometidos por cada responsable.
- Presentar informe anual del comportamiento de los riesgos con su mapa de calor actualizado y los resultados de la gestión realizada.

8.1.3. Política de Gestión de incidentes de Ciberseguridad

Un incidente de seguridad informática es un evento o serie de eventos de seguridad no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la Ciberseguridad.

Los incidentes se gestionan a partir de una solución SOCLess a través de alertas reportadas por un servicio automatizado de procesamiento de eventos y detección de amenazas que facilitan la investigación y disminuyen los tiempos de respuesta.

Todo evento o incidente de seguridad debe ser comunicado oportunamente con el fin de tomar las acciones correctivas necesarias para su remediación, por lo tanto, se requiere:

- Contar con un medio y los canales corporativos establecidos para reporte formal de los eventos o incidentes de seguridad informática.

- Contar con un plan de respuesta ante incidentes de Ciberseguridad que incluya las fases de: planificación y preparación, detección y reporte, evaluación y decisiones, respuesta y lecciones aprendidas. Acorde a lo establecido en los documentos **Gestión de Incidentes de Seguridad (DI-SI-PO-10) y Tratamiento de incidentes de Seguridad (DI-SI-IT-5).**
- Definir el nivel riesgo corporativo acorde a lo establecido por el negocio.
- Contar con una priorización para su atención, según evaluación técnica de la criticidad de este.
- Dar una respuesta oportuna indicando acciones de remediación tomadas para contener el riesgo, plan de acción a seguir, actividades de erradicación, tiempo estimado para implementar, responsables y demás información relevante requerida.
- Todo evento o incidente de seguridad debe quedar registrado y contar con la respectiva documentación y medición.
- El plan de respuesta ante incidentes de Ciberseguridad debe ser socializado con los involucrados e interesados.

8.1.4. Política de gestión de vulnerabilidades

La identificación oportuna de vulnerabilidades es una de las principales actividades que desde la gestión de Ciberseguridad se ejecuta. Triple A E.S.P es consciente de la importancia y la criticidad de identificar de manera proactiva vulnerabilidades y/o brechas de seguridad en los activos IT/OT que puedan poner en riesgo la seguridad y operación del negocio.

La compañía cuenta con una línea base para la detección e identificación de vulnerabilidades:

- Servicio de procesamiento de eventos de seguridad y detección de amenazas.
- Detección y respuesta para Endpoints (EDR)
- Plataforma de seguridad perimetral (Firewall)
- Seguridad Perimetral para aplicaciones (WAF)
- Plan anual de pruebas de seguridad (Ethical Hacking, análisis de vulnerabilidades)
- Reportes de vulnerabilidades de seguridad que afectan tecnologías existentes.

El área de Ciberseguridad se compromete a:

- Monitorear alertas generadas en la consola de eventos de seguridad, solicitar la investigación de los eventos que se reportan y que afectan a la compañía representando un riesgo a la seguridad.
- Monitorear y hacer seguimiento periódico sobre la consola del EDR, para garantizar el uso de las versiones actualizadas permitidas y la cobertura total de los activos de TI definidos en el alcance según los inventarios actualizados.
- Hacer seguimiento a la definición de políticas de seguridad en el Firewall y su afinamiento periódico o si surge un cambio operativo o técnico que impacte en las reglas de seguridad perimetral.
- Realizar análisis de vulnerabilidades para la Infraestructura TI y equipos de usuario final, sujeto a los recursos definidos para esta actividad.
- Ejecutar pruebas de Ethical Hacking para los sistemas de información críticos del negocio y posterior a la primera prueba, se debe realizar un retest que evidencie el cierre de las brechas identificadas o la implementación de controles alternos para mitigarlas.
- Seguimiento al cierre de las desviaciones identificadas en las pruebas de seguridad realizadas anualmente.

8.2 CONTROLES A PERSONAS

8.2.1. Política de Ciberseguridad del recurso humano

- **Antes de asumir el empleo**

  - ✓ La Gerencia de Gestión Humana debe verificar hoja de vida, antecedentes judiciales, certificaciones laborales y registros académicos del solicitante.

  - ✓ Los acuerdos contractuales con los colaboradores deben contemplar cláusulas relacionadas con Ciberseguridad, derechos de autor, acuerdos de confidencialidad y no divulgación.

- **Durante la ejecución del empleo**

  - ✓ Todo colaborador debe recibir entrenamiento en seguridad informática y ciberseguridad además de conocer y cumplir las políticas, procedimientos y estándares, según sea relevante para el desempeño de sus funciones.

- ✓ El área de Ciberseguridad debe generar un programa anual de toma de conciencia con temas relacionados en seguridad informática y ciberseguridad y evaluar el nivel de adherencia de este.

- ✓ La Gerencia de Gestión Humana, cuenta con un proceso disciplinario para emprender acciones contra empleados que hayan cometido alguna violación a las políticas institucionales, donde se incluye, la seguridad informática y ciberseguridad.

- ✓ Es responsabilidad de todos los empleados informar acerca de cualquier evento, incidente o vulnerabilidad de seguridad detectada y cualquier violación que se evidencie sobre la seguridad informática y ciberseguridad.

- ✓ Es obligación de cada empleado, cumplir con los acuerdos de confidencialidad pactados y toda la normativa relacionada con Ciberseguridad y derechos de autor.

- **Terminación y/o cambio de cargo**

- ✓ Cuando un empleado cambia de cargo, inicia licencias, vacaciones o finaliza su relación laboral con la compañía, la Gerencia de Gestión Humana debe notificar al área de Sistemas para gestionar las novedades y bajas respectivas de manera oportuna, con el fin de realizar los ajustes o retiros pertinentes de los roles o perfiles que el empleado tenga asignado, según sea el caso.

- ✓ El jefe directo debe notificar a los proveedores externos con los cuales el excolaborador tenía contacto a nombre de la organización, para que estos conozcan que este ya no cuenta con autorización para actuar a nombre de la compañía.

8.3 GESTIÓN DE ACTIVOS

8.3.1 Política de gestión de activos IT/OT/Digitales

Son activos de TI/OT y digitales los recursos como sistemas de información, servidores, equipos de comunicaciones, seguridad perimetral, almacenamientos, librerías, computadores de escritorio, laptop, celulares, tablet o dispositivos para usuarios finales, equipos OT, Sistemas de Control Industrial (ICS), dispositivos IoT, aplicaciones digitales, entre otros necesarios para la operación del negocio y para que los colaboradores desempeñen las labores asignadas.

- El área de Infraestructura TI, aplicaciones y mesa de servicios de sistemas deben contar con inventarios completos y actualizados de los activos (hardware y software) que se encuentran bajo su custodia.
- El área de Operaciones del negocio debe contar con el inventario de tecnologías de operación (OT) y Sistemas de Control Industrial (ICS), actualizados, clasificados y priorizados según su criticidad.
- La Dirección de Innovación Digital debe contar con el inventario actualizado de soluciones digitales clasificadas y priorizadas según su criticidad.
- Todos los activos IT/OT/digitales deben tener un propietario asignado y deberá ser identificado y actualizado periódicamente.
- Cada responsable debe garantizar el manejo adecuado del activo cuando es eliminado, dado de baja o destruido.
- Los sistemas de información de terceros o externos deben estar dentro del catálogo de aplicaciones corporativas.
- Cada colaborador, socio, proveedor o tercero de Triple A E.SP. deberá responder por el uso adecuado de los activos de IT/OT/digital que estén asignados a su cargo.
- En caso de presentarse cualquier daño, pérdida o robo de los activos y que se encuentren por fuera de la cobertura de un seguro será responsabilidad del área a la cual fue asignado el activo.
- Los colaboradores, socios, proveedores, y terceros de Triple A E.S.P, deben devolver todos los activos de TI/OT de la compañía que se encuentren a su cargo (físicos y electrónicos), al terminar el empleo, contrato o acuerdo.

8.3.2. Política Directorio activo y uso de equipos de computo

- ✓ Todos los empleados que se conectan a la red deben contar con un usuario de dominio nombrado e identificable.
- ✓ Los usuarios deberán mantener sus activos de IT con controles de acceso, utilizando una contraseña segura, acorde a la política de contraseña vigente.
- ✓ Solo se subirán al directorio activo corporativo los equipos suministrados por Triple A E.S.P, no está permitido subir equipos de terceros, ni personales.
- ✓ Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina durante la noche.
- ✓ Los usuarios de los equipos de cómputo deberán seguir las buenas prácticas y principios éticos establecidos por Triple A E.S.P.
- ✓ La mesa de servicios de Sistemas debe contar con una herramienta de acceso remoto segura y licenciada para soporte y mantenimiento a equipos de usuarios finales.
- ✓ En caso de que se presente un hurto o robo, el empleado debe reportarlo de manera inmediata a la mesa de soporte IT, además de esto deberá efectuar la denuncia ante los entes pertinentes y entregarla al día hábil siguiente del evento.
- ✓ El uso correcto de los equipos de cómputo y su disponibilidad debe darse bajo los lineamientos definidos en el **Reglamento de seguridad y buen uso de los recursos informáticos (DI-SI-DC-1) y el Plan de mantenimiento de equipos de sistemas (DI-SI-DC-4)**

8.3.3 Política para manejo de medios de almacenamiento

La información clasificada como: Confidencial, Uso Interno o Restringida, debe ser tratada con base en lo siguiente:

- **Gestión de medios**
  - ✓ El área de Ciberseguridad socializara a los responsables de todas las áreas, sobre la no utilización de medios de almacenamiento externos (memorias USB, disco duro externo).
  - ✓ Los responsables de la información deberán solicitar autorización al superior responsable del área y al Oficial de ciberseguridad, para el uso de medios de almacenamiento externos.
  - ✓ El área de Infraestructura TI y la mesa de servicios de sistemas deberán borrar de manera segura la información de los medios de almacenamiento que estén bajo su custodia, basándose en el respectivo procedimiento, en el momento que se requiera.

- **Movimiento de medios físicos**
  - ✓ Usar transporte o servicios de mensajería confiable, en caso de requerir la transferencia de algún medio que contenga información vital para la compañía.
  - ✓ Realizar los procesos de envío, según lo establecido por la compañía y utilizando los servicios de mensajería autorizados.
  - ✓ Empacar el medio de manera tal, que proteja su contenido contra cualquier daño físico que pudiera presentarse durante su transporte. Utilizar cajas de cartón y protectores como icopor, plástico de burbujas, etc., para el caso de equipos de cómputo o servidores críticos, los objetos más delicados deben ser embalados con papel film industrial y/o huacales de madera de forma que se protejan contra golpes fuertes.

8.4 GESTIÓN DE ACCESOS

8.4.1 Política de control de accesos físico

- El área de Gestión Humana deberá otorgar una identificación al personal que requiere acceso a las instalaciones de Triple A E.S.P., autorizar su ingreso y conceder por parte de las áreas contratantes los privilegios necesarios para el acceso físico.
- El área seguridad física deberá contar con mecanismos de control de acceso físico para las áreas seguras o restringidas; tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que Triple A E.S.P considere pertinentes.
- Se deben analizar, validar y aprobar de manera previa, todas las solicitudes de acceso de proveedores o terceros a las áreas restringidas o que contengan información crítica para la empresa, adicionalmente, debe brindarse por parte del área responsable de la vista del tercero acompañamiento permanente durante su estancia en dichas áreas.
- El área de Infraestructura TI deberá registrar en una bitácora, el ingreso de los visitantes a las áreas restringidas de Sistemas de Triple A E.S.P.

- El área de Gestión Humana deberá bloquear y/o solicitar de manera inmediata la inactivación de los privilegios de acceso físico a las instalaciones de Triple A E.S.P tan pronto el jefe inmediato del colaborador reporte la desvinculación.

- Se deberá realizar la devolución del carnet institucional tan pronto el colaborador termine su vinculación con Triple A E.S.P.

8.4.2 Política de control de accesos lógico

Se debe contar con procedimientos formalmente definidos que cubran los siguientes puntos:

- El área de Gestión Humana es responsable de solicitar a la mesa de servicios de Sistemas la creación de accesos de los nuevos ingresos y el cese de los colaboradores.
- Los accesos a los sistemas de información deben ser de acuerdo con las funciones que desempeña el colaborador, tercero o proveedor de servicio, siguiendo el principio del mínimo privilegio.
- Se debe contar con la matriz de roles y perfiles definidos por cada responsable de procesos y aprobados por la organización.
- El área de mesa de servicios de Sistemas asigna a los usuarios los accesos y privilegios necesarios a las aplicaciones y plataformas según lo solicite Gestión Humana (nuevos ingresos) y/o el jefe directo del cargo para cambios internos.
- Las cuentas de los terceros o proveedores de servicios que requieran acceso a los sistemas de información deben ser solicitadas por el Gerente o Jefe responsable del servicio.
- Todos los accesos deben contar con un segundo factor de autenticación (MFA), en caso de no poderse implementar debe quedar documentada la respectiva justificación y aprobación de la Gerencia responsable.
- Cumplir con lo estipulado en el documento **Política de Administración y Gestión de Accesos a los Sistemas de Información (DI-SI-POL-1)**
- La gestión de Ciberseguridad realiza el monitoreo de todos los accesos lógicos, trimestralmente.
- Se deshabilitará el acceso de las aplicaciones y servicios internos a aquellas cuentas que no tengan actividad más de 90 días.

8.4.3 Política de contraseña segura

Esta política de contraseñas se aplica a los sistemas de información, servicios digitales o plataformas de Triple A E.S.P:

- La longitud de la contraseña debe ser como mínimo de 14 caracteres
- La contraseña debe ser alfanumérica, mayúsculas y minúsculas, y un carácter especial, por ejemplo: !# $ %

- Tiempo de vigencia de la contraseña 30 días.
- El número máximo de intentos fallidos será de 3 antes de que se bloquee.

- Sin rehúso.

Además de la política de contraseñas aplicada, el usuario debe seguir las siguientes recomendaciones:

- La contraseña no debe contener el nombre o apellido del usuario, fecha de nacimiento, ni el número de documento de identidad de este o del grupo familiar.
- No colocar nombres de mascotas, ni espacios en blanco.
- Se consideran contraseñas no válidas las que tengan palabras relacionadas al negocio, área, cargo y/o año o consecutivo de números, como: Acueducto2024, Acueducto12345, Alcantarillado5678, TripleA01012022, Sistemas123456, etc.
- No utilizar en la contraseña, palabras o nombres comunes que puedan figurar en diccionarios.
- No almacenar las contraseñas de manera física.
- No compartir la contraseña bajo ningún concepto con otras personas, aunque sean de su mismo entorno.

8.4.4 Política de cuentas con Altos Privilegios

La solicitud de una cuenta de usuario privilegiado debe ser autorizada formalmente por el responsable del área de Sistemas y acompañada de una justificación de necesidad de uso. Debe cumplir con lo establecido en el procedimiento para altas, bajas y modificaciones de usuarios con acceso privilegiado.

- Deben cumplir con la política de acceso lógico y contraseña segura.
- Los accesos realizados con cuentas de usuario privilegiados deben ser registrados y controlados periódicamente.
- Una cuenta de usuario privilegiado sólo podrá ser utilizada en la actividad de administración o configuración del sistema para la cual se requieren dichos privilegios. No podrá ser utilizada en actividades rutinarias para la que exista un perfil de menores privilegios que lo permita.
- Las cuentas de usuario privilegiado tipo ADMIN, ROOT o similares, definidas por defecto, en sistemas y componentes, no pueden ser usadas. Siempre que sea posible las mismas deben ser eliminadas o deshabilitadas, además de modificadas sus contraseñas por omisión. Se debe contar con un mecanismo de recuperación de acceso privilegiado, dicho mecanismo debe mantener las garantías de reserva.
- El acceso privilegiado debe realizarse desde dispositivos debidamente fortalecidos para tal fin.

8.5 ACCESO REMOTO

8.5.1 Política de acceso remoto por teletrabajo

El área de Ciberseguridad realizará campañas de sensibilización dentro del plan anual de toma de conciencia, en donde se socialicen los riesgos del teletrabajo o uso de equipos no corporativos y las acciones que se deben ejecutar para mitigarlos. Se deben tener en cuenta los siguientes lineamientos:

- El jefe inmediato, interventor del contrato o líder del proceso debe definir la necesidad de acceso remoto a los sistemas y recursos internos de la organización y la información sobre la cual se requiere acceso.
- Para funcionarios con laptops y/o que realizan teletrabajo, se debe entregar instalada la VPN o la herramienta de seguridad establecida para el acceso remoto.
- No se permite el uso de equipos PERSONALES dentro de la compañía conectados o no a la red; salvo autorización del Gerente de cada área.

Si al empleado no se le puede asignar por algún motivo **justificado** un equipo de cómputo corporativo, la decisión de uso de equipo personal será aprobada por el comité de Ciberseguridad, para estos casos la mesa de servicios de sistemas deberá garantizar la implementación de controles de seguridad sobre los respectivos equipos de cómputo para minimizar riesgos, siendo los responsables de:

- Realizar la instalación de los controles de ciberseguridad vigentes.
- Validar los siguientes aspectos:
  - ✓ Sistema operativo licenciado, con soporte activo por parte del fabricante y con los últimos parches de seguridad instalados.
  - ✓ Verificar la existencia de cuenta de usuario de uso exclusivo para el funcionario qué utilice el equipo de cómputo.
- Cuando al funcionario ya se le asigné su equipo corporativo, la mesa de servicios de sistemas debe retirar todas las herramientas corporativas de seguridad del equipo personal que venía utilizando.

8.5.2 Política de acceso remoto para Terceros

En el caso de terceros que por la naturaleza del contrato o servicio que prestan requieran acceso remoto a los recursos tecnológicos de la organización, el interventor del contrato o líder del área a la que prestan servicios deberá garantizar que cuenten con los requerimientos mínimos de seguridad sobre los respectivos equipos de cómputo a utilizar, los cuales deben ser validados por la mesa de servicios de sistemas y avalados por Ciberseguridad, certificando que se cuenta con lo siguiente:

- Software antimalware licenciado y actualizado en su versión más reciente.
- Sistema operativo licenciado, con soporte activo por parte del fabricante y con los últimos parches de seguridad instalados.
- Existencia de cuentas de usuario nombradas y de uso exclusivo para el funcionario que utilice el equipo de cómputo.
- Instalación la herramienta de seguridad establecida para acceder a los recursos corporativos de Triple A E.S.P.
- Cumplir con lo establecido en el documento, **Reglamento de conexión de contratistas a la red Triple A (DI-SI-DC-2)**.

8.6 CONTROLES CRIPTOGRAFICOS

8.6.1 Política de Controles Criptográficos

Se debe cifrar toda información sensible, **clasificada como confidencial** para resguardar su privacidad e integridad. Se requiere utilizar controles criptográficos en los siguientes casos:

- Protección de claves de acceso a sistemas de información, bases de datos, documentos electrónicos, datos y servicios.
- Para la transmisión fuera de la organización de información que por su clasificación se considere reservada o confidencial.
- Para la protección de la información a resguardar, como resultado de la evaluación del riesgo realizada por el propietario de la información o lo establezca la Subgerencia de Cumplimiento y/o el Oficial de Ciberseguridad.
- Se utilizan técnicas criptográficas para autenticar a los usuarios o entidades externas que requieren hacer uso de los sistemas de información, plataformas o servicios de Triple A.
- Evitar el uso de sistemas de cifrado obsoletos. Se deben aplicar los algoritmos y sistemas de cifrado conocidos y evaluados ampliamente. Se recomienda el uso de sistemas de cifrado asimétrico en detrimento de los sistemas de cifrado simétrico.
- Se debe cumplir lo estipulado en la sección: **"Requerimientos Protocolos / Puertos Seguros / Otras técnicas de seguridad" que hace parte del Lineamiento General de Ciberseguridad.**
- Se deben utilizar protocolos criptográficos actualizados con el fin de garantizar la confidencialidad en el acceso a los sistemas, tanto internos como externos, Se consideran los siguientes protocolos:
  - ✓ SFTP para la transferencia segura de ficheros
  - ✓ HTTPS para la transferencia segura de datos en servicios web críticos (pagos online, descarga de información sensible, etc.).

8.7 SEGURIDAD FÍSICA

8.7.1 Política de Áreas Seguras

- Toda área o equipo informático, debe cumplir con todas las políticas funcionales y procedimientos de seguridad física y protección ambiental, con el fin de evitar el acceso por personas no autorizadas, daño e interferencia a los recursos e Infraestructura TI.
- Los colaboradores deben ingresar a las sedes de Triple A E.S.P con la identificación que se les ha asignado.
- En caso las identificaciones asignadas sean extraviadas o robadas debe ser comunicado a la Gerencia de Gestión Humana previo denuncio ante las autoridades respectivas.

- El Data Center debe contar con medidas de protección de los equipos frente a amenazas como incendios, problemas de energía, inundación, robo, entre otros.
- El ingreso al Data Center debe ser restringido y autorizado por el área encargada.

8.7.2 Política de escritorio y pantalla limpios

- No tener información restringida o confidencial almacenada en el escritorio (pantalla) del equipo.
- Se deben considerar las siguientes medidas de seguridad para la información restringida y/o confidencial en formato físico y/o digital:
  - ✓ Almacenarla en lugares cerrados (mobiliario, cajones) y bajo llave, cuando se ausente de su lugar de trabajo por un largo periodo de tiempo.
  - ✓ Evitar exponer información restringida, confidencial o de uso interno en los módulos de trabajo.

  - ✓ Todo documento debe ser recogido de la zona de impresión o eliminar la información expuesta.
  - ✓ Al retirarse o finalizar la jornada laboral, los documentos físicos y dispositivo removible que contenga información restringida y/o confidencial debe guardarse en un lugar seguro y bajo llave.

- ✓ Cumplir con demás requisitos relacionados acorde a lo establecido en el documento, **Reglamento de seguridad y buen uso de los recursos informáticos (DI-SI-DC-1).**

8.8 SEGURIDAD DE LOS TERCEROS

8.8.2 Política de Ciberseguridad para la relación con proveedores

A continuación, se reúne las Políticas de Seguridad que deben cumplir los proveedores que tengan acceso a la información, intercambien, procesen, almacenen, modifiquen o creen nueva información confidencial, o los que utilicen sus equipos de cómputo en la red de Triple A E.S.P.:

- Todo proveedor y/o tercero que tenga acceso a los activos de información y preste servicios a Triple A E.S.P, debe contar con políticas, normas y estándares de ciberseguridad al interior de su organización; las cuales deben desarrollarse y mantenerse actualizadas acorde con los riesgos a los que se ve enfrentada su organización y capacitar periódicamente su personal en temas de seguridad informática y ciberseguridad.
- Informar cualquier fuga, pérdida o alteración de la información que sea propiedad de Triple A E.S.P y la correspondiente medida de mitigación.
- Todo proveedor que esté relacionado contractualmente con Triple A E.S.P, debe otorgar a este último el derecho de auditar la seguridad de los procesos y controles implementados que se encuentren relacionados en el respectivo contrato o servicio.
- Se deberán generar acuerdos de confidencialidad, acuerdos de niveles de servicio y acuerdos de intercambio de información (cuando aplique).
- En los contratos con terceros y proveedores de servicios se debe incluir la cláusula corporativa de ciberseguridad.
- Todo proveedor que se conecte o requiera conectar cualquier equipo de cómputo o dispositivo electrónico a la red interna de Triple A E.S.P, debe cumplir los siguientes requerimientos:

  - ✓ Software antimalware licenciado y actualizado en su versión más reciente.
  - ✓ Sistema operativo licenciado, con soporte activo por parte del fabricante y con los últimos parches de seguridad instalados.
  - ✓ Existencia de cuentas de usuario nombradas y de uso exclusivo para el funcionario que utilice el equipo de cómputo.

- ✓ Cumplir con demás requerimientos relacionados según lo indicado en el documento, **Reglamento de conexión de contratistas a la red Triple A (DI-SI-DC-2)**

- El área de Infraestructura TI debe disponer de un segmento de red exclusivo para Terceros.
- Todos los terceros deben cumplir lo estipulado en la Política de Seguridad Informática de Triple A E.S.P., el incumplimiento de esta da lugar a revisiones por parte del interventor responsable con el fin de reevaluar la continuidad del contrato o servicio que se tenga establecido.

8.9 SEGURIDAD DE LAS OPERACIONES

8.9.1 Política de restricciones a las instalaciones y uso del software

- Todo software que se instale sobre los dispositivos de Triple A E.S.P. debe estar relacionados en el inventario de aplicaciones corporativas previamente aprobado por la Subgerencia de Sistemas.
- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor. La mesa de servicios de sistemas debe desinstalar cualquier software ilegal y reportarlo para su respectiva investigación, en caso de ser un software malicioso o que comprometa la seguridad debe ser notificado al área de Ciberseguridad.
- La mesa de servicios de sistemas debe mantener una base de datos actualizada que contenga un inventario de software autorizado para su uso e instalación y acorde a las necesidades de cada área.

8.9.2 Política de Cloud Computing (nube)

- La adquisición de servicios en la nube como Infraestructura como servicio (IAAS), software como servicio (SAAS) y plataforma como servicio (PAAS) debe contar con certificaciones como: CSA, ISO27001, 27701, 27018, 27032, ISO22301, SOC 2, entre otras que se requieran y así mismo deben evidenciarlo cuando sea solicitado.
- Asimismo, la Infraestructura TI debe cumplir con los controles de seguridad descritos en las diferentes secciones de esta política y lo definido en el **Lineamiento de seguridad para servicios Cloud.**

8.9.3 Política de Hardening

- Los lineamientos para el hardening y su actualización son avalados por el área de Ciberseguridad.
- Aplica para los activos de IT y bases de datos que soportan los Sistemas de información o procesos de negocio críticos, ya sea en ambientes on premise o cloud.

- La ejecución de las actividades de hardening son responsabilidad del área de Infraestructura TI y se debe ejecutar sobre la infraestructura y bases de datos críticas existentes y en cada nueva implementación de servidores o base de datos.
- El área de Ciberseguridad debe monitorear el cumplimiento de hardening, por lo menos una vez al año.
- En caso de requerirse excepciones para un servidor en particular, estas son revisadas y aprobadas por el Oficial de Ciberseguridad, la Jefatura de Infraestructura TI y la Subgerencia de Sistemas.

8.9.4 Política de protección contra software malicioso

- Los equipos de cómputo, portátiles y servidores conectados a la red deben contar con el EDR corporativo licenciado y en su versión actualizada permitida.
- El EDR corporativo debe mantenerse en la versión más reciente permitida.
- Se deberá borrar el correo spam, cadenas y cualquier otro correo recibido con estas características. No se debe hacer reenvío de estos.
- Cuando se sospeche de una infección o cuando el EDR detecte una, reportar inmediatamente a la mesa de servicios de Sistemas para la revisión del caso
- La mesa de servicios de sistemas es responsable de la instalación del EDR corporativo en los equipos de usuarios finales, desinstalando cualquier otro software antivirus o antimalware no oficial para Triple A E.S.P.
- El área de Infraestructura TI es responsable de la instalación del EDR corporativo en los servidores, desinstalando cualquier otro software antivirus o antimalware no oficial para Triple A E.S.P.
- Los equipos de cómputo y portátiles de proveedores y/o terceros que requieran conectarse a la red interna, deben contar con un antimalware de su empresa y cumplir con los lineamientos de seguridad establecidos por Triple A E.S

8.9.5 Política de Respaldos de Información

- Las políticas de respaldos son definidas por el responsable funcional, Infraestructura TI y aplicaciones, estas deben ser diseñadas de acuerdo con la criticidad y uso de la información que se está respaldando.
- Se deben mantener actualizadas, inventariadas e identificadas las políticas de copias de respaldo de los sistemas de información corporativos, la actualización se debe realizar al menos una vez al año.
- Para los sistemas y servicios críticos se debe contar mínimo con:
  - ✓ 1 copia de respaldo externa al lugar donde se encuentra la aplicación, servidor o información. (Sitio alterno)
  - ✓ 1 copia de respaldo externa a las instalaciones de Triple A E.S.P. (Sitio Externo)
- El área de Infraestructura TI debe monitorear la ejecución de las copias de seguridad, así como liderar las pruebas periódicas de restauración para los respaldos críticos, acorde a un plan de pruebas definido anualmente.
- Se debe contar con soluciones de respaldo (On premise o cloud) que garanticen la disponibilidad de toda la información y del software crítico de Triple A E.S.P.
- Como complemento se debe seguir lo establecido en el documento **Controles de copias de seguridad logs y restauración (DI-SI-PO-2).**
- Los colaboradores deben almacenar la información laboral en el espacio de OneDrive asignado. No se respalda información alojada localmente en los equipos de cómputo.
- La información personal no será respaldada, ni recuperada por tanto no se debe guardar en los equipos de cómputo, ni en las nubes corporativas.

8.9.6 Política de gestión parches

La gestión de parches es una de las prácticas más importantes como medida de seguridad; si los parches no se despliegan lo suficientemente pronto, una plataforma de IT podría verse seriamente comprometida.

Se debe cumplir con los siguientes aspectos:

- Infraestructura TI y el área de Operación deben contar con un plan para ejecutar todas las actualizaciones críticas y de seguridad dispuestas por los fabricantes de las tecnologías IT/OT.
- Infraestructura TI y el área de Operación debe contar con un plan de trabajo para la ejecución de los ciclos de actualizaciones o parchados, los informes de la ejecución que incluyan tratamiento de riesgos, excepciones justificadas y controles compensatorios para estas.

- El negocio debe permitir los espacios requeridos para ejecutar las ventanas de mantenimiento, definiéndose en conjunto con TI un horario y días fijos semanalmente, para solución de casos críticos entre los que se listan la ejecución de las actualizaciones y parchados.
- Los planes de trabajo para la ejecución de parchados deben pasar por el comité de gestión de cambios quienes evalúan el cada caso y se deja evidencia de su aprobación o no en la respectiva acta.
- La mesa de servicios de sistemas debe ejecutar todas las actualizaciones críticas y de seguridad dispuestas por los fabricantes de acuerdo con el sistema operativo y/o software de usuario final.
- La ejecución de parchados se debe realizar como mínimo dos veces al año, por lo tanto, se debe contar con un plan por semestre. Salvo se identifique una vulnerabilidad crítica la cual se debe parchar en el menor tiempo posible.

8.9.7 Política de Monitoreo TI

El área de infraestructura TI es responsable de monitorear el rendimiento y disponibilidad de las tecnologías más críticas para la operación, se debe tener en cuenta:

- Identificar los activos a ser monitoreados y su impacto sobre otros activos o servicios.
- Se deben monitorear las BD, Servidores, backups, de las aplicaciones de misión crítica. Clasificarlos según su criticidad y los elementos que los componen (servicio, aplicación, base de datos, sistema operativo, máquina, conectividad)
- Definir parámetros o umbrales de operación “normales”
- Categorizar las alertas
- Identificar un responsable encargado de dar solución oportuna
- Definir los niveles de escalamiento y métodos de comunicación de las alertas.
- Contar con herramientas de monitoreo con gestión centralizada.
- El monitoreo se ejecuta acorde a lo indicado en el documento **Gestión de Capacidad (DI-SI-PO-4)**

8.9.8. Política de registros de auditoría

En la medida de lo posible, se deben registrar las actividades del usuario, errores, trazabilidad, eventos de seguridad, cambios en la configuración u otros que se presenten sobre los diferentes sistemas informáticos (aplicaciones, bases de datos, servidores, componentes de red y de seguridad), almacenando como mínimo los siguientes datos:

- Identificación del usuario.
- Actividades y registros de transacciones ejecutadas en el sistema.
- Fecha y hora de ingreso y salida del sistema u ocurrencia del evento.
- Identificación del dispositivo.
- Identificación del elemento donde se realiza la acción (archivos, bases de datos, máquina virtual, fichero, componente de hardware).
- Ubicación del dispositivo desde donde ingresa al sistema, si es posible.

Se requiere contar con los registros requeridos para tener trazabilidad sobre cada sistema informático (aplicaciones, Bases de datos, servidores, componentes de red y de seguridad) con el fin de poder efectuar un correcto monitoreo y tener trazabilidad de eventos.

Conservación y protección de logs
Los administradores de los diferentes sistemas informáticos no deben tener permiso para la eliminación o modificación de los registros de sus propias actividades.

Se deben implementar los mecanismos técnicos pertinentes para evitar los cambios no autorizados sobre la información del log.
Los responsables de cada sistema de información junto con Infraestructura TI deben definir los períodos de retención adecuados para cada log según la criticidad de este y la capacidad en recursos que se tengan para almacenarlos.

8.10 SEGURIDAD EN LAS COMUNICACIONES

8.10.1 Política de seguridad para los servicios de red

- Se debe salvaguardar la confidencialidad de la información restringida que pase a través de redes públicas empleando protocolos seguros de comunicación.
- Se debe contar con soluciones como Firewalls IPS/IDS, VPN, que gestionen y controlen el acceso remoto y de terceros a los recursos de Triple A E.S.P
- Establecer los roles y responsabilidades para la adecuada gestión de las redes y mantener controles de acceso y autenticación acorde al principio de mínimo privilegio y controles MFA.
- Realizar los monitoreos continuos con el fin de establecer las medidas preventivas y/o correctivas que se requieran sobre la Infraestructura de networking y detectar anomalías que puedan llegar a materializarse como un incidente de seguridad.
- Garantizar que la gestión de la red (interna o externa) se realice acorde a las buenas prácticas de seguridad, niveles de servicio y con el respectivo proceso para la atención de requerimientos sobre la red.
- Garantizar el envío de logs para el adecuado monitoreo de eventos de seguridad.

- Garantizar el uso de buenas prácticas: DMZ, ACL, SSL, SSH
- Separar lógicamente la red según el rol del usuario, tipo de dispositivos, consumo, criticidad de la información, tecnología, entre otras.
- Implementar la segmentación adecuada de las redes IT y OT para garantizar la seguridad de cada entorno.
- Mantener un diseño seguro de la red acorde a las buenas prácticas y a las necesidades del negocio.
- Establecer modelo de confianza cero para proporcionar una capa de seguridad adicional sobre los accesos internos y externos.

8.10.2 Política de Seguridad física de la red

- Garantizar el adecuado tendido de cableado estructurado conforme a los estándares.
- Garantizar la seguridad y control de accesos a los centros de cableado y Datacenter.

- Hacer revisiones periódicas a los centros de cableado y/o Datacenter.
- Certificar, asegurar y marquillar los puntos de red.

8.10.3 Política para Transferencia De Información

Establecer y normalizar la trasferencia de información con el objetivo de mantener la Ciberseguridad transferida dentro de la organización Triple A E.S.P y de igual manera con agentes externos y proveedores, mediante el uso adecuado de los recursos de comunicación como el correo electrónico, VPNs, carpetas y recursos compartidos, SFTP, etc.

- Acuerdos sobre transferencia de información:
  - ✓ Los procedimientos para asegurar trazabilidad y no repudio.
  - ✓ Los estándares técnicos mínimos para la transmisión de información.
  - ✓ Realizar controles de acceso a la información.
  - ✓ Establecer responsabilidades y obligaciones para evitar la pérdida de información en el momento de mantener y transmitir información.

- Mensajería Electrónica:
  - ✓ La protección de mensajes contra acceso no autorizado, modificación o denegación del servicio en cuanto a la trasferencia de información.
  - ✓ Asegurar el direccionamiento y trasporte correctos del mensaje.
  - ✓ La confiabilidad y disponibilidad del servicio.
  - ✓ Las condiciones legales, por ejemplo, los requisitos para firmas electrónicas.

- ✓ Autorizaciones previas al utilizar recursos de mensajería y redes sociales.

8.11 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

8.11.1 Política de desarrollo seguro

El área encargada del soporte y administración de aplicaciones son encargados de asegurar que los desarrollos internos y externos en los sistemas de información cumplan con los requisitos de seguridad definidos en la fase inicial del ciclo de desarrollo, con las buenas prácticas de seguridad sugeridas en OWASP para el desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido.

Los desarrolladores de los sistemas de información deben considerar las siguientes prácticas:

- **Principio del Menor Privilegio:** El área responsable debe conceder a las cuentas de usuario la menor cantidad de privilegios para llevar a cabo las actividades de desarrollo.
- **Defensa en Profundidad:** Se debe proveer a la aplicación de más de un mecanismo de defensa, con el fin de proteger los servidores de bases de datos, los cuales contienen información sensible.
- **Manejo Adecuado de Errores:** Se debe utilizar mecanismos de manejo de errores con el fin de publicar la menor información posible.
- **Pruebas de Seguridad y de Aceptación:** Todo nuevo desarrollo realizado deberá contemplar las pruebas de seguridad y de aceptación dependiendo del tipo de proyecto. Es necesario que se mitiguen los riesgos identificados antes del paso a producción o entrada en operación del software, lo anterior es evaluado por el comité de cambios.
- **Detección de vulnerabilidades:** Los desarrolladores deben tener la capacidad de evitar, encontrar y resolver las vulnerabilidades que se puedan presentar en la etapa de desarrollo de las aplicaciones. Se deben implementar análisis de vulnerabilidades a todos aquellos desarrollos que incluyan integraciones con software o hardware de terceros y subsanarse las vulnerabilidades antes del paso a producción o entrada en operación.

- **Lista de chequeo de seguridad:** Todo desarrollo efectuado, ya sea interno o contratado a través de un proveedor externo, debe cumplir con el "**Requerimientos de seguridad para desarrollo de software.**"

Para todo desarrollo interno o externo debe revisar y cumplir lo establecido en los documentos: **Metodología de Desarrollo (DI-SI-DC-13), Administración de Cambios (DI_SI-DC-11) y Gestión de Requerimientos (DI-SI-DC-12).**

8.12 GESTIÓN DE CONTINUIDAD TI

8.12.1 Política de recuperación de los servicios de TI ante desastres

Actuar diligentemente frente a una situación de crisis o emergencia, recuperando los servicios y la operación en el menor tiempo posible dentro de nuestras capacidades, resguardando prioritariamente la seguridad de las personas y la reputación corporativa, para esto Triple A E.S.P deberá:

- La definición de los sistemas críticos de Triple A E.S.P se da tomando como base el BIA elaborado por la subgerencia de cumplimiento.
- Las áreas de Infraestructura TI y Ciberseguridad deben implementar y mantener el Plan de Recuperación de los Servicios de TI ante Desastres (DRP) para los sistemas críticos del negocio, según los requisitos establecidos por el negocio.

- Cumplir con los requisitos legales y reglamentarios, propios de las actividades de Triple A E.S.P, la cual se compromete a proporcionar los recursos adecuados y el presupuesto necesario para cumplir con el Plan de Recuperación de los Servicios de TI ante Desastres acorde a las necesidades del negocio.
- El área de Infraestructura TI debe diseñar e implementar medidas de tratamiento y estrategias de continuidad tecnológica que mantengan el riesgo de las operaciones en los niveles mínimos definidos por el área de riesgo corporativa.
- Anualmente Infraestructura TI debe ejecutar un plan de pruebas de recuperación que incluya a proveedores, personal técnico y funcional la medición del tiempo de recuperación objetivo para el DRP y el punto de recuperación objetivo para los respaldos.

- El área de Ciberseguridad debe revisar y garantizar que exista un plan de Recuperación ante Desastres TI vigente, actualizado, validado y participar en el plan de pruebas anuales.

8.13 CUMPLIMIENTO

8.13.1 Política de cumplimiento Ciberseguridad

El área de Ciberseguridad el Cumplimiento de requisitos legales y contractuales para:

- Identificar los requisitos legales y contractuales aplicables a Triple A E.S.P en materia de Ciberseguridad con el fin de garantizar el cumplimiento de estos.
- Velar por la implementación de controles de seguridad en la infraestructura TI, OT y soluciones Digitales, para la protección de los datos del negocio.
- Definir los procedimientos necesarios que garanticen la adecuada protección y administración de los activos de información de Triple A E.S.P.
- Monitorear aleatoriamente el cumplimiento de los requisitos de seguridad informática por parte de los proveedores en la gestión de los servicios y contratos críticos de TI.

8.13.2 Política sobre Revisiones de Ciberseguridad

- Definir los planes de monitoreo anuales o después de cambios significativos para verificar el cumplimiento de las políticas, lineamientos y procedimientos de Ciberseguridad establecidos en la compañía.
- Evaluar el cumplimiento de las políticas, normas y procedimientos de seguridad informática y ciberseguridad por parte de los directores, gerentes, jefaturas, coordinadores y los empleados,
- Evaluar el grado de concientización de los empleados, midiendo también el nivel de adherencia de la compañía en esta materia.

El incumplimiento a la política de seguridad informática y Ciberseguridad traerá consigo, las consecuencias legales que apliquen a la normativa de Triple A E.S.P, incluyendo lo establecido en las normas que competen al Gobierno nacional en cuanto a ciberseguridad se refiere.
Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

9. REGISTROS

No aplica

10. ANEXOS

No aplica