CONTENIDO

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 20 de junio de 2024 -**Comité de Seguridad de la Información**

La presente Política de Seguridad y Privacidad de la Información entra en vigencia mediante el Liderazgo de la Dirección y la aprobación del Comité de Seguridad del **Grupo A3Sec**. Sus cambios serán definidos, implementados, aprobados, difundidos o comunicados cada vez que sean requeridos para su cumplimiento y reemplazados por una nueva política.

2. INTRODUCCIÓN

El **Grupo A3Sec** blinda entornos digitales evolucionando permanentemente, añadiendo su deber y compromiso de custodiar procesos e información privilegiada, con el objetivo de contrarrestar ataques cibernéticos de la industria y elevar el perfil de seguridad de sus clientes.

La Dirección del **Grupo A3Sec** reconoce el valor de los datos como un pilar importante en el logro de los objetivos estratégicos, calidad de servicio y la necesidad constante de brindar un tratamiento efectivo que asegure la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, por lo cual, ha establecido e implantado el Sistema de Gestión de Seguridad y Privacidad de la Información SGSPI, teniendo en cuenta las buenas prácticas y estándares de industria como ISO/IEC 27001:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad”, el Real Decreto por el que se regula el Esquema Nacional de Seguridad (ENS), RD 311/2022, de 3 de mayo, PCI DSS “Payment Card Industry Data Security Standard” incluyendo controles de distintos marcos de referencia (frameworks), circulares y decretos aplicables a nivel global. La presente Política Corporativa de Seguridad y Privacidad de la información regula el marco de responsabilidad, manejo de la información y el ciberespacio del objeto social alineados a la misión, visión, procesos, prestación de servicios, así como, asegura la continuidad de sus operaciones.

3. ÁMBITO Y ALCANCE

Datos de identificación corporativa	
Sede	**Razón Social**
España	A3Sec, Grupo S.L.
México	A3Sec, Sociedad Anónima de Capital Variable
Colombia	A3Sec SAS - Sociedad por acciones simplificada

La Política Corporativa de Seguridad y Privacidad de la Información se aplica a todo el Grupo A3sec, desde las instalaciones físicas, colaboradores, contratistas, proveedores, aliados, clientes, integrantes de diferentes comités, procesos físicos, digitales, inteligencia artificial o cualquier actor que tenga acceso de cualquier forma o motivo a la información.

También es aplicable a todo activo de información o del ciberespacio que el Grupo A3sec posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para la falta de protección de estos activos frente a la presente política.

La aplicación de esta política se realizará mediante un proceso sistemático, documentado y conocido por las partes interesadas incluyendo procesos estratégicos, misionales, apoyo y evaluación definidos en el Sistema de Gestión de Calidad SGC.

Así también, como apoyo a la Política Corporativa de Seguridad y Privacidad de la información se normalizará como alcance el Manual de Políticas SGSPI e información documentada que contiene cada dominio o control implementado por buenas prácticas de estándares, normas, frameworks y todos los controles de protección de seguridad, privacidad y ciberseguridad del Sistema de Gestión de Seguridad y Privacidad (SGSPI) del **Grupo A3sec**.

4. OBJETIVOS

La Política Corporativa de Seguridad y Privacidad de la información:

A. Establece la orientación de la Dirección y el Comité de Seguridad de la información hacia el Grupo A3sec, fija el marco de actuación necesario para proteger activos de información y ciberespacio, frente a amenazas internas, externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento y garantizar el adecuado tratamiento de la información registrada en sus bases de datos.

B. Promover la comprensión y las responsabilidades individuales para todas las partes interesadas, con el objeto de mantener acciones obligatorias de seguridad, privacidad y ciberseguridad para reducir brechas de riesgo.

C. Alinear y comunicar la estrategia de seguridad, privacidad y ciberseguridad para preservar la confianza de clientes y órganos de supervisión, fortaleciendo los servicios de monitoreo y gestión de eventos e incidentes de seguridad de la información y ciberseguridad así como en la nube (SOC-NOC) prestados a través del Centro de Seguridad y Vigilancia Digital - CSVD de A3SEC; Servicio de gestión de vulnerabilidades; Servicio de Vigilancia Digital y Cibernética.

D. Mantener un nivel aceptable de exposición de riesgo que permita mantener de manera sistémica la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información acorde con las necesidades de las partes interesadas.

5. MISIÓN DEL SGSPI

La misión del SGSPI del **Grupo A3sec**, es garantizar la protección de la información en cualquier estado contemplando las posibles amenazas del entorno empresarial, industria y ciberespacio, para mantener y preservar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los Servicios de Detección y Respuesta para el mantenimiento de la operación unificada de seguridad.

Estamos altamente comprometidos con la innovación, la mejora continua y la seguridad de la información como uno de los puntos principales en el modelo de gobierno. Para ello, A3Sec ha obtenido las certificaciones correspondientes a nivel global para establecer así un marco de calidad y seguridad de la información para construir servicios a las organizaciones con las que trabaja.

6. MARCO NORMATIVO

El presente marco normativo es adaptado acorde a la legislación de cada país donde opera el Grupo A3sec, para ampliar la información y solicitar la matriz de requisitos legales.

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de la Administraciones Públicas. (Esquema nacional de seguridad).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. (Esquema nacional de seguridad).
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero.

7. PREVENCIÓN

Las áreas del **Grupo A3sec** en la medida de lo posible, implementan las medidas mínimas de seguridad determinadas por el SGSPI, así como cualquier control adicional identificado a través de evaluación de riesgos, trazabilidad y tratamiento de los mismos. Para garantizar el cumplimiento de la política:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

8. DETECCIÓN

El **Grupo A3sec** pone sus esfuerzos principalmente en procesos que permitan la detección y respuesta nombrando al Centro de Seguridad y Vigilancia (CSVD) para el monitoreo de sus redes y procesos internos, con el fin de detectar y mitigar los posibles eventos que generen riesgos en las operaciones diarias, sus servicios y establecer su línea de defensa.

9. RESPUESTA

Los procesos del **Grupo A3sec** se encuentran disponibles y con respuesta efectiva para quien sea autorizado a conocerla, implantando en cada uno de sus estados, pilares de seguridad.

- Designado punto de contacto para las comunicaciones con respecto a incidentes detectados en otras áreas o en otros organismos.
- Ha establecido protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta ERI.

10. CONSERVACIÓN

El sistema de información garantizará la conservación de los datos e información en soporte electrónico. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

11. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El **Grupo A3Sec** entendiendo la importancia de una adecuada gestión de la información, establece y se compromete con la implementación, operación y la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), buscando establecer un marco de confianza para las partes interesadas, en el ejercicio de la operación de sus servicios, soportado en lineamientos claros y alineados con la misión y visión; apoyando el logro de sus objetivos estratégicos y el cumplimiento de los requisitos legales, regulatorios y contractuales de seguridad y privacidad de la información.

12. PRINCIPIOS DE SEGURIDAD

- Soportar las decisiones de seguridad en datos.
- Minimizar el tiempo de exposición ante los ataques.
- Aumentar la visibilidad y las capacidades de detección y respuesta.

Implantando en cada uno de sus estados, principios de confidencialidad que dicta la garantía que la información y los datos serán protegidos para que no sea divulgada a personal no autorizado; integridad para garantizar la correctitud y completitud desde que se origina el dato hasta que es eliminado; disponibilidad para garantizar el acceso autorizado a procesos, servicios y datos cada vez que sea requerido; autenticidad para garantizar fuentes verídicas de donde proceden los datos y trazabilidad para garantizar que puedan ser trazadas todas las actividades de las actuaciones para personas y procesos de forma constante.

13. GOBIERNO DE SEGURIDAD, PRIVACIDAD Y CIBERSEGURIDAD

La Dirección del **Grupo A3sec** está comprometida con la estrategia, gobierno y la dirección de la gestión de la seguridad, ciberseguridad y privacidad de la

información incluyendo el apoyo en la asignación de recursos y promoción de una cultura de seguridad, por lo cual, ha conformado la estructura organizativa del SGSPI, con el fin de velar por su correcto funcionamiento y cumplimiento.

12.1. ROLES, RESPONSABILIDADES Y AUTORIDADES DEL SGSPI

El **Comité de Seguridad y privacidad** del Grupo A3sec apoya y promueve el desarrollo, implementación, gestión y mantenimiento del SGSPI, asegurando su efectividad.

Así mismo asume los roles correspondientes a "**Responsable de la información**" y "**Responsable del servicio**" dentro de los órganos del SGSPI.

Así mismo es el órgano colegiado donde se toman las decisiones referentes al tratamiento de los datos de carácter personal, delegadas por el "**Responsable del Tratamiento, A3SEC**".

El comité de seguridad y privacidad se encuentra conformado por: la Dirección del Grupo A3sec, Responsable de seguridad, Responsable del Sistema, Technical manager, Administradores de seguridad, Equipo CSVD y el secretario.

Las funciones del Comité de Seguridad y privacidad son:

- Especificar los requisitos de seguridad, ciberseguridad y privacidad de la información acorde a la estrategia aprobada por la Dirección del Grupo A3sec.
- Determinar los requisitos de la información tratada por los propietarios y custodios en cada uno de sus niveles del servicio y de la información.
- Velar por el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- Realizar evaluaciones y tratamiento a posibles debilidades en los procesos, procedimientos y recursos tecnológicos que permitan la materialización de riesgos asociados con la información.

- Revisar, aprobar o derogar políticas, procedimientos o buenas prácticas dispuestos en los documentos oficiales del SGSPI según los estándares y frameworks dispuestos por A3sec.
- Revisar, analizar y tomar decisiones sobre incidentes que afecten la seguridad, ciberseguridad y privacidad de la información.
- Analizar y tomar decisiones sobre el resultado de la evaluación de riesgos y promover su tratamiento.
- Velar y hacer cumplir los controles técnicos y funcionales para la protección de la información contribuyendo al mantenimiento de certificaciones oficiales.
- Generar seguimiento a las métricas dispuestas para SGSPI y velar por su cumplimiento anual.
- Establecer los propósitos para los cuales, se recogen y procesan los datos personales, así como los métodos y procesos utilizados para mantener su protección de datos.
- Asegurar el cumplimiento de la responsabilidad legal y las obligaciones normativas vigentes.

a. Responsable de Seguridad:

Determina la seguridad, privacidad y ciberseguridad con controles pertinentes para satisfacer los requisitos establecidos por el Comité de Seguridad y privacidad operando en la supervisión del sistema.

Las funciones del Responsable de Seguridad son:

- Proponer, elaborar y presentar al Comité de Seguridad y privacidad de la Información la metodología de evaluación de riesgos y los medios para la clasificación de los activos de información y el ciberespacio.
- Recibir, analizar, interpretar y supervisar las regulaciones, estándares o requisitos de los órganos de control, relacionados con la seguridad, ciberseguridad y privacidad de la información.
- Desarrollar, implementar y mantener el cumplimiento de las políticas, procedimientos, controles y mejores prácticas globales aprobadas por el Comité de Seguridad y privacidad de la Información.
- Definir y hacer seguimiento a las métricas de seguridad y privacidad de la Información establecidas para la medición de resultados del SGSPI

correspondientes a la misión, visión y objetivos estratégicos.

- Coordinar con los propietarios de los activos de la información los controles para la protección de los datos.
- Apoyar a los funcionarios y contratistas para que cumplan con las responsabilidades de su rol frente al SGSPI.
- Elaborar, revisar, aprobar y presentar al Comité de Seguridad y Privacidad la Declaración de Aplicabilidad.
- Elaborar, difundir y hacer cumplir el plan de capacitaciones de Seguridad, ciberseguridad y privacidad de la información a todo el Grupo A3sec conjuntamente con Talento Humano.
- Coordinar la realización de auditorías internas y de terceras partes al SGSPI.
- Facilitar y promover el desarrollo de la mejora continua sobre seguridad, ciberseguridad y privacidad de la información.
- Validar que se cumpla el establecimiento y mantenimiento de registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSPI.
- Recomendar y presentar al Comité de Seguridad y Privacidad, las actualizaciones de políticas, normas y estándares de seguridad y privacidad de la información acorde al tratamiento de los riesgos efectuados
- Participar y supervisar la atención de incidentes, así mismo remitir a la autoridad competente las notificaciones con efectos adversos.

b. Delegado de datos personales:

Encargado de la supervisión y monitoreo de datos personales atendiendo a las medidas determinadas por el Comité de Seguridad y Privacidad.
Las funciones del Delegado de datos personales son:

- Supervisar el cumplimiento de la normativa de protección de datos personales.
- Identificar cambios en la normativa de datos personales y comunicarlas al comité de seguridad y privacidad.
- Coordinar la respuesta ante posibles violaciones de datos personales.
- Actuar como punto de contacto con las autoridades de protección de datos.
- Sugerir controles de protección de datos en proyectos o procesos que impliquen alto riesgo.

- Difundir y socializar concienciación sobre protección de datos personales.
- Mantener la Política General de Protección de datos revisada, actualizada y aprobada por el Comité de Seguridad y Privacidad.
- Atender los lineamientos y requerimientos que tenga a su cargo de Protección de Datos Personales.
- Ser el punto de contacto para solicitudes internas y externas sobre privacidad en la organización.
- Administrar el correo corporativo designado para administración de solicitudes específicas de Protección de Datos Personales.

c. Responsable del sistema:

Encargado de la operación del Sistema de Seguridad y Privacidad de la Información atendiendo a las medidas determinadas por el Responsable de Seguridad.

Las funciones del Responsable del Sistema son:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida.
- Proporcionar orientación, asesoramiento y asistencia sobre cuestiones que afectan la seguridad, ciberseguridad y privacidad de la información.
- Mantener los procedimientos de control de acceso establecidos por el comité de seguridad y Privacidad
- Comunicar al Responsable de seguridad los cambios operativos que afecten al sistema
- Supervisar las medidas de seguridad y privacidad tecnológicas que aplican a los proveedores de componentes.
- controlar e integrar las medidas de seguridad dispuestas por el SGSPI.
- La configuración autorizada y aprobación de modificaciones sustanciales de hardware y software.
- Determinar la Categoría del Sistema.
- Investigación de los incidentes de seguridad y comunicarlo a quién corresponda si procede.
- Establecer Planes de Contingencia o Emergencia y llevar a cabo ejercicios calendarizados.
- Acordar el uso de determinada información o prestación de servicio si se detectan vulnerabilidades graves en el sistema, decisión que debe ser acordada junto con el Responsable de Seguridad previamente.

d. Administrador de Seguridad:

Se encuentra asociado al área Técnica y opera el Sistema de Seguridad y Privacidad de la Información atendiendo a las medidas de seguridad determinadas por el Comité de seguridad y privacidad.

Las funciones del Administrador de Seguridad de la Información son:

- Implementación, gestión y mantenimiento de las medidas de seguridad aplicables al SGSPI.
- Gestión, configuración y actualización, administración del hardware y software en los que se basan los mecanismos y servicios de seguridad del SGSPI .
- Implementar y administrar los controles técnicos establecidos para mitigar los riesgos de seguridad, privacidad y ciberseguridad del Grupo A3Sec.
- La gestión del acceso en la asignación de privilegios concedidos a los usuarios del sistemas, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Monitorear las violaciones de seguridad y aplicar acciones correctivas para asegurar que se provea la seguridad adecuada.
- Asegurar que la infraestructura TI mantenga los controles de seguridad, privacidad y ciberseguridad en los procedimientos aprobados.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que siempre se ajustan las autorizaciones pertinentes.
- Informar al Comité de Seguridad y Privacidad o al responsable del sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta la resolución.
- Revisar y evaluar periódicamente las políticas de seguridad sobre las plataformas y sugerir al responsable del sistema cambios necesarios.
- Apoyar la revisión de productos y servicios en todas sus etapas desde su creación, puesta en operación y salida a producción en temas de seguridad.

- Servir de punto de apoyo respecto a cambios en la plataforma tecnológica, para asegurar que los aspectos de seguridad sean considerados en las etapas iniciales de los proyectos.
- Probar continuamente la seguridad de los elementos y determinar si requieren la actualización de dispositivos, software para solucionar problemas de seguridad o mejorar la seguridad con nuevas características.
- Actualizar parches de seguridad en los elementos que se deben proteger.
- Implantar las líneas bases de seguridad.

e. Encargado del tratamiento:

Se encuentra asociado a personal encargado de trabajar, procesar o administrar los datos personales del grupo A3sec (sin poder de decisión sobre los mismos) siguiendo las directrices y empleando los medios designados por el responsable.

Las funciones del Encargado del tratamiento son:

- Garantizar la custodia de la aceptación de uso y almacenamiento de datos personales en procesos digitales y físicos.
- Procesar los datos personales conforme a lo establecido por el Grupo A3sec y respetando las directrices de los clientes.
- implementar las medidas técnicas y organizativas necesarias para garantizar un nivel de protección adecuado
- Asegurar que los datos personales cumplan procesos de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad.
- Comunicar y asistir al Delegado de Datos Personales en respuesta de solicitudes si así es requerido.
- Asegurar el cumplimiento de la normativa de protección de datos en las plataformas técnicas.

f. Propietario de la información:

Se encuentra asociado a cualquier usuario, software o modelo de inteligencia artificial que cree u origine cualquier tipo de información.

Las funciones del Propietario de la Información son:

- Identificar todas las fuentes de información de sus procesos y realizar la clasificación de la información según los criterios establecidos por las políticas de seguridad de la información, así como las fuentes de amenazas y tratamientos del mismo.
- Asegurar que se cumpla el control y el tratamiento de los activos de información para preservar su confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad.
- Mantener un nivel apropiado de protección física y lógica de los activos de información participando en actividades de revisión y efectividad de los controles de los activos a su cargo.
- Realizar revisión y actualización periódica de los activos de información y del ciberespacio.
- Comunicar al responsable de seguridad los cambios realizados en los activos de información, con el fin de generar proceso de identificación de riesgos y ajustar los controles correspondientes.
- Comunicar al proceso responsable la necesidad del respaldo de la información para garantizar su disponibilidad

g. Custodio de la información:

Se encuentra asociado a cualquier usuario, software, modelo de inteligencia artificial, proveedor, cliente u organismo de control que almacene, procese, consulte o tenga conocimiento de cualquier tipo de información.

Las funciones del Custodio de la Información son:

- Proteger la información manteniendo los controles definidos por el propietario de la información.
- Solicitar aprobación del propietario de la información antes de realizar la divulgación o modificación de esta.
- Implementar los controles de acceso definidos o aprobados por el propietario de la información.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
- Mantener la etiqueta y clasificación de la información delegada por el propietario de la información.

- Comunicar al proceso responsable la necesidad del respaldo de la información para garantizar su disponibilidad
- Comunicar al Propietario de la información o al Responsable de Seguridad cualquier eventual que se tenga con la información custodiada

h. Talento Humano:

Se encuentra asociado a la administración del talento y gestión del ingreso, opera el Sistema de Seguridad y Privacidad de la Información atendiendo a las medidas de seguridad determinadas por el Comité de seguridad y privacidad.

Las funciones de Talento humano son:

- Ejecutar procesos de verificación de antecedentes a los candidatos que aspiren a vincularse laboralmente a la Organización según permita la legislación de cada país.
- Garantizar que los términos y condiciones de los contratos de los colaboradores cumplan con las directrices de seguridad de la información antes de la firma de este.
- Asegurar que los colaboradores del Grupo A3sec, tengan conocimiento de los procesos de seguridad de la información desde su incorporación en la Organización.
- Garantizar que los colaboradores aceptan al momento de su vinculación los acuerdos de confidencialidad, la Política Corporativa de Seguridad y Privacidad de la información, Política de uso aceptable de los activos y de recursos de información; para su privacidad, confidencialidad, integridad trazabilidad y autenticidad y asegurar su uso restringido
- Solicitar que los accesos lógicos otorgados a los colaboradores por el proceso de Infraestructura (Devops) y los administradores de seguridad sean acordes con los permisos del perfil dispuesto al empleado.
- Solicitar que los accesos físicos otorgados a los colaboradores por el área encargada sean acordes a los permisos del perfil dispuesto al empleado.
- Velar porque se lleven a cabo los procesos disciplinarios por incumplimiento de los procesos y directrices del SGSPI.
- Solicitar y velar que los colaboradores que cuenten con procesos de cambio de puesto, promoción de cargo o que tengan modificaciones en sus funciones y

responsabilidades, cuenten únicamente con los accesos físicos y lógicos para cumplir sus labores diarias.

- En el proceso de terminación del contrato de trabajo de un colaborador del Grupo A3sec, por cualquier causa, solicitar y asegurar que genere la entrega de los activos de información y ciberespacio, del cual, el colaborador es propietario o custodio, así como el bloqueo de los accesos lógicos y físicos correspondientes.
- Mantener un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial, por parte de los trabajadores, el cual deberá ser informado a estos desde el proceso de inducción.
- Coordinar y velar de forma activa que se cuente con procesos de sensibilización y formación y material de capacitación del SGSPI de forma anual como sea considerado por el comité de seguridad y privacidad.
- Seguir los controles adecuados para la contratación y manejo de proveedores.

- **Seguridad física:**

Adoptará las medidas de seguridad que le competan, dentro de las determinadas por el Responsable de Seguridad e informará a éste de su grado de implantación y eficacia

Las funciones de Seguridad Física son:

- Asegurar que las zonas físicas de Organización cuenten con los controles de seguridad física acordes a los lineamientos del Sistema de Gestión Seguridad y Privacidad de la Información SGSPI.
- Asegurar que los colaboradores de la Organización cuenten con los accesos físicos como puertas, archivos, tomas de datos, Biométricos, dispositivos periféricos, entre otros, asignados para su cargo.
- Cumplir con los controles ambientales de las zonas físicas de la Organización, predispuestas en el Sistema de Gestión Seguridad y Privacidad de la Información SGSPI..
- Centralizar los costos y compras que sean efectuados para implementar la seguridad física de la organización.

- **Codificación y Formación:**

Se encuentra asociado a la administración de la documentación y capacitación, opera el Sistema de Seguridad y Privacidad de la Información atendiendo a las medidas determinadas Comité de seguridad y privacidad.

Las funciones de Codificación y Formación son:

- Asegurar que todos los procedimientos, manuales, instructivos, formatos o anexos documentados sean revisados y actualizados con procesos de mejora continua, con el fin de prever e implementar controles respectivos.
- Realizar difusión de las políticas, procedimientos y guías aprobadas por el Comité de Seguridad, así como generar la publicación de acuerdo con el lineamiento de acceso a la información de la Organización.

- **Auditor:**

Se encuentra asociado a la evaluación y el cumplimiento del Sistema de Seguridad y Privacidad de la Información reportando al Comité de seguridad.

Las funciones del Auditor son:

- Realizar revisiones o evaluaciones independientes sobre la Seguridad y Privacidad de la Información e informar a la Alta Dirección y al Comité de Seguridad sobre el cumplimiento de las políticas , procesos y procedimientos.
- Identificar y reportar posibles debilidades en los procesos, procedimientos y recursos tecnológicos que permitan la materialización de riesgos asociados con la información.

Las demás responsabilidades y funciones específicas para cada uno de los roles del sistema, se encuentran descritas en el manual de funciones que conserva el área de Talento Humano del Grupo A3sec.

12.2. DESIGNACIÓN DE RESPONSABLES

El Responsable de Seguridad de la Información será nombrado por la Dirección y el Comité de seguridad y privacidad, el nombramiento se revisará cada 2 años o cuando el puesto quede vacante, los conflictos entre los distintos elementos de la

organización serán resueltos también por el presente comité, así como la asignación, designación de otros roles o su renovación.

14. LINEAMIENTOS GENERALES

Los activos de información y del ciberespacio sujetos a la Política Corporativa de Seguridad y Privacidad deben contar con evaluaciones de riesgo frente amenazas y vulnerabilidades a los que están expuestos, teniendo en cuenta metodologías aplicables para su revisión periódica sobre el ingreso, cambio, modificación y uso de los activos o cuando se reporten eventos, incidentes o alguna amenaza a nivel industria.

Los activos de información son transversales a los procesos estratégicos, misionales, apoyo y evaluación definidos en el Sistema de Gestión de Calidad SGC. Por lo cual, se ha establecido la revisión constante y el control de su administración mediante los propietarios y custodios de la información asignados.

Todos los colaboradores y usuarios de partes externas deben:

- Cumplir con su responsabilidad y alcance designados a las funciones de propietario o custodio de la información y dado el caso, roles adicionales frente al SGSPI.
- Participar en jornadas de actualización de activos de información.
- Clasificar la información en función de los requisitos legales, valor, criticidad de divulgación o modificación no autorizada.
- Desarrollar procedimientos para el empleo adecuado de los activos de información.
- Asegurar y cumplir con los controles de uso aceptable de los activos.
- Devolver al terminar el empleo, contrato o acuerdo de servicio, todos los activos de información a su cargo que sean propiedad del Grupo A3sec.

Toda la información que el Grupo A3sec hubiere informado, anunciado, revelado, comunicado, entregado, procesado, divulgado, publicado o dado a conocer a cualquier persona, órgano regulatorio, cliente, software o procesos de inteligencia artificial debe ser tratada conforme los términos y controles previstos en los procedimientos y políticas del SGSPI.

Toda información creada o procesada por primera vez deberá considerarse como restringida, hasta que se determine otro nivel de clasificación, pudiendo ser interna o pública según aplique y se justifique por el propietario de la información.

La divulgación de información clasificada como restringida e interna hacia terceras partes debe estar acompañada de la debida autorización de causa y objeto, adicionalmente deberán conciliar un contrato de confidencialidad explícitamente para que pueda ser compartida y usada.

Los datos procesados que contengan información externa de datos personales, financieros o catalogados como sensibles se mantendrán protegidos como información restringida y con los controles aplicables acorde a la normatividad vigente de cada país.

El acceso de usuarios no registrados ante el Grupo A3sec, debe ser permitido sólo al sitio web e información clasificada como pública, cualquier uso de recursos de información o infraestructura de TI no es permitido a usuarios invitados o no registrados sin contar con los mecanismos de autorización correspondientes.

La infraestructura TI debe ser protegida por los responsables, siguiendo los lineamientos de protección con enfoque multinivel que involucre controles humanos, físicos, técnicos, modelos de IA, monitoreo y administrativos conformes en el SGSPI.

Los proyectos dirigidos al **Grupo A3sec** o realizados por la organización debe ser comunicados y analizados en la gestión de riesgos, con el fin, de efectuar sugerencias de control y se integre con la estrategia de seguridad, privacidad y ciberseguridad del SGSPI.

El **Grupo A3sec** tiene establecida la política de uso aceptable de los activos, la cual debe ser conocida y aceptada por todos los colaboradores, contratistas o prestadores de servicios que accedan de cualquier forma a los activos de información.

Son reservados los derechos de auditoría, dentro de las actividades de seguimiento a los colaboradores y terceras partes, con propósito de corroborar el cumplimiento

de las políticas y procedimientos vigentes del SGSPI, con el fin de velar por el correcto uso de los activos de información.

El **Grupo A3sec** proveerá los mecanismos para que la información sea accedida y utilizada por el colaborador de acuerdo con sus responsabilidades; sin embargo, se reserva el derecho de revocar el personal, el privilegio de acceso a la información y tecnologías que la soportan, si las condiciones lo ameritan.

15. TRATAMIENTO DE DATOS PERSONALES

El **Grupo A3Sec** recopila, trata y divulga datos personales confidenciales solo cuando es necesario para cumplir con las obligaciones impuestas por la ley o si existe un motivo imperativo comercial para hacerlo según lo permitido por la ley aplicable o con el consentimiento del miembro del personal.

El administrador a través de la dirección de correo electrónico: *dataprotection@a3sec.com*, brinda respuesta a las solicitudes de información sobre los datos personales recolectados para tratamiento.

16. CUMPLIMIENTO COLABORADORES

El trabajador, colaborador o personal contratado por prestación de servicio u otro, deben conocer los diferentes lineamientos y usos de la presente Política de Seguridad y Privacidad de la información y demás normativas del SGSPI y firmar su conformidad, así mismo siendo responsabilidad del Comité de Seguridad y privacidad de la información disponer los medios necesarios para que la información se encuentre disponible en el momento de su incorporación a través del documento Manual Politicas del SGSPI y los procedimientos implementados.

17. CUMPLIMIENTO TERCEROS

En todo contrato celebrado con proveedores o terceros que involucre el conocimiento o uso de la información; se extiende el cumplimiento de la presente Política de Seguridad y Privacidad de la información, se establecerán canales de

comunicación para la implementación de los controles correspondientes al SGSPI así como el marco de actuación ante incidentes de seguridad.

Cuando algún aspecto de la presente Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

18. SANCIONES

Los incumplimientos serán sancionados, conforme a la magnitud y característica del aspecto no cumplido. Además de la aplicación de las sanciones disciplinarias o administrativas, el trabajador, colaborador o prestador de servicio que no ha dado cumplimiento a sus obligaciones con respecto a estas políticas podrán incurrir en responsabilidad civil o patrimonial cuando ocasione un daño que debe ser indemnizado y/o en responsabilidad penal de acuerdo a las leyes vigentes de cada país, cuando su conducta constituya un comportamiento considerado delito según las leyes predispuestas para ello.

El incumplimiento de la presente política por parte de un proveedor constituye una justa causa para dar por terminado de manera unilateral el respectivo contrato. Igualmente, facultará al Grupo A3sec para llevar a cabo la imposición de las multas o sanciones pactadas, sin que esto represente para la Organización obligación alguna de pagar sumas a título de indemnización.

19. DIFUSIÓN Y SENSIBILIZACIÓN

Resulta clave para el SGSPI integrar en la cultura organizacional, la implementación del plan de difusión, capacitación y sensibilización en torno a la seguridad, privacidad y ciberseguridad, por lo cual, el Comité de Seguridad de la Información velará por su cumplimiento, ya que posteriormente de la aprobación de políticas o procedimientos vinculados deberán ser difundidos para su aplicación y cumplimiento.

El Responsable de Seguridad procurará que todos los colaboradores reciban el entrenamiento en materia de los procedimientos y controles estipulados para la

protección de la seguridad, privacidad y ciberseguridad correspondiente al SGSPI del **Grupo A3sec.**

Todos los colaboradores del Grupo A3sec tendrán que cursar y completar las capacitaciones y actividades de sensibilización de forma virtual o presencial según sea requerido y el control de su cumplimiento será llevado a cabo por el área de talento humano y calidad.

20. CONSERVACIÓN DE LA POLÍTICA

El presente documento debe ser revisado mínimo una vez al año y actualizado cada vez que se realicen cambios relevantes que afecten la adecuada protección de la información, considerando los cambios en la misión, visión objetivos estratégicos, productos y servicios, infraestructura TI, partes interesadas, activos de información, tratamiento de riesgos o cambios en los estándares o procedimientos de seguridad, privacidad y ciberseguridad que así lo requieran para mantener la efectividad del SGSPI.

La Política de Seguridad y Privacidad de la información constituye una política de alto nivel destinada a normar los aspectos más relevantes del marco de seguridad, privacidad y ciberseguridad de la información, por lo cual, se promulgan y se declaran los siguientes documentos adicionales que indican a mayor detalle las medidas de protección de la información.

- Estrategia de Gobierno SGSPI
- Manual Políticas SGSPI
- Política de Uso Aceptable
- Procedimientos, guías, formatos, registros del SGSPI
- Manual SGSPI

<Control de cambios/>

Versión	Fecha	Descripción del cambio	Responsable de la aprobación del cambio
0.1	21/04/2017	Versión inicial	Enrique Pinzón Fajardo
0.2	06/03/2018	Revisión y actualización	Cesar Moreno
0.3	01/06/2018	Revisión y actualización: Se incluye la Política Corporativa, Objetivos, Contexto Interno y Externo, Partes Interesadas, entre otras.	Diana Aguirre
1.0	19/06/2018	Versión Oficial Vigente	Comité de Seguridad
2.0	10/01/2019	-Se cambian los objetivos de seguridad. -Se modifica el contexto interno, específicamente el ítem 8.4: los objetivos estratégicos de la Grupo A3Sec de acuerdo al Plan Estratégico del año 2019.	Comité de Seguridad
3.0	05/04/2019	-Se incluye el principio dentro de la Política Corporativa, de acuerdo a los compromisos de la Revisión por la Dirección. -Se ajustan las partes interesadas, dejando	Comité de Seguridad

		únicamente las relevantes para el SGSI.	
4.0	04/12/2019	Se ajusta los roles del equipo del CSVD de acuerdo a los cambios de estructura interna	Comité de Seguridad
4.1	21/02/2020	Se anexa la información de los proveedores al capítulo 10 Partes Interesadas.	Comité de Seguridad
4.2	18/12/2020	Se modifica el Organigrama corporativo debido a los recientes cambios estructurales en la organización	Comité de Seguridad
5.0	22/01/2021	Se modifican los proyectos inicialmente definidos en el manual para apoyar la gestión del SGSI. Se retiran los proyectos ejecutados de 2018 y 2019 y se actualiza con proyectos de 2020 y 2021.	Comité de Seguridad
6.0	30/09/2021	-Integración del sistema de gestión de seguridad y privacidad de la información.	Comité de Seguridad
6.1	28/10/2021	Se actualiza el código de este documento de AE-MA-001-COL a AE-MA-001-COR. Se hace el cambio de las siglas SGSI (Sistema de Gestión de Seguridad de la Información) por SGSPI (sistema de Gestión de Seguridad y Privacidad de la información).	Comité de Seguridad

6.2	29/12/2021	Se redirecciona el link a la política de seguridad y privacidad, al análisis de contexto del negocio y las partes interesadas (Documentos actualizados del SGC)	Comité de Seguridad
6.3	21/12/2022	Ajuste en Diagrama de Gobierno de Seguridad, ajuste en tabla de objetivos de seguridad, actualización de tabla de estrategia, actualización de tabla de objetivos estratégicos, incorporación de seguimiento de incidentes como parte de actividades del comité de seguridad. Inclusión de la sección DOCUMENTACIÓN ASOCIADA.	Comité de Seguridad
6.3	19/01/2023	Modificación de la palabra CSVD por IXDR y alcance	Comité de Seguridad
6.4	23/11/2023	Se ajusta el tipo de documento a utilizar en el manejo de las decisiones tomadas en el comité.	Comité de Seguridad
6.5	20/12/2023	Se reemplaza la palabra IXDR por detección y respuesta ya que aprueba el nuevo portafolio de servicios que a su vez ya fue aprobado por el comité de dirección.	Comité de Calidad
7.0	20/06/2024	Se incluyen nuevos apartados de acuerdo a lo citado en el ENS Aprobación y entrada en vigor, Misión del SGSPI,Lineamientos generales,Tratamiento de datos personales, Cumplimiento colaboradores,	Comité de Seguridad

		Cumplimiento terceros, Sanciones, Difusión y sensibilización, Conservación de la política nuevo. También se incluyen e incluyen los roles y perfiles aprobados y se ajustan los apartados de Introducción,Ámbito y Alcance, Objetivo y Marco Normativo	
7.1	18/07/2024	Se incluye información de las responsabilidades del delegado de datos personales y del encargado del tratamiento	Comité de Seguridad
7.2	27/08/2024	Se modifica los roles referentes al comité de seguridad	Comité de Seguridad