1. ALCANCE

Esta política aplica a toda la Organización, sus colaboradores, contratistas y terceros de **AS•NET**.

2. DEFINICIONES

- **Activo de información:** Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que almacena, procesa o transmite información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de AS•NET.

- **Confidencialidad.** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

- **Integridad.** Propiedad de exactitud y completitud.

- **Riesgo.** Efecto de incertidumbre sobre los objetivos.

- **SGSI.** Sistema de Gestión de Seguridad de la Información

- **Ciberseguridad.** Capacidades de AS•NET para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

- **Ciberespacio.** Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

- **Ciberataque.** Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

- **SIEM.** Sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red. Suelen ser sistemas de centralización de logs.

3. POLÍTICAS

La dirección de **AMERICAN SMART SYSTEMS & NETWOKS** (En adelante **AS•NET**), entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema De Gestión De Seguridad De La Información - SGSI basado en la NTC-ISO-IEC 27001:2013 buscando establecer un marco de confianza en el ejercicio de sus deberes con las partes interesadas, todo enmarcado en el estricto cumplimiento de las leyes y normas correspondientes, en concordancia con la misión y visión de la Organización.

La dirección de **AS•NET** igualmente considera crucial la implementación de procedimientos para la protección de los dispositivos que se encuentran interconectados para el procesamiento de información digital almacenada en el ciberespacio, así la ciberseguridad ayudara a los recursos humanos y técnicos dispuestos por **AS•NET** a mitigar ataques cibernéticos que puedan alterar la misión y visión de la organización.

Para **AS•NET**, la protección de la información y los dispositivos que la contienen, pretende la disminución del impacto generado sobre sus activos de información, por los riesgos identificados de manera sistemática con objeto de mantener la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a toda la organización, en la cual se incluyen sus colaboradores, terceros, aprendices, practicantes, proveedores y partes interesadas en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del **SGSI** estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en los procesos misionales de la Organización.
- Cumplir con los principios de seguridad de la información y ciberseguridad.
- Mantener la confianza de sus clientes, socios y colaboradores.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Establecer las políticas, procedimientos, estándares de configuración e instructivos en materia de seguridad de la información y ciberseguridad.
- Fortalecer la cultura de seguridad de la información en los colaboradores, terceros, aprendices, practicantes y clientes de **AS•NET**.
- Garantizar la continuidad del negocio frente a incidentes.

AS•NET ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios de seguridad que soportan el **SGSI** de **AS•NET**:

- Las responsabilidades frente a la seguridad de la información serán conocidas, comprendidas aceptadas y cumplidas por cada uno de los colaboradores, proveedores, aliados estratégicos o terceros.

- **AS•NET** protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos de información del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- **AS•NET** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- **AS•NET** protegerá su información de las amenazas originadas por parte del personal.

- **AS•NET** controlará la operación de sus procesos de negocio garantizando la seguridad de los activos de información.

- **AS•NET** implementará controles de acceso a los activos de información.

- **AS•NET** procurará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- **AS•NET** asegurará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva del SGSI.

- **AS•NET** velará por la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los incidentes.

- **AS•NET** cumplirá sus obligaciones legales, regulatorias y contractuales establecidas.

3.1. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- Preservar la confidencialidad de la información, evitando su divulgación y el acceso a personas, entidades y procesos no autorizados.

- Mantener la integridad de la información asegurando su exactitud y completitud, y evitando su deterioro.

- Asegurar la disponibilidad de la información en todos los soportes de almacenamiento y medios de respaldo para cuando sea requerida.

- Identificar riesgos y establecer controles, limitando y previniendo las consecuencias de los diferentes incidentes, para asegurar la recuperación inmediata de las operaciones y minimizar los daños a la organización.

- Capacitar y concientizar continuamente al personal en temas relacionados con la seguridad de la información.

- Garantizar la protección y la seguridad de la información que nos suministran nuestros clientes para el desarrollo de los proyectos.

- Gestionar eficientemente la accesibilidad de la información de los colaboradores de AS•NET de acuerdo con el perfil definido, buscando minimizar a su vez los riesgos de seguridad de la información.

- Gestionar los incidentes en materia de seguridad de la información, utilizando las directrices establecidas por **AS•NET**.

- Garantizar la continuidad del negocio, minimizando los posibles impactos a los servicios prestados.

- Proteger los activos de información y gestionar las vulnerabilidades.

- Mejorar continuamente el **SGSI**, revisando su desempeño y su eficacia.

- Implementar un sistema de monitoreo (**SIEM**) obteniendo un seguimiento del alertamiento en caso de ciberataques.

3.2. NIVEL DE CUMPLIMIENTO

Todos los colaboradores, proveedores, aliados estratégicos y terceros deberán cumplir las políticas descritas en este documento y en todos los manuales, procedimientos y demás documentos que componen el SGSI.

3.3. REVISIÓN DE LA POLÍTICA

Esta política se encuentra disponible a las partes interesadas en la intranet de **AS•NET** y en la página WEB, asimismo, será objeto de actualización, al menos una vez al año o cuando ocurran cambios significativos en el contexto interno o externo de **AS•NET** o ante la ocurrencia de incidentes de Seguridad de la Información que ameriten la actualización de la misma.

4. DOCUMENTOS DE REFERENCIA

Normas

- **PCI DSS 3.2.1** Norma de seguridad de datos. Requisitos y procedimientos de evaluación de seguridad.
- **ISO-IEC 27000:2014** Sistemas de Gestión de Seguridad de la Información – Vocabulario
- **NTC-ISO-IEC 27001:2013** Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos
- **GTC-ISO-IEC 27002:2015.** Tecnología de la Información. Técnicas de Seguridad, Código de Practica para Controles de Seguridad de la Información.
- **ISO/IEC 27032.** Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad
- **Circular Externa 007 de 2018.** Superintendencia Financiera de Colombia. Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad

5. CONTROL DE CAMBIOS

Fecha	Versión	Ítem del Cambio	Modificación
18/06/2019	1	-	Documento Inicial
22/05/2020	2	- 2 3 3.1	Título de la política Definiciones: se realizó la inclusión de las definiciones de los términos ciberseguridad, ciberespacio, ciberataque y SIEM Políticas se adiciona párrafo de la importancia de la ciberseguridad Objetivos de seguridad de la información y ciberseguridad

Elaboró:	**Revisó:**	**Aprobó:**
Rodrigo Navarrete	Comité de Seguridad de la Información	José Fernando Rodríguez
Cargo: Analista de Seguridad de la Información	**Cargo:** Comité de Seguridad de la Información	**Cargo:** CEO