SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ANAS WAYUU
EMPRESA PROMOTORA DE SALUD INDÍGENA
E.P.S.I.
Juntos Gestionamos Salud.

Maicao, La Guajira

CONTENIDO

1. INTRODUCCIÓN

La base para que la EPSI Anas Wayuu pueda operar de una forma confiable en materia de Seguridad Informática e información, comienza por la definición de políticas de seguridad de la información y la aprobación de un manual, que permita evaluar y gestionar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información, para lo cual se ha tomado como referencia la ISO 27001 de 2013, a efectos de implementar la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

- ✓ Seguridad de Personal.
- ✓ Seguridad Física y Ambiental.
- ✓ Administración de Operaciones de Cómputo.
- ✓ Controles de Acceso Lógico.
- ✓ Cumplimiento.

2. PROPÓSITO

El presente documento tiene como finalidad, contar con una guía del modelo del Sistema de Gestión de Seguridad de la Información de la EPSI ANAS WAYUU, señalando las políticas, responsabilidades, principios, criterios, directrices y conductas de todos los funcionarios dentro de los lineamientos de ética y la buena administración definida por la entidad. Igualmente, permitir la evaluación y efectividad del SGSI, así como facilitar las auditorías.

3. GLOSARIO

- **Análisis de Riesgo:** Proceso para analizar los peligros que plantean los eventos de causa natural y humana a los activos de una organización.

- **Antivirus:** Es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

- **Área Segura:** Espacio físico donde se almacena o procesa información crítica de la entidad.

- **Certificado SSL:** Autentica y verifica que los usuarios que envían sean quienes afirman ser, también proporciona confidencialidad para el receptor con los medios para cifrar una respuesta.

- **Cifrado:** Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

- **Control:** Medio para gestionar el riesgo, incluye políticas, procedimientos, guías, practicas o estructuras.

- **Control de Acceso:** Describe la restricción de los derechos de acceso a las redes, los sistemas, las aplicaciones, las funciones y los datos.

- **Contrafuegos (Firewall):** es un dispositivo de seguridad de red que monitorea el tráfico hacia o desde su red. Permite o bloquea el tráfico según un conjunto definido de reglas de seguridad.

- **Confidencialidad:** Propiedad mediante la cual la información no se hace disponible o revelada a individuos, entidades o procesos no autorizados.

- **Integridad:** Propiedad de protección de la exactitud, uniformidad, confiablidad y completitud de la información.

- **Disponibilidad:** Propiedad mediante la cual la información es accesible y utilizable por solicitud de una entidad autorizada.

- **Dato:** Información amplia o concreta que permite una deducción o conocimiento exacto.

- **DoS:** Ataque de Negación de Servicios; es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

- **DDoS:** Es similar al DoS pero este se origina des múltiples y coordinadas fuentes.

- **Información:** Conjunto de datos sobre una materia determinada, además es un activo esencial para los negocios de una organización y por tanto debe ser protegida de forma adecuada.

- **Incidente:** La consecuencia de la materialización de una amenaza, la cual modifica el estado del activo de información.

- **Gestión de Activos:** Es el inventario y el esquema de clasificación para los recursos de información.

- **Google Cloud:** consiste en un conjunto de recursos físicos, como computadores y unidades de disco duro y recursos virtuales, como máquinas virtuales que se encuentran en centros de datos en todo el mundo.

- **Malware:** es un software malicioso que tiene como objetivo infiltrarse o dañar una computadora o sistema de información

- **Política de seguridad:** Documento que aborda las restricciones y los comportamientos de los miembros de una organización y específica a menudo como se puede acceder a los datos y la forma de acceso.

- **Riesgo:** Posibilidad (probabilidad) que suceda algún evento que impacte (consecuencia) sobre los objetivos de negocio (AS/NZS 4360) y se expresa como la combinación de probabilidad e impacto (ISO 31000).

- **Seguridad de la información:** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

- **Unidad de red:** es cualquier ubicación virtual a la que solo se puede acceder a través de la red, la cual debe ser configurada previamente por la oficina TIC.

- **Virus:** es un software malicioso que tiene por objetivo de alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario.

- **Vulnerabilidad:** Deficiencia, debilidad del activo, sistema de información, aplicación, software y hardware que puede ser explotada para causar daño o mal funcionamiento del mismo.

- **VPN:** Virtual Prívate Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

4. SUSTENTOS LEGAL Y NORMATIVO TECNICO

Constitución Política Artículo 15	Reconoce como Derecho Fundamental el Habeas Data; **Artículo 20**. Libertad de Información.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la Protección de Datos Personales.
Ley 1437 de 2011	Procedimiento Administrativo y aplicación de criterios de seguridad.
Ley 1341 de 2009	Tecnologías de la Información y aplicación de seguridad.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
Ley 527 de 1999	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Decreto 415 de 2016	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 1083 de 2015	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 2952 de 2010	Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.
CONPES 3701 de 2011	Lineamientos de Política para ciberseguridad y ciberdefensa.
CONPES 3854 de 2016	Política Nacional de Seguridad digital
ISO 27001	NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

5. POLÍTICA

a. OBJETIVO

Las políticas tienen como objetivo establecer los lineamientos que debe cumplir la EPSI Anas Wayuu, para asegurar la gestión de la seguridad de la información, durante la ejecución de todos los procesos que se realicen dentro y fuera de la organización, bajo un enfoque de gestión integral del riesgo, así como el cumplimiento de los objetivos corporativos, la política de seguridad de la información garantiza:

- ✓ La calidad y el mejoramiento continuo de los procesos.
- ✓ La satisfacción del cliente interno y externo mediante un talento humano capacitado y competente.
- ✓ La cultura de prevención y control sobre los eventos de Seguridad y Salud en el trabajo.
- ✓ La generación de procesos interculturales y diferenciales de la atención en salud indígena.
- ✓ La cobertura integral en salud con una red idónea y suficiente, fortaleciendo la gestión de los riesgos en salud.
- ✓ El crecimiento financiero, social y ambiental sostenible satisfaciendo las necesidades presentes y protegiendo las generaciones futuras.

b. ALCANCE

El sistema de gestión de seguridad de la información, aplica de manera obligatoria a todos los usuarios internos y externos, que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la EPSI Anas Wayuu.

c. EVALUACIÓN

El manual del SGSI y las políticas, serán evaluadas semestralmente y se actualizarán cada vez que sea necesario, según las necesidades que demande la empresa y las exigencias normativas.

d. SANCIONES

El incumplimiento al presente Manual y política podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya

sanción será aplicada por las autoridades competentes según el reglamento interno de trabajo de la EPSI Anas Wayuu y la ley 1273 de 2009.

e. SOCIALIZACIÓN

El manual de seguridad de la información y las políticas serán socializados a funcionarios, contratistas, pasantes, proveedores, aprendices y practicantes, una vez sea aprobado por la alta gerencia, así mismo cada vez que se realicen actualizaciones o modificaciones al presente manual.

Nota: Cada vez que exista una vinculación laboral se realizará la socialización manual de seguridad de la información y las políticas por parte de la Dirección de Aseguramiento, Tecnología y Comunicaciones con el apoyo de la Oficina de Gestión Humana. Así mismo las actividades de **sensibilización, comunicación y capacitación** de seguridad de la información, se estarán desarrollando según el plan de (PCSC) de la EPSI Anas Wayuu.

f. CONFIDENCIALIDAD

Todo usuario, proveedor, contratista que utilice, administre, procese, actualice, cree o consulte activos de información de las EPSI Anas Wayuu, firmará un acuerdo de confidencialidad de la información, así como el estricto apego al Manual y políticas de Seguridad de la Información. Este proceso será llevado a cabo, por los siguientes responsables:

- ✓ Oficina Gestión Humana para Contratación de personal.
- ✓ Direcciones involucradas en el proceso de contratación de Proveedores o Contratistas.

g. ACCESO AL CENTRO DE COMPUTO

El acceso físico y lógico al centro de cómputo de la EPSI Anas Wayuu, solo está permitido al personal autorizado por la dirección de Aseguramiento, Tecnología y Comunicaciones.

h. USO DE EQUIPOS E INFORMACIÓN

Los activos de información de la EPSI Anas Wayuu, solo podrán utilizarse para el cumplimiento de las funciones y objetivos que fueron designados a colaboradores, contratistas, pasantes, proveedores, aprendices y practicantes.

i. ACCESO LÓGICO A LOS ACTIVOS DE INFORMACIÓN

El acceso a los sistemas de información, será administrado por la Dirección de Aseguramiento, Tecnología y Comunicaciones, de conformidad con los niveles de accesibilidad definidos por la entidad, de acuerdo con el cargo y funciones de sus empleados, o las funciones que deban realizar pasantes, contratista o terceros. Cada usuario es responsable de la custodia del mecanismo de control de acceso que le sea proporcionado.

j. VIDA ÚTIL DE EQUIPOS

La vida útil de los equipos de cómputo o comunicaciones estará sujeto a las recomendaciones del fabricante. La entidad garantizara el mantenimiento preventivo y/o correctivo según sea el caso, las revisiones estarán a cargo de la Dirección Aseguramiento, Tecnología y Comunicaciones.

k. GESTIÓN DE RIESGO

La EPSI Anas Wayuu tiene un plan de gestión de riesgos que deberá ser revisado bimestralmente y ajustado según sea el caso, por la Dirección Aseguramiento, Tecnología y Comunicaciones.

l. HARDWARE LIMPIOS

La EPSI Anas Wayuu, establecerá medidas de protección para evitar daños o accidentes.

6. LINEAMIENTOS

Anas Wayuu EPSI como entidad promotora de salud indígena tiene un compromiso decidido hacia la seguridad de la información propia y de terceros que se la hayan confiado, incluyendo información de carácter personal, deber que involucra a los colaboradores que actúan en su nombre, así como toda parte interesada que pueda tener acceso a dicha información.

La gestión de seguridad de la información en la organización está basada en una arquitectura de control y bajo el enfoque de la gestión del riesgo, la cual incluye medidas preventivas y correctivas de la organización y de los sistemas tecnológicos para proteger así la información en aras de cumplir los objetivos institucionales manteniendo su confidencialidad, disponibilidad e integridad.

Nuestro compromiso reúne la gestión del cumplimiento y de la conformidad sobre los requisitos aplicables, tanto del ordenamiento jurídico pertinente y contractual, haciendo especial énfasis en los aspectos de privacidad, transparencia y nivel de servicio, así como de la protección adecuada de información de carácter reservado.

Para asegurar la continua pertinencia de la gestión integral de la seguridad de la información frente a posibles cambios en el contexto, especialmente en partes interesadas, requisitos legales aplicables, asumimos el deber de mantener y mejorar de forma continua la gestión de la seguridad de la información y riesgos asociados.

a. SANCIONES POR INCUMPLIMIENTO

El incumplimiento al presente Manual acarreará, responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes según el reglamento interno de trabajo de la EPSI Anas Wayuu y la ley 1273 de 2009.

b. BENEFICIOS

El manual del sistema de gestión de seguridad de la información de la EPSI permite mantener políticas y reglas de custodia y administración de la información, bajo la norma ISO 27001 de 2013 y el cual aporta:

- Reduce el riesgo de pérdidas de información.
- Permite establecer metodologías para gestionar la seguridad de la información.
- Genera culturas orientadas a la protección del dato y el buen uso de la información.
- Le permite a la EPSI Anas Wayuu cumplir con la legislación vigente en materia de seguridad de la información.
- Garantiza la continuidad de la operación de la institución.
- Garantiza el cumplimiento de los objetivos institucionales.
- Motivación para el personal, ya que se desarrollan en una entidad comprometida con la seguridad de la información.

c. SOCIALIZACIÓN DE LAS POLÍTICAS

El manual del sistema de gestión de seguridad de la información de la EPSI será socializado una vez sea aprobado por la alta dirección y cada vez que se realice actualizaciones o modificaciones. Dicha socialización va dirigida a todos los Usuarios (empleados, contratistas, pasantes y terceros) de la EPSI Anas Wayuu, así mismo cada vez que ingrese un nuevo funcionario a la empresa; la socialización la realizará la dirección de

Aseguramiento, Tecnología y Comunicaciones con el apoyo de la Oficina de Gestión Humana. Las actividades de **sensibilización, comunicación y capacitación** de seguridad de la información, se estarán desarrollando según el plan de (PSCC) implementado por la EPSI Anas Wayuu.

d. EVALUACIÓN DE LAS POLÍTICAS

El manual del sistema de gestión de seguridad de la información de la EPSI será evaluado semestralmente y se actualizará cada vez que sea necesario según las necesidades que demande la EPSI y la exigencia de nuevas normativas o leyes de estado.

7. POLÍTICA PARA LOS DISPOSITIVOS MÓVILES

El presente manual estipula los lineamientos y protocolos que deben seguir los usuarios de dispositivos móviles de la EPSI Anas Wayuu durante las actividades realizadas dentro y fuera de la entidad, bajo una orientación aplicada a la mejora continua y de la gestión del riesgo.

Todo usuario de dispositivos móviles de la EPSI Anas Wayuu deberán utilizarlos para las actividades específicas que fueron descritas al momento de la asignación del dispositivo.

La Dirección de Aseguramiento, Tecnología y Comunicaciones debe mantener actualizados y asegurados los dispositivos móviles mediante los mecanismos institucionales para proteger la información que es almacenada en los mismos, de igual manera deberán proteger la información sensible o confidencial que por necesidades institucionales deba ser almacenada o trasmitida, ya sea dentro de la red interna de la EPSI Anas Wayuu o a dispositivos externos.

Los usuarios que hagan o hacen uso de dispositivos móviles de la EPSI Anas Wayuu, deben conocer y aplicar las medidas para la prevención de fuga de información sensible o confidencial.

La Dirección de Aseguramiento, Tecnología y Comunicaciones será el encargado de la asignación, monitoreo y mantenimiento de los dispositivos móviles de la EPSI Anas Wayuu.

a. REGLAS DE USO DE LOS DISPOSITIVOS MÓVILES:

- Para la trasmisión, procesamiento, almacenamiento y consulta de cualquier tipo de información de la entidad en dispositivos móviles tales como; iPad/Tablet, Disco duros externos, dispositivos USB, se debe realizar bajo la autorización y supervisión de la Dirección de Aseguramiento, Tecnología y Comunicaciones.

- El ingreso y salida de dispositivos móviles que no estén dentro del inventario de activos de la EPSI Anas Wayuu deberá registrarte en el formato diseñado para dicho control.

- La conexión a la red de la EPSI Anas Wayuu se realizará bajo el rol de invitados con la autorización de la dirección de aseguramiento, de Tecnología y Comunicaciones.

- Los usuarios externos de la EPSI Anas Wayuu no tienen acceso a la red por ser privada.

- Todo activo de información que salga de la entidad debe ser autorizado por la alta dirección de cada proceso y supervisada por la dirección de aseguramiento, tecnología y comunicaciones.
- Los dispositivos móviles de la EPSI Anas Wayuu deben ser de uso exclusivo para el desempeño de las actividades laborales en la entidad, no debe contener información ajena a la EPSI.

b. INSTALACIÓN DE SOFTWARE

- Está prohibido la instalación de software en los dispositivos móviles de la EPSI Anas Wayuu.
- La Dirección de Aseguramiento, Tecnología y Comunicaciones es la dependencia autorizada para la instalación de software en los dispositivos móviles.

8. POLÍTICA DE TELETRABAJO

Conforme a lo declarado en la política general de seguridad de la información, esta también aplica en los casos de una relación laboral contractual bajo la modalidad de teletrabajo.

De conformidad con lo dispuesto por el artículo 2° de la ley 1221 de 2008 “Teletrabajo. Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.”

La EPSI debe garantizar que los equipos, dispositivos móviles y recursos tecnológicos que puedan ser usados para el desarrollo de una actividad de teletrabajo garanticen la seguridad de la información.

a. APLICABILIDAD

La presente política aplica para todos los colaboradores, terceros, aprendices, practicantes y proveedores en todos los niveles jerárquicos de la EPSI Anas Wayuu que tengan dentro del desarrollo de sus actividades acceso a cualquier tipo de información de la entidad.

b. REGLAS

- Ningún colaborador de la EPSI contratado bajo la modalidad de teletrabajo podrá desarrollar actividades propias de la EPSI para el tratamiento de la información en equipos, dispositivos móviles o herramientas tecnólogas que no esté autorizado por la Dirección De Aseguramiento, Tecnología Y Comunicaciones.

- Los usuarios de teletrabajo no podrán utilizar conexiones inseguras (wifis abiertas, redes públicas, módems USB).
- Los usuarios de teletrabajo deben separar los entornos de teletrabajo del entorno de sus actividades personales, como son cuentas de usuarios y manejos de correos no institucionales.

9. POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LOS USUARIOS

Todo usuario de bienes y servicios informáticos deberá firmar un acuerdo en el que acepte las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información de la EPSI Anas Wayuu, así como el estricto apego al Manual del Sistema de Gestión de la Seguridad de la Información y Políticas para Usuarios.

a. OBLIGACIONES DE LOS USUARIOS

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas del Sistema de Gestión de la Seguridad de la Información.

b. ACUERDOS DE USO Y CONFIDENCIALIDAD

Todos los usuarios de bienes y servicios informáticos de la EPSI Anas Wayuu deberán firmar el acuerdo de confidencialidad y uso adecuado de los recursos informáticos y de información de la EPSI Anas Wayuu establecido en el contrato laboral y en el formato Creación de Usuario y/o Asignación de Contraseñas.

c. ENTRENAMIENTO EN SEGURIDAD INFORMÁTICA

Una vez aprobado el presente manual del Sistema de Gestión de la Seguridad de la Información por la alta gerencia, toda la planta de personal de la EPSI deberá ser capacitada y entrenada de acuerdo a sus disposiciones, cuando existan nuevas contrataciones de personal, la Dirección de Aseguramiento, Tecnología y Comunicaciones tendrá la responsabilidad de realizar dichas capacitaciones y entrenamientos al ingreso del trabajador, previa comunicación de la Oficina de Gestión Humana.

Los manuales y políticas se alojarán en la intranet para ser objeto de consulta de todos los funcionarios en tiempo real y de disponibilidad en horas laborales.

d. MEDIDAS DISCIPLINARIAS

En los eventos que la Dirección de Aseguramiento, Tecnología y Comunicaciones advierta el incumplimiento de las disposiciones contenidas en el presente Manual, lo remitirá de forma inmediata a su conocimiento, al comité de seguridad de la información, para que sus integrantes evalúen el impacto y la gravedad de la falta cometida y de acuerdo a las responsabilidades atribuidas mediante la resolución 012/2018 se trasladen a quienes deban aplicar las medidas disciplinarias.

Si con ocasión de proceso disciplinario, se establece la comisión de delitos o violación de derechos de los usuarios, la Oficina de Gestión Humana deberá comunicarlo a las autoridades competentes.

10. POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL

Los mecanismos de control de acceso físico para el personal, no deben permitir el acceso a las instalaciones y áreas restringidas de la EPSI Anas Wayuu a personas no autorizadas, para garantizar la protección de los equipos de cómputo, la fuga de información, y de comunicaciones de la empresa.

a. RESGUARDO Y PROTECCIÓN DE LA INFORMACIÓN

- ✓ La EPSI tendrá actualizado sus herramientas tecnológicas (antivirus, firewall, parches, licencias) como medida tendiente a garantizar la confiabilidad y seguridad de la información y para el buen desarrollo de las funciones de la planta de personal.

- ✓ La Dirección de Aseguramiento, Tecnología y Comunicaciones monitoreara la red permanentemente para validar posibles vulneraciones a la seguridad de la información de forma interna y externa.
- ✓ Los usuarios dando cumplimiento al manual del Sistema de Gestión de la Seguridad de la Información deberán reportar de forma inmediata a la Dirección de Aseguramiento, Tecnología y Comunicaciones cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones y/o la información.
- ✓ Los usuarios no están autorizados a realizar backup sobre dispositivos de almacenamiento portátiles personales, CD-ROM y USB.
- ✓ Es responsabilidad del usuario evitar en todo momento la fuga de la información de la EPSI Anas Wayuu que se encuentre almacenada en los equipos de cómputo que tenga asignados.
- ✓ La Dirección de Aseguramiento, Tecnología y Comunicaciones realiza frecuentemente copias de seguridad de los sistemas de información y de los datos almacenados en los equipos de cómputo, servidores y los resguarda en la nube, lo cual garantiza la disponibilidad de la información en caso de pérdida, corrupción o eliminación accidental.
- ✓ La EPSI Anas Wayuu cuenta con los servicios de Google Cloud, en la cual se encuentra almacenada la información de la entidad, proporcionando así un respaldo que asegure la continuidad del servicio ante posibles fallas, lo cual eleva la confiabilidad y la disponibilidad del sistema al evitar interrupciones significativas.

b. CONTROLES DE ACCESO FÍSICO

Aplicabilidad:

La presente política aplica para todos los colaboradores, terceros, aprendices, practicantes, contratistas y proveedores en todos los niveles de la EPSI Anas wayuu que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la entidad.

- ✓ Conforme a lo declarado en la política general de seguridad de la información la presente política establece los lineamientos que debe cumplir la EPSI Anas wayuu con respecto al control de acceso, bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo.
- ✓ Las computadoras personales, portátiles, módems, y cualquier activo de tecnología de información de propiedad de la entidad, podrán salir de las instalaciones de la EPSI Anas wayuu únicamente con la autorización de salida de la Dirección de Aseguramiento, Tecnología y Comunicaciones y el Técnico de Almacén.

- ✓ La asignación de derechos de acceso operará exclusivamente sobre una base contractual, de forma que será requisito la existencia de una relación contractual vigente entre las partes que determine específicamente que tipo de información va a estar en el dominio de quien suscribe el acuerdo, que acciones realizará sobre esa información y las razones de la misma.

c. SEGURIDAD EN ÁREAS DE TRABAJO

- ✓ Se debe garantizar por la dirección de Aseguramiento, Tecnología y Comunicaciones la seguridad de la red, de acuerdo a los protocolos de cableado estructurado (TIA/EIA 598-A y TIA/EIA 598-B).
- ✓ Mantener la energía regulada para el buen funcionamiento del hardware.
- ✓ Los colaboradores tienen la obligación bloquear sus equipos de cómputo una vez se ausente del mismo, por cualquier motivo.
- ✓ Los colaboradores deberán apagar los equipos de cómputo una vez terminada la jornada laboral.

d. GESTIÓN Y PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN

Para la gestión de los activos de información, los usuarios deben cumplir con lo siguiente:

- ✓ La Dirección de Aseguramiento, Tecnología y Comunicaciones es el responsable de la configuración y parametrización de los equipos de cómputo, dispositivos móviles y todas las herramientas tecnológicas que se adquieran por parte de la EPSI Anas Wayuu.
- ✓ El activo de información asignado, deberá ser para uso exclusivo de las actividades desarrolladas dentro de la EPSI Anas Wayuu y en los casos que exista un desplazamiento fuera de las instalaciones deberá tener la autorización de la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, abrir o desarmar equipos, ni retirar sellos de los mismos; en caso de requerir este servicio deberá solicitarlo por medio del correo electrónico, adjuntando el formato de traslado de equipos de cómputo.
- ✓ Los funcionarios no permitirán el uso del equipo de cómputo a persona ajenas a la EPSI Anas Wayuu.
- ✓ No se podrán consumir alimentos o ingerir bebidas frente a los equipos de cómputo.

- ✓ Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o de la CPU.
- ✓ Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- ✓ Se prohíbe la utilización de cualquier activo de información de la EPSI Anas Wayuu para propósitos de carácter personal.
- ✓ Está prohibido el uso de cualquier activo de información de la EPSI Anas Wayuu, con el fin de infringir cualquier ley local o nacional.
- ✓ Se prohíbe la utilización de cualquier activo de Información de la EPSI Anas Wayuu para guardar o transportar material ilegal, pornográfico o su utilización en actividades no relacionadas con las funciones de su cargo.
- ✓ Se prohíbe utilizar fondos de escritorio o protectores de pantalla no autorizados por la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ Se prohíbe colocar calcomanías y cualquier otro elemento decorativo a los activos de información de la EPSI.
- ✓ Cada responsable debe asear el exterior de sus equipos de cómputo a diario utilizando para ello un paño seco.

e. MANTENIMIENTO DE EQUIPOS DE CÓMPUTO

- ✓ Únicamente el personal autorizado por la Dirección de Aseguramiento, Tecnología y Comunicaciones serán los responsables de los mantenimientos preventivos y correctivos.
- ✓ La Dirección de Aseguramiento, Tecnología y comunicaciones socializara el cronograma de mantenimientos preventivos y correctivos.
- ✓ La instalación del hardware y software será responsabilidad de la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ El traslado de hardware será responsabilidad de la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ Los usuarios deberán informar las incidencias o fallas del hardware o software a la Dirección de Aseguramiento, Tecnología y Comunicaciones, por los medios dispuestos para la resolución de las mismas (Mesa de Ayuda, línea 152).

f. PÉRDIDA DE EQUIPO

- ✓ En casos de pérdida del activo de información la Dirección de Aseguramiento, Tecnología y Comunicaciones deberá informar a la Oficina de Talento Humano para

que adelante las actuaciones pertinentes conforme a lo dispuesto en el reglamento interno del trabajo.

- ✓ Dirección de Aseguramiento, Tecnología y Comunicaciones deberá informar al comité de seguridad de la información sobre la perdida.
- ✓ En caso de hurto o extravío del equipo de cómputo o accesorios bajo su resguardo, el usuario deberá dar aviso inmediato a la Dirección de Aseguramiento, Tecnología y Comunicaciones, Oficina de Gestión Humana y Almacén de la desaparición y presentar la denuncia ante las autoridades competentes.

g. DAÑO DEL EQUIPO

- ✓ El equipo de cómputo o cualquier activo de información que sufra algún daño por uso inadecuado, descuido o negligencia por parte del usuario que resguarda el equipo, la Dirección de Aseguramiento, Tecnología y Comunicaciones deberá generar un informe detallado sobre las causas del incidente, el cual será remitido a la Oficina de Gestión Humana para que se adelante el proceso correspondiente.

11. POLÍTICAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

La Dirección de Aseguramiento, Tecnología y Comunicaciones debe definir y garantizar que estén documentados las responsabilidades para el manejo y tratamiento de la información por las operaciones computacionales y de redes. Así mismo la Dirección de Aseguramiento, Tecnología y Comunicaciones debe definir los controles que permitan monitorear la apropiada operación tecnológica y la seguridad de la información.

a. USO DE MEDIOS DE ALMACENAMIENTO

- ✓ La Dirección de Aseguramiento, Tecnología y Comunicaciones debe garantizar que todos los medios de almacenamiento utilizados en la EPSI Anas Wayuu estén controlados por las herramientas tecnológicas.
- ✓ Está prohibido la utilización de memorias USB, dispositivos de almacenamiento bluetooth, unidades de CD-ROM.

b. INSTALACIÓN DE SOFTWARE

La Dirección de Aseguramiento, Tecnología y Comunicaciones establecerá mecanismos que bloqueen la instalación de software ilegal y el cambio de configuración de los equipos asignados al usuario sin autorización.

- ✓ Los usuarios que requieran la instalación de software que no sea propiedad de la EPSI Anas Wayuu, deberá justificar el uso y solicitar autorización a la Dirección de Aseguramiento, Tecnología y Comunicaciones a través del formato de soporte técnico, firmado por la dirección de su dependencia, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación.
- ✓ Antes de realizar cualquier instalación, se deberán realizar pruebas para determinar el nivel de riesgo asociado a ese software.
- ✓ Todo equipo de cómputo, de propiedad de la organización o alquilado, deberá tener deshabilitada la opción de instalación de software.
- ✓ Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, o cualquier equipo conectado a la red de la EPSI Anas Wayuu, que no esté autorizado por la Dirección de Aseguramiento, Tecnología y Comunicaciones.

c. IDENTIFICACIÓN DE INCIDENTES POR VIRUS O ATAQUES INFORMÁTICOS

- ✓ El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo a la Dirección de Aseguramiento, Tecnología y Comunicaciones lo antes posible por los medios dispuestos para los reportes de incidentes, aportando evidencias y una descripción clara de la incidencia de seguridad informática.
- ✓ La Dirección de Aseguramiento, Tecnología y comunicaciones deberá monitorear el antivirus institucional para mantener las licencias vigentes.

d. ADMINISTRACIÓN DE LA CONFIGURACIÓN

Los usuarios de la EPSI Anas Wayuu no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la EPSI Anas

Wayuu, sin la autorización de la Dirección de Aseguramiento, Tecnología y Comunicaciones.

e. SEGURIDAD PARA LA RED

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Dirección de Aseguramiento, Tecnología y Comunicaciones, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la EPSI Anas Wayuu, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

f. USO DE CORREO ELECTRÓNICO

- ✓ El usuario debe utilizar el correo electrónico de la EPSI Anas Wayuu única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su cargo o comisión, quedando prohibido cualquier otro uso.
- ✓ Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario y/o texto de un correo electrónico.
- ✓ Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- ✓ La oficina de Tecnología y Comunicación promueve y avala únicamente como mecanismos de comunicación electrónicos el uso del correo electrónico y el Chat institucional.
- ✓ La oficina de Tecnología y Comunicación monitoreará periódicamente o por solicitud del comité de gerencia, el contenido de e-mail y los accesos a Internet para verificar la adecuada utilización de este recurso.

g. CONTROLES CONTRA EL CÓDIGO MALICIOSO

- ✓ Para prevenir infecciones por virus informático, los usuarios de la EPSI Anas Wayuu no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ Los usuarios de la EPSI Anas Wayuu deben verificar que la información y los medios de almacenamiento, Discos Compactos (CD), estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Dirección de Aseguramiento, Tecnología y Comunicaciones.

- ✓ Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libre de virus utilizando el software antivirus autorizado antes de ejecutarse.
- ✓ Ningún usuario de la EPSI Anas Wayuu debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas de la EPSI Anas Wayuu. El incumplimiento de este estándar será considerado una falta grave.
- ✓ Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la Dirección de Aseguramiento, Tecnología y Comunicaciones para la detección y erradicación del virus.
- ✓ Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la EPSI Anas Wayuu: Antivirus, Outlook, office, Navegadores u otros programas.

h. USO DE INTERNET

- ✓ El acceso a Internet provisto a los funcionarios de la EPSI Anas Wayuu es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones que desempeña.
- ✓ El acceso a internet para los funcionarios de la EPSI Anas Wayuu, estará limitado de acuerdo a la necesidad de acceso que requiera para el desarrollo de sus funciones.
- ✓ Las solicitudes de inclusión, modificación o eliminación en los privilegios de acceso al uso de internet, se presentará por escrito o mediante correo electrónico a la mesa de ayuda, con la aprobación del director o jefe de proceso y serán revisados y avalados por la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ Los funcionarios de la EPSI Anas Wayuu tienen prohibido el acceso a los siguientes portales o páginas web.

- Páginas de contenido pornográfico.
- Portales de reproducción de música.
- Portales que inducen al terrorismo.
- Portales de piratería informática.
- Emisoras de radio vía internet.
- Portales de juegos, apuestas y sitios de entretenimiento.
- Sitios web que pongan en riesgo la seguridad de la infraestructura tecnológica de la EPSI.

✓ Los funcionarios de la EPSI Anas Wayuu no podrán ingresar sin autorización de la dirección de tecnología y comunicaciones a los siguientes portales o páginas web.

- Redes sociales.
- Portales de reproducción de video.
- Portales de descargas de archivos de audio, video, software o aplicaciones informáticas.

✓ Los servicios y equipos tecnológicos utilizados para el acceso a internet son propiedad de la EPSI Anas Wayuu y la entidad se reserva el derecho de monitorear el acceso y el tráfico de internet de cada equipo de cómputo.

✓ Todos los sitios web y descargas son monitoreados a través del firewall de la EPSI y pueden ser bloqueados en el momento en que la entidad lo requiera o estimen que son dañinos o no productivos para el buen funcionamiento de la EPSI Anas Wayuu.

✓ Los funcionarios no podrán hacer uso de los equipos informáticos a su cargo para realizar a través de internet fraudes informáticos, pirateo de software, películas o música.

✓ Las redes sociales institucionales no podrán ser utilizadas para solicitar, anunciar o publicar información no relacionada con las actividades de la EPSI Anas Wayuu.

i. UNIDAD DE RED

✓ La EPSI Anas Wayuu cuenta con un espacio de transferencia de archivos en red, que está disponible para los empleados. Esta herramienta permite el acceso compartido a archivos y recursos, facilitando la colaboración y la gestión centralizada de datos que generalmente son asignadas a través de una red local (LAN).

- ✓ Las unidades de red compartidas son para la transferencia de información, no para almacenamiento, ya que es responsabilidad de cada persona guardar la información en el equipo de cómputo suministrado por la entidad.
- ✓ El proceso de tecnología y comunicaciones realizará periódicamente la limpieza y/o eliminación de la información almacenada en las unidades de red, lo anterior con el fin de garantizar la disponibilidad de espacio de almacenamiento, optimizando los recursos de la entidad.

12. POLÍTICAS DE CONTROLES DE ACCESO LÓGICO (Sistemas operativos y de información)

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; tales como su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de la EPSI Anas Wayuu, para los cuales deberá garantizar la confidencialidad.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la EPSI Anas Wayuu debe ser proporcionado por el dueño de la información, con base en el principio de la “necesidad de saber” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

a. CONTROLES DE ACCESO LÓGICO

- ✓ Establecer roles y responsabilidades en la seguridad de información según la guía implementada por la EPSI Anas Wayuu.
- ✓ El acceso lógico a la red corporativa y a los sistemas de información de la EPSI Anas Wayuu se hará mediante autenticación de usuario y contraseña.
- ✓ Todos los usuarios de servicios de información son responsables por el usuario y contraseñas que recibe para el uso y acceso de los recursos.
- ✓ Los permisos para el acceso a los sistemas de información de la EPSI Anas Wayuu se asignarán a los funcionarios de acuerdo a la matriz de roles y perfiles por el mismo administrador del sistema de la EPSI.
- ✓ El acceso a los sistemas de información se debe controlar mediante listas de control de acceso y se deben permitir solo los protocolos necesarios para la interacción normal entre usuario y servidor.
- ✓ El acceso de los funcionarios autorizados que desempeñen funciones o roles de gerencia, dirección y coordinación a la red corporativa de la EPSI Anas Wayuu desde sitios ajenos a las instalaciones de la empresa, se deberá hacer por VPN site to client utilizando protocolos seguros para establecer la conexión.

- ✓ Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Dirección de Aseguramiento, Tecnología y Comunicaciones antes de usar la infraestructura tecnológica de la EPSI Anas Wayuu.
- ✓ Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la EPSI Anas Wayuu, salvo que tenga la autorización de la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, igualmente tiene prohibido utilizar las credenciales de otros usuarios.
- ✓ El acceso a la información reservada y confidencial solo se permitirá de acuerdo al rol que desempeñe el funcionario, de acuerdo a la matriz de roles y perfiles.
- ✓ En el caso de archivo físico, el acceso será dado en las instalaciones donde resida dicho archivo de acuerdo al rol y perfil de acceso que tenga el usuario y no estará permitida la extracción parcial o total.
- ✓ Cuando los datos sobre los cuales se esté brindando acceso sean de carácter personal, se deberá suscribir un acuerdo de transferencia y responsabilidad de datos personales.
- ✓ El ajuste y remoción de derechos de acceso será realizado inmediatamente finalice la relación contractual y si es necesaria una etapa de transferencia, tales derechos de acceso estarán a cargo de quien recibe la información.
- ✓ Mensualmente se realizarán actividades de revisión de derechos de acceso a la red corporativa y a los sistemas de información. De ser necesario aplicar algún tipo de ajuste éstos serán realizados de forma inmediata. En el evento que se realicen actualizaciones de la matriz de roles y permisos, la EPSI registrará tal situación en acta.
- ✓ En el evento de presentarse cambios en el contexto (requisitos y contratos) se realizarán las actividades de revisión de derechos de acceso. De ser necesario aplicar algún tipo de ajuste, éstos serán realizados de forma inmediata.

b. ADMINISTRACIÓN Y USO DE CONTRASEÑA

Conforme a lo declarado en la política general de seguridad de la información la presente política establece los lineamientos que debe cumplir la EPSI Anas Wayuu con relación a la creación y uso de contraseñas, bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo.

c. APLICABILIDAD

La presente política aplica para todos los usuarios, aprendices y practicantes en todos los niveles de la EPSI Anas Wayuu que tengan dentro del desarrollo de sus funciones un acceso lógico que implique el uso de un usuario y contraseña para gestionar información de la entidad.

d. LINEAMIENTOS

- ✓ La asignación de contraseña debe ser realizada de forma individual, por lo que el uso de contraseña compartida está prohibido sin importar las circunstancias.
- ✓ Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá levantar una solicitud utilizando los formatos de calidad a la Dirección de Aseguramiento, Tecnología y Comunicaciones para que se le proporcione un nuevo password, una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a la infraestructura tecnológica.
- ✓ Está prohibido que las contraseñas se registren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.
- ✓ Los usuarios tienen la obligación de cambiar sus credenciales de acceso, cada 60 días.
- ✓ Todas las aplicaciones que se utilicen deben tener clave de acceso y establecer perfiles de usuarios para acceder a la información. (Administrador de base de datos y sistemas de información).
- ✓ La Dirección de Aseguramiento, Tecnología y Comunicaciones cambiará inmediatamente la clave de acceso a los empleados o contratistas que tengan ausencias definitivas de sus cargos o terminación de contrato. Para que esto sea posible la Oficina de Gestión Humana debe informar por escrito al Jefe de Tecnología y Comunicaciones sobre la novedad del personal, relacionando claramente los datos de los empleados entrantes y salientes.
- ✓ Cuando un usuario maneje aplicaciones específicas y sea removido de su puesto de trabajo de manera provisional o permanente, deberá hacer entrega formal del equipo a su cargo, las claves de acceso e instruir a su reemplazo en la utilización del software que administra.
- ✓ Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- Deben estar compuestos de al menos ocho (8) caracteres de longitud, deben ser alfanuméricos (números, letras y símbolos o caracteres especiales) dentro de los cuales se deben incluir lo siguiente:

    - Dos Letras Mayúsculas.
    - Dos Números.
    - Un Carácter especial.
    - Las contraseñas de los servicios de red expiran cada 120 días.
    - Los usuarios pueden cambiar en cualquier momento su contraseña, cumpliendo con los parámetros establecidos.

- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario y no deben contener caracteres que expresen listas secuenciales y caracteres de control.

- No deben ser idénticos o similares a contraseñas que hayan usado previamente.

- Se recomienda que las contraseñas institucionales sean diferentes a las personales.

13. POLÍTICAS DE USO DE CONTROLES CRIPTOGRÁFICOS Y CONTROL DE LLAVES

Conforme a lo declarado en la política general del Sistema de Gestión de Seguridad de la Información se establece las reglas con relación a la criptografía, e incluyendo estándares para su implementación, garantizando así con esto la preservación de la confidencialidad e integridad de la misma.

a. APLICABILIDAD

La presente política aplica a todos los sistemas de información de apoyo a procedimientos y actividades de la EPSI Anas Wayuu.

b. LINEAMIENTOS

La EPSI Anas Wayuu empleara la criptografía para los siguientes servicios:

- ✓ Servicios de confidencialidad: utilizando cifrado de información para proteger información sensible o crítica, así sea transmitida o almacenada.

- ✓ Servicios de Integridad/Autenticación: utilizando firmas digitales o códigos de autentificación de mensajes para proteger la autenticidad e integridad de la información crítica o sensible que es almacenada o transmitida.
- ✓ Servicios de Autorización.
- ✓ Servicio de Irrefutabilidad.
- ✓ Uso de firma digital.
- ✓ No Repudio: utilizando técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.
- ✓ El sistema de gestión de salud SGA Software Encripta una cadena mediante un algoritmo no reversible (hash-1).

14. POLÍTICA DE ESCRITORIOS LIMPIOS

Todo usuario de equipos de cómputo de la EPSI Anas Wayuu deberán utilizar los mecanismos institucionales para proteger la información que reside sus estaciones de trabajo, de igual manera deberán proteger la información sensible o confidencial.

Esta política estipula los lineamientos y protocolo que deben seguir los usuarios de equipos de cómputo de la EPSI Anas Wayuu durante las actividades que se realicen tanto dentro como fuera de la entidad, bajo una orientación aplicada a la mejora continua y de la gestión del riesgo.

Los usuarios que hagan o hacen uso de equipos de cómputo de la EPSI Anas Wayuu, deben conocer y aplicar las medidas para la prevención de fuga de información sensible o confidencial.

a. USO DEL ESCRITORIO LIMPIO

- ➢ Los usuarios de equipos de cómputo de la EPSI Anas Wayuu siempre que abandonen su estación de trabajo debe asegurarse de bloquear la computadora con protección de contraseña y adicionalmente guardar en un lugar seguro cualquier documento que contenga información confidencial.
- ➢ Los usuarios de equipos de cómputo de la EPSI Anas Wayuu, deben mantener el escritorio limpio de información de la entidad. Solo debe estar la papelera de reciclaje y los accesos directos de aplicaciones que sean utilizadas para el desempeño de sus labores.
- ➢ Los funcionarios de la EPSI Anas Wayuu cuando abandonen su escritorio al finalizar la jornada laboral, no deben dejar documentos sobre él. Es fundamental que archive

sus documentos aplicando los principios archivísticos del proceso de Gestión Documental.

- Los funcionarios de la EPSI Anas Wayuu cuando impriman un documento deben retirarlo inmediatamente de las bandejas de las impresoras.
- Los funcionarios de la EPSI Anas Wayuu tienen prohibido dejar memos en los escritorios con las contraseñas de acceso a las plataformas tecnológica de la entidad.
- Los funcionarios de la EPSI Anas Wayuu no deben colocar documentos de la entidad en las canecas de basuras sin realizarles el debido proceso de trituración.
- Los funcionarios de la EPSI Anas Wayuu tienen prohibido dejar los dispositivos móviles en los escritorios al ausentarse de él.
- Los funcionarios de la EPSI Anas Wayuu deben borrar las anotaciones consignadas en los tableros (pizarrones) al terminar las juntas o reuniones.

15. POLÍTICA DE COPIA DE RESPALDO

Conforme a lo declarado en la política general de seguridad de la información, la presente política establece los lineamientos que debe cumplir la EPSI Anas Wayuu con respecto a la seguridad, disponibilidad e integridad de la información ante la ocurrencia de un incidente disruptivo del tipo pérdida o alteración de la información, bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo.

a. APLICABILIDAD

La presente política aplica para todos los usuarios, aprendices, y practicantes en todos los niveles de la EPSI Anas Wayuu que tengan dentro del desarrollo de sus funciones un acceso lógico que implique el uso de un usuario y contraseña para gestionar información de la entidad.

16. POLÍTICA DE SEGURIDAD PARA LA TRANSFERENCIA DE INFORMACIÓN

Conforme a lo declarado en la política general de seguridad de la información, la presente política establece los lineamientos que debe cumplir la EPSI Anas Wayuu con respecto a la seguridad de la trasferencia de información durante la ejecución de procesos que

impliquen la transmisión y recepción dentro y fuera de la organización, bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo.

a. APLICABILIDAD

La presente política aplica para todos los usuarios, aprendices, y practicantes en todos los niveles de la EPSI Anas Wayuu que tengan dentro del desarrollo de sus funciones acceso a cualquier tipo de información de la entidad.

- No está permitido que ningún funcionario de la EPSI Anas Wayuu circule con información en medios de almacenamiento externos (memorias USB, CD, DVD, discos duros externos, etc.).

- La transferencia de información digital entre funcionarios, contratistas y en general con los terceros se debe hacer solo por los medios ofrecidos por la EPSI Anas Wayuu para tal fin, tales como herramientas Exchange, One Drive, Share Point, Teams, Google drive.

- No está permitida la transferencia de información por medio de software o herramientas de chat como por ejemplo Skype empresarial.

- Toda transferencia de información (interna o externa, desde o hacia la organización) debe estar identificada contemplando como mínimo conjunto de datos, remitente, destinatario, medio de transferencia y justificación de la misma. Para el caso de transferencias sucesivas, este elemento solo será identificado por única vez a menos que cambie el conjunto de datos.

- Para mantener la integridad de la información la transferencia de datos entre sistemas de información propios y de terceros se debe hacer mediante protocolos seguros.

- No está permitida la transferencia de información reservada, confidencial o de carácter privado fuera del territorio colombiano, lo cual incluye herramientas de acceso compartido ni suites de colaboración.

- Se deben establecer acuerdos de transferencia de información entre la organización y partes externas las cuales deben estar soportadas como mínimo por cláusula de confidencialidad, no divulgación y responsabilidad en el tratamiento de datos

personales. Se deben revisar regularmente y documentar, los requisitos para los acuerdos de confidencialidad y no divulgación de la información para la trasferencia de información entre EPSI Anas Wayuu y partes externas, de acuerdo al contexto y dando cumplimiento a la normatividad vigente aplicable.

- La trasferencia de información de carácter reservado y confidencial no está permitida por medio de correo electrónico, la demás información de la organización transferida por este medio debe estar acompañada por el aviso de confidencialidad y tratamiento de datos personales.

- Todos los equipos de cómputo deberán tener deshabilitados los puertos USB, y la unidad óptica solo cumplirá la función de lectura.

17. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON PROVEEDORES

La EPSI Anas Wayuu, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de políticas que busca establecer un marco de confianza en el ejercicio de los deberes entre la EPSI y los proveedores, enmarcado en el estricto cumplimiento de las leyes.

Todo proveedor usuario de la información de la EPSI Anas Wayuu deberá utilizar los mecanismos institucionales para proteger la información que reside en los activos de almacenamiento de información, igualmente deberá proteger la información sensible o confidencial que por necesidades institucionales se realice por transferencia de archivo.

Esta política establece los lineamientos y protocolos que deben seguir los proveedores usuarios de información de la EPSI Anas Wayuu durante las actividades que se realicen tanto dentro como fuera de la entidad, bajo una capacitación periódica.

a. USO DE LA INFORMACIÓN

- Las responsabilidades frente a la seguridad de la información serán publicadas y aceptadas por cada uno de los proveedores de la EPSI Anas Wayuu.

- La EPSI Anas Wayuu protegerá la información generada, procesada o resguardada por los procesos, del acceso otorgado a los proveedores mediante los acuerdos de voluntades, las cuales deben incorporar requisitos de seguridad de la información, cumplimiento del sistema de gestión de seguridad de la información una vez sea

socializado, cláusula de confidencialidad y la aplicación obligatoria a las acciones relacionadas con su actividad.

- Todo proveedor debe firmar y aplicar el acuerdo de transferencia de información de la EPSI Anas Wayuu.

18. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN GESTIÓN DE PROYECTOS

Conforme a lo declarado en la política general de seguridad de la información, la presente política establece los lineamientos que debe cumplir la EPSI Anas Wayuu en relación con su alcance a proyectos de cualquier tipo, bajo un enfoque aplicado de mejora continua y de gestión integral del riesgo.

a. LINEAMIENTOS

- Todo proyecto deberá incorporar requisitos y riesgos de seguridad de la información que incluya como mínimo la adhesión a las políticas de seguridad de la información, cláusula de confidencialidad y la aplicación de las prácticas que estén relacionadas con su actividad.

- Todo proyecto deberá incorporar mecanismos de seguimiento, medición y control para poder conocer la aplicación de los lineamientos generales y específicos en seguridad de la información.

19. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

La gerencia o directivas de la EPSI Anas Wayuu, debe apoyar activamente la seguridad de la información dentro de la organización, con objetivos claros, y el conocimiento de las responsabilidades de la seguridad de la información, el cual, tiene el compromiso de gestionar bajo un enfoque basado en riesgos de la seguridad de la información.

El comité de seguridad de la información de la EPSI Anas Wayuu, lo integra los siguientes cargos:

- Gerencia.
- Director de Aseguramiento, Tecnología y Comunicaciones.
- Oficial de Cumplimiento (Jefe de Tecnología y Comunicaciones)

El comité de seguridad de la información de la EPSI Anas Wayuu tendrá las siguientes funciones:

- Aprobar las políticas de seguridad de la información y su manual, previa revisión del oficial de cumplimiento.
- Revisar semestralmente el estado general de la seguridad de la información.
- Evaluar los incidentes de seguridad de la información y monitorear el proceso de respuesta.
- Evaluar los proyectos de seguridad de la información.
- Definir roles específicos y responsables del Sistema de Seguridad de la Información.
- Evaluar los controles del sistema de seguridad de la información.

El comité deberá reunirse por lo menos una vez en el año, para revisar las políticas y su manual y cada vez que se requiera para el cumplimiento de sus funciones.

La coordinación del comité estará a cargo del Director de Aseguramiento, tecnología y comunicaciones, quien deberá evaluar previamente todas las iniciativas de las que deba de conocer el comité.

20. INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

La Dirección de Aseguramiento, tecnología y comunicaciones será la responsable de realizar los inventarios de activos de la información, establecer su procedimiento, clasificación y evaluación.

21. SEGURIDAD FÍSICA Y AMBIENTAL

La presente política de control busca prevenir el acceso físico no autorizado, igualmente el daño, la interferencia a la información e instalaciones de procesamiento de la EPSI Anas Wayuu.

Las instalaciones de la EPSI Anas Wayuu, tiene áreas seguras, las cuales deberán estar protegidas por un perímetro de seguridad, y contar con controles ambientales y aquellas otras medidas necesarias para garantizar la confidencialidad, la integridad y disponibilidad de la información.

Se consideran áreas seguras:

- Centro de cómputo, de comunicaciones, cuarto de equipos de todas las sedes de la EPSI Anas Wayuu.
- Cuartos de centro de cableado.
- Áreas de gestión documental, radicación y archivo.
- Área de almacenamiento de archivo.
- Cuartos y plantas eléctricas.
- Cuartos de UPS y banco de baterías.
- Despachos de gerencia, direcciones, gestores.

22. PERÍMETRO DE SEGURIDAD FÍSICA

Las instalaciones de la EPSI Anas Wayuu tienen definidas unas áreas de recepción a la entrada de los edificios, adicionalmente cuentan con el servicio de vigilancia privada; servicio que tiene un Guarda de Seguridad asignado las 24 horas del día, los siete días de la semana, los empleados deben identificarse mediante el carnet de la entidad, en caso de ser un visitante se permite el acceso con autorización de un funcionario de la entidad, registrando el ingreso en el libro de minuta del guarda de seguridad.

El archivo central de la entidad está resguardado por acceso con cerradura de seguridad mecánica.

Los cuartos de comunicaciones, centros de cableado cuentan con un control de acceso con cerradura de seguridad mecánica y solo el personal de Infraestructura y del área de tecnología y comunicaciones están autorizados a ingresar. En caso de ser necesario el ingreso de un proveedor de servicio se debe registrar la actividad y el tiempo de permanencia dentro de esta área.

23. SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES

La EPSI Anas Wayuu para mitigar el riesgo de pérdida de información de sus instalaciones adopta las siguientes medidas:

- El personal de vigilancia de la Entidad, así como el personal de vigilancia del edificio, deben revisar todo bolso o paquetes del personal al ingresar o salir de las instalaciones.

- Todo ingreso de contratistas o visitantes para los fines de semana deberá ser solicitado previamente a la Dirección de Aseguramiento y Tecnología y Comunicaciones, indicando el motivo del requerimiento, en caso de ser autorizado se informará vía correo electrónico a la vigilancia del edificio el ingreso del personal.

- El ingreso del personal en los días no hábiles, deberá ser registrado en la Minuta de control de ingreso y novedades por el guarda de seguridad.

24. GESTIÓN DE OPERACIONES Y COMUNICACIONES

Para asegurar las operaciones que se realizan diariamente con respecto al procesamiento de la información en los sistemas de información, y en las instalaciones de la entidad, la EPSI Anas Wayuu tiene los siguientes controles:

- Se registran los eventos de actividad de usuario en los sistemas de información para tener la trazabilidad de la operación.
- Todas las estaciones de trabajo, computadores de la entidad cuentan con un antivirus licenciado para la detección, prevención y recuperación contra malware.
- A nivel de red, cuenta con firewall y listas de control de acceso para proteger la información y las aplicaciones.
- La EPSI Anas Wayuu en toda cotización, propuesta comercial y contrato requiere una cláusula de confidencialidad y no divulgación para proteger la información de la organización.

25. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La adquisición, desarrollo y mantenimiento de los sistemas de información de EPSI Anas Wayuu, están contratados con terceros los cuales deben cumplir las políticas de seguridad en relación con proveedores y en gestión de proyectos del presente documento.

Para cada proyecto nuevo, mejora sustancial o cambio a los sistemas de información de EPSI Anas Wayuu, se debe ejecutar un análisis de riesgo antes de iniciar.

26. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

La EPSI Anas Wayuu gestiona los incidentes y eventos de seguridad de la información mediante el reporte oportuno de los empleados, terceros, aprendices, practicantes y

proveedores en todos los niveles de la organización y el análisis de la información recolectada del suceso para reducir la afectación negativa de la continuidad de las operaciones de la organización.

Para asegurar un enfoque consistente y eficaz de la comunicación de un incidente de seguridad de la información, se debe seguir el procedimiento de gestión de incidentes del SGSI - Políticas de tratamiento y protección de datos personales.

Para garantizar la protección de datos personales, la EPSI Anas Wayuu cumple con lo estipulado en la Ley 1581 de 2012, el cual tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías, de conformidad al manual de políticas de protección de datos personales.

27. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

a. DERECHOS DE PROPIEDAD INTELECTUAL

- ✓ Está prohibido por las leyes de derechos de autor y por la EPSI Anas Wayuu, realizar, copias no autorizadas de software, ya sea adquirido o desarrollado por la EPSI Anas Wayuu.
- ✓ Los sistemas de información desarrollados por personal interno o externo que controle la Dirección de Aseguramiento, Tecnología y Comunicaciones son catalogados propiedad intelectual de la EPSI Anas Wayuu.
- ✓ Todo equipo de cómputo de propiedad de la EPSI Anas Wayuu o alquilado, será utilizado de forma exclusiva para los fines de la organización y queda prohibido su uso para fines personales.
- ✓ Los empleados de la EPSI Anas Wayuu, deben mantener y mejorar continuamente el inventario de los activos de la información.
- ✓ Todos los empleados deben reportar a la Mesa de Servicios (Help Desk) cualquier evento que pueda afectar la integridad, disponibilidad y confidencialidad de cualquier activo de información de la Entidad.
- ✓ Todas las actividades de administración y operación que se realicen en los activos de información deben ser orientadas a garantizar el correcto cumplimiento de los objetivos de la EPSI Anas Wayuu.

b. REVISIONES DE CUMPLIMIENTO

- ✓ La Dirección de Aseguramiento, Tecnología y Comunicaciones realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Usuarios.
- ✓ La Dirección de Aseguramiento, Tecnología y Comunicaciones podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan.
- ✓ El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad de Personal.
- ✓ Los responsables de los procesos establecidos en la EPSI Anas Wayuu deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

c. VIOLACIONES DE SEGURIDAD INFORMÁTICA

- ✓ Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática, salvo que medie autorización de la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ Está prohibido realizar pruebas a los controles de los diferentes elementos de Tecnología de Información. Ninguna persona puede probar o intentar comprometer los controles internos, salvo que medie autorización de la Dirección de Aseguramiento, Tecnología y Comunicaciones, con excepción de, los Órganos Fiscalizadores.
- ✓ Ningún usuario de la EPSI Anas Wayuu debe intentar probar fallas de la Seguridad Informática identificadas o conocidas, salvo que sea autorizado las pruebas y aprobadas por la Dirección de Aseguramiento, Tecnología y Comunicaciones.
- ✓ No se debe escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir intencionalmente cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño, acceso a las computadoras, redes o información de la EPSI Anas Wayuu.

28. CONTROL DE CAMBIOS

VERSIÓN	PAGINAS	FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN DEL CAMBIO
1.0	Veintisiete (27)	21/Oct/2015	Creación de las políticas y estándares de seguridad
2.0	Treinta (30)	12/sep./2016	Circular externa 016 de 2016
3.0	Treinta y cinco (35)	12/dic/2017	Normatividad vigente
4.0	Cuarenta y tres (43)	11/ene/2018	Ajustes según Plan de mitigación de Riesgos
5.0	Cuarenta y uno (41)	10/Oct/2018	Logo
5.1	Cuarenta y uno (41)	13/Abr/2022	Corrección de numeral repetido (Numeral 11) y ajuste de la matriz del marco normativo
6.0	Cuarenta (40)	06/09/2023	Adición de ítems (Numeral 9.1) y Actualización del Glosario y de Dirección de Soporte Estratégico a Oficina de Gestión Humana