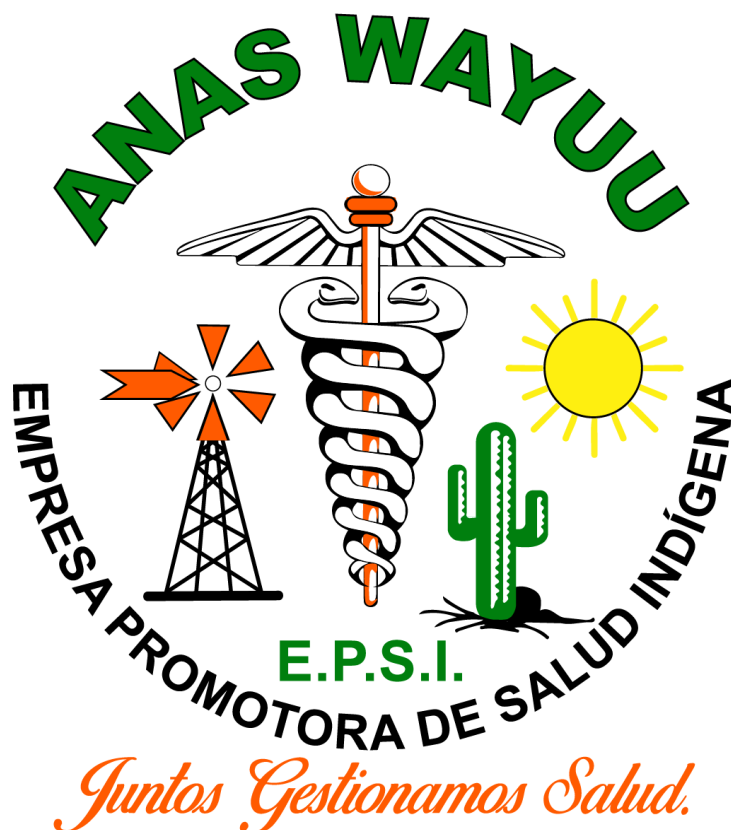


MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



Maicao, La Guajira

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	2 de 32		

CONTENIDO

1. OBJETIVO	4
2. ALCANCE.....	4
3. DEFINICIONES.....	4
4. MARCO DE POLÍTICAS.....	5
4.1 CREACIÓN DE POLÍTICAS	5
4.2 ACTUALIZACIÓN DE POLÍTICAS.....	5
4.3 APROBACIÓN DE POLÍTICAS	6
4.4 NOMBRE DE LAS POLÍTICAS	6
4.5 ESTRUCTURA DE LAS POLÍTICAS	6
5. DIRECTRICES	6
5.1 GOBERNANZA Y CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN	7
5.1.1 Funciones y responsabilidades en materia de seguridad de la información.....	7
5.1.2 Segregación de funciones	9
5.1.3 Responsabilidades de gestión	9
5.1.4 Contacto con las autoridades y grupos de interés especiales	10
5.1.5 Seguridad de la información en la gestión de proyectos	11
5.2 CUMPLIMIENTO LEGAL Y PROTECCIÓN DE LA INFORMACIÓN	12
5.2.1 Requisitos legales, reglamentarios y contractuales.....	12
5.2.2 Derechos de Propiedad Intelectual	13
5.2.3 Protección de los registros	13
5.2.4 Protección de los sistemas de información durante las pruebas de auditoría .	14
5.2.5 Cumplimiento de las políticas, reglas y normas de seguridad de la información	15
5.2.6 Revisión independiente de la seguridad de la información	17
6. POLÍTICAS	18
6.1 POLÍTICA USO DE CIFRADO	18
6.2 POLÍTICA PARA LA GESTIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.....	18
6.3 GESTIÓN DE ACTIVOS.....	19

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	3 de 32		

6.3.1 Política de gestión de activos	19
6.3.2 Política de transferencia de información.....	20
6.3.3 Política de uso aceptable de la información y otros activos asociados.....	21
6.4 GESTIÓN DE AMENAZAS Y VULNERABILIDADES	22
6.4.1 Procedimiento para la gestión de vulnerabilidades técnicas	22
6.4.2 Política de inteligencia contra amenazas y protección contra malware	22
6.5 GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23
6.6 POLÍTICA DE CONTROL DE ACCESO Y GESTIÓN DE LA IDENTIDAD	24
6.7 PROTECCION DE LA INFORMACION	24
6.7.1 Política de dispositivos del usuario.....	24
6.7.2 Política de trabajo y acceso remoto.....	25
6.8 POLÍTICA PARA EL DESARROLLO SEGURO.....	26
6.9 SEGURIDAD DE LAS RELACIONES CON LOS PROVEEDORES.....	27
6.9.1 Política de seguridad de la información de los servicios en la nube.....	27
6.9.2 Política para la seguridad de las relaciones con los proveedores	27
6.10 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS	28
6.10.1 Seguridad física.....	28
7. DECLARACIÓN DE APLICABILIDAD	29
8. MATERIALES NECESARIOS	29
9. DOCUMENTOS Y REGISTROS ASOCIADOS	30
10. RESPONSABLE DE SOCIALIZACIÓN.....	30
11. RESPONSABLE DE EJECUCIÓN.....	31
12. CONTROL DE CAMBIOS.....	31

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	4 de 32		

1. OBJETIVO

Establecer un marco formal para la protección de los activos de información de la EPSI Anas Wayuu, garantizando la confidencialidad, integridad y disponibilidad de dichos activos. Este documento proporciona las directrices necesarias para gestionar riesgos, cumplir con los requisitos legales y reglamentarios aplicables, y fomentar una cultura de seguridad dentro de la organización. Asimismo, busca alinear las prácticas de seguridad de la información con los objetivos estratégicos de la empresa, promoviendo una gestión eficaz y el fortalecimiento de la confianza de todas las partes interesadas.

2. ALCANCE

El presente manual de políticas de seguridad de la información es aplicable a todas las áreas y procesos de la EPSI Anas Wayuu que intervienen en el ciclo de vida de la información, abarcando desde su creación y almacenamiento, hasta su transmisión, modificación, uso, eliminación y respaldo, incluyendo sus activos de información, infraestructura tecnológica, sistemas de comunicación, aplicaciones, bases de datos y cualquier otro recurso relacionado con el manejo de la información.

Las políticas definidas en este manual son de cumplimiento obligatorio para todos los empleados, contratistas, proveedores y partes interesadas que tengan acceso a la información de la EPSI Anas Wayuu, sin excepción. Adicionalmente, el alcance del manual incluye las instalaciones físicas de la empresa, así como cualquier infraestructura externa utilizada para el tratamiento de la información, incluyendo servicios en la nube y entornos remotos, esto con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información en todo momento.

3. DEFINICIONES

- **Activo de Información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	5 de 32		

- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

4. MARCO DE POLÍTICAS

El marco de políticas proporciona una estructura básica para gestionar la seguridad y privacidad de la información de manera efectiva y garantizar la protección de los activos de información y otros activos asociados, adaptado a las necesidades y contexto específico de la EPSI Anas Wayuu, considerando sus riesgos, recursos, requisitos legales y regulatorios.

La política de seguridad y privacidad de la información se sustenta en una variedad de políticas específicas por temas relacionadas con aspectos de seguridad y privacidad de la información. Algunas de estas se presentan en la NTC ISO/IEC 27002.

4.1 CREACIÓN DE POLÍTICAS

Las políticas de la EPSI Anas Wayuu son creadas por los procesos responsables de las mismas, con el acompañamiento del Sistema de Gestión de Seguridad de la Información-SGSI.

4.2 ACTUALIZACIÓN DE POLÍTICAS

Cualquier modificación a las políticas debe ser dirigida por los líderes de proceso, al Director de Aseguramiento y Tecnología y el proceso de calidad.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	6 de 32		

4.3 APROBACIÓN DE POLÍTICAS

Las políticas de la EPSI Anas Wayuu son aprobadas por los líderes de proceso con base en las recomendaciones del responsable de Seguridad de la Información, el proceso de calidad y el Director de Aseguramiento y Tecnología quien posteriormente las presentará ante el Comité de Seguridad y Privacidad de la Información para su respectiva aprobación.

4.4 NOMBRE DE LAS POLÍTICAS

Se hará referencia a las políticas de seguridad y privacidad de la información relacionadas al Anexo de la NTC IEC 27001 y NTC IEC 27701.

4.5 ESTRUCTURA DE LAS POLÍTICAS

La estructura de las políticas de seguridad de la información es:

- Título de la política.
- Portada.
- Encabezado.
- Pie de página.
- Tabla de contenido.
- Objetivo.
- Alcance.
- Definiciones.
- Marco legal.
- Generalidades.
- Control de cambios.

5. DIRECTRICES

La sección de Directrices Generales tiene como objetivo establecer un marco fundamental para garantizar una gestión integral, responsable y alineada con los principios de seguridad de la información. Estas directrices abarcan aspectos clave relacionados con la asignación de funciones, el cumplimiento de requisitos legales y contractuales, la gestión de derechos

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	7 de 32		

y registros, así como la interacción con actores internos y externos esenciales para la seguridad organizacional.

Esta sección aborda controles específicos del Anexo A de la norma ISO/IEC 27001:2022, que incluyen responsabilidades claras de las partes interesadas, la segregación de funciones para reducir riesgos, la protección adecuada de los registros y derechos de propiedad intelectual, y la revisión independiente de las prácticas de seguridad. También se incluyen lineamientos para asegurar el cumplimiento continuo de las políticas y normas establecidas, así como la interacción efectiva con autoridades y grupos de interés especializados.

Adicionalmente, se contemplan las medidas necesarias para proteger los sistemas de información durante las pruebas de auditoría, con el fin de garantizar que estas actividades se lleven a cabo de forma segura y alineada con los objetivos de la organización.

Estas directrices proporcionan las bases para fortalecer el Sistema de Gestión de Seguridad de la Información, promoviendo prácticas responsables y una cultura organizacional que priorice la protección de los activos de información en todo momento.

5.1 GOBERNANZA Y CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

La EPSI Anas Wayuu establece las bases para una gestión estratégica y responsable de la seguridad de la información en la organización. A través de estas directrices, se aseguran que existan roles y responsabilidades asignadas, así como el cumplimiento de normativas legales y contractuales, y se promueve la protección de activos clave como registros y derechos de propiedad intelectual. Además, se refuerzan las relaciones con autoridades y grupos de interés, y se garantiza la realización de auditorías y revisiones independientes para impulsar la mejora continua y la alineación con los objetivos organizacionales.

5.1.1 Funciones y responsabilidades en materia de seguridad de la información

La asignación de las funciones y responsabilidades de seguridad de la información se debe realizar de acuerdo con la política de seguridad de la información y las políticas específicas de cada tema presentes en este manual. La organización debe definir y gestionar las responsabilidades de:

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	8 de 32		

- Protección de la información y otros activos asociados.
- Llevar a cabo procesos específicos de seguridad de la información.
- Actividades de gestión de riesgos de seguridad de la información y, en particular, aceptación de riesgos residuales.
- Todo el personal que utilice la información de una organización y otros activos asociados.

Estas responsabilidades se deben complementar, cuando sea necesario, con una guía más detallada para sitios específicos e instalaciones de procesamiento de información. Las personas con responsabilidades asignadas en materia de seguridad de la información pueden asignar tareas de seguridad a otras personas. Sin embargo, siguen siendo responsables y deben determinar que cualquier tarea delegada se ha realizado correctamente.

La responsabilidad a nivel directivo de la seguridad de la información estará en cabeza de la Gerencia.

La responsabilidad funcional en seguridad de la información recaerá en el rol definido como director de aseguramiento y tecnología, quien es responsable de generar, monitorear, documentar y comunicar los requerimientos en materia de seguridad de la información en la organización.

Se define el rol de Custodio del Activo de información quien tendrá la responsabilidad de mantener el adecuado control de seguridad y de clasificación de los activos asignados. Si bien las posibles implementaciones de los controles específicos que se requieran podrían delegarse a terceros, la responsabilidad seguirá siendo del Custodio del Activo de información.

Todo el personal, incluyendo a los usuarios de la información y a los operadores de los sistemas de procesamiento, debe conocer, difundir, adherirse y garantizar la observancia de la Política de Seguridad de la Información vigente.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	9 de 32		

5.1.2 Segregación de funciones

La EPSI Anas Wayuu establece que se deben separar las obligaciones y áreas de responsabilidad para:

- Inicio, aprobación y ejecución de un cambio.
- Solicitud, aprobación y aplicación de los derechos de acceso.
- Diseño, implementación y revisión del código.
- Desarrollo de software y administración de sistemas de producción.
- Utilización y administración de aplicaciones.
- Utilización de aplicaciones y administración de bases de datos.
- Diseño, auditoría y garantía de los controles de seguridad de la información.

La separación de obligaciones como principio se debe aplicar siempre que sea posible y factible. Cuando sea difícil separar, se deben considerar otros controles, como el seguimiento de las actividades y la supervisión de la dirección.

En entornos con un gran volumen de roles, la EPSI Anas Wayuu debería considerar la implementación de un motor de reglas automatizado o un sistema de gestión de identidades y accesos (IAM). Estas herramientas son fundamentales para la detección y remediación de conflictos, facilitando la validación de políticas de acceso y la auditoría de permisos.

5.1.3 Responsabilidades de gestión

El objetivo es garantizar que todo el personal sea consciente y cumpla con sus responsabilidades en materia de seguridad de la información.

La dirección tiene la responsabilidad de garantizar que el personal:

- Se encuentre debidamente informados sobre sus roles y responsabilidades de seguridad de la información antes de que se le conceda acceso a la información de la organización y a otros activos asociados.
- Se proporcionan orientaciones que indican las expectativas de seguridad de la información de su role dentro de la organización.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	10 de 32		

- Tienen el mandato de cumplir la política de seguridad de la información y las políticas específicas de la organización;
- Lograr un nivel de sensibilización sobre la seguridad de la información pertinente para sus roles y responsabilidades dentro de la organización;
- El cumplimiento de los términos y condiciones de empleo, contrato o acuerdo, que comprende la política de seguridad de la información de la organización y los métodos de trabajo apropiados;
- Se les proporcionan recursos adecuados y tiempo de planificación de proyectos para implementar los procesos y controles relacionados con la seguridad de la organización.

Nadie podrá alterar, eliminar o deshabilitar bajo ningún propósito, cualquiera de los controles de seguridad técnicos y administrativos dispuestos para la protección de su información e infraestructura. Las excepciones legítimas deben ser autorizadas formalmente por el Director de Aseguramiento y Tecnología.

Todos los colaboradores tendrán la responsabilidad de notificar cualquier evento que viole las políticas de seguridad de la información o cualquier actividad sospechosa que atente contra la seguridad de los activos de información de la compañía.

La organización y todos sus miembros deberán respetar las leyes y normatividad vigente relacionadas con los derechos de autor, delitos informáticos, comercio electrónico, entre otras aplicables durante su trabajo en la entidad.

Los usuarios no podrán utilizar al interior ningún tipo de dispositivo de hardware que no les haya sido provisto formalmente por la EPSI Anas Wayuu para el desarrollo de su trabajo. Las excepciones deben ser solicitadas formalmente por cada director de área, donde se indique claramente la justificación del requerimiento y contar con el visto bueno del Director de Aseguramiento y Tecnología.

5.1.4 Contacto con las autoridades y grupos de interés especiales

Como parte de las directrices de gobernanza, la EPSI Anas Wayuu establece procedimientos claros para el contacto y la comunicación con las autoridades y competentes en materia de seguridad de la información. Este control tiene como objetivo

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	11 de 32		

garantizar que, en caso de incidentes, investigaciones u otros eventos relevantes, se pueda interactuar con las autoridades de manera eficiente, cumpliendo con los requisitos legales y reglamentarios aplicables.

Para ello, la EPSI Anas Wayuu dispone de un documento auxiliar titulado "Listado de Contacto de Autoridades y Grupos de Interés Especial", en el cual se recopilan los datos de contacto actualizados de las autoridades pertinentes y otras organizaciones relevantes.

La actualización y mantenimiento de este listado es responsabilidad del Director de Aseguramiento y Tecnología. Adicionalmente, se debe garantizar que los datos sean accesibles únicamente a personal autorizado y que se realicen revisiones periódicas para asegurar su precisión.

Cualquier interacción con las autoridades debe ser documentada y gestionada según los procedimientos establecidos en el marco del Sistema de Gestión de Seguridad de la Información (SGSI), priorizando siempre la transparencia, la confidencialidad y el cumplimiento normativo.

5.1.5 Seguridad de la información en la gestión de proyectos

En la EPSI Anas Wayuu, la gestión de proyectos incorpora medidas de seguridad de la información desde las etapas iniciales, con el objetivo de garantizar la protección de los activos de información en todas las fases del ciclo de vida del proyecto. Este enfoque contribuye a minimizar riesgos, proteger datos sensibles y alinear las iniciativas con los objetivos estratégicos de seguridad de la organización.

Para cada proyecto, se deben identificar y documentar los requisitos de seguridad de la información en función de su alcance, naturaleza y nivel de criticidad. Estas medidas incluyen, pero no se limitan a:

- **Evaluación de riesgos:** Identificar, evaluar y mitigar los riesgos relacionados con la información y los sistemas utilizados o generados durante el proyecto.
- **Asignación de responsabilidades:** Designar roles específicos para la gestión de la seguridad de la información dentro del equipo del proyecto.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	12 de 32		

- **Control de acceso:** Garantizar que los accesos a la información relacionada con el proyecto estén restringidos a personal autorizado.
- **Cumplimiento normativo:** Asegurar que los proyectos cumplan con las políticas internas y las regulaciones externas aplicables en materia de seguridad de la información.

El cumplimiento de estas directrices será supervisado por el Director de Aseguramiento y Tecnología y deberá integrarse como parte de las revisiones periódicas del proyecto. Además, los aprendizajes derivados de los proyectos finalizados se documentarán como lecciones aprendidas para reforzar las prácticas futuras.

5.2 CUMPLIMIENTO LEGAL Y PROTECCIÓN DE LA INFORMACIÓN

La siguiente sección aborda las directrices esenciales para garantizar que la EPSI Anas Wayuu cumpla con los requisitos legales, reglamentarios y contractuales aplicables, así como con las políticas internas y estándares de seguridad de la información. En este apartado se incluyen medidas para proteger los derechos de propiedad intelectual, salvaguardar registros críticos y asegurar que los sistemas de información estén debidamente protegidos durante actividades como auditorías. Estas directrices refuerzan el compromiso de la entidad con la conformidad normativa, la protección de activos y el mantenimiento de la integridad del Sistema de Gestión de Seguridad de la Información.

5.2.1 Requisitos legales, reglamentarios y contractuales

La EPSI Anas Wayuu está comprometida con el cumplimiento de todos los requisitos legales, reglamentarios y contractuales aplicables a la seguridad de la información, asegurando la alineación con las normativas locales, nacionales e internacionales. Este control establece la necesidad de identificar, documentar y monitorear las leyes y regulaciones relevantes, tales como normativas de protección de datos personales, legislación sobre ciberseguridad y cláusulas contractuales específicas relacionadas con la protección de la información.

Para garantizar su cumplimiento, la EPSI Anas Wayuu:

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	13 de 32		

- Mantiene un registro actualizado de todos los requisitos legales y reglamentarios aplicables el cual se puede constatar en el Listado maestro de documentos.
- Realiza revisiones periódicas para identificar cambios en el marco normativo y su impacto en el Sistema de Gestión de Seguridad de la Información (SGSI).
- Asegura que las obligaciones contractuales sean evaluadas y cumplidas como parte de los acuerdos con socios y proveedores.

5.2.2 Derechos de Propiedad Intelectual

La EPSI Anas Wayuu también reconoce la importancia de proteger los derechos de propiedad intelectual, tanto propios como de terceros, en todos los procesos relacionados con la seguridad de la información. Este control busca garantizar el uso legal y ético de activos digitales e intelectuales, previniendo violaciones de derechos de autor y respetando licencias de software, patentes y marcas registradas.

Para ello, la EPSI Anas Wayuu:

- Asegura el registro de la propiedad intelectual de la organización.
- Asegura que todos los empleados, contratistas y proveedores cumplan con las políticas internas respecto al uso de software con licencia y la manipulación de contenido protegido por derechos de autor.
- Desarrolla procedimientos para el monitoreo del uso correcto de software y contenido digital, minimizando el riesgo de infracciones.
- Realiza capacitaciones periódicas sobre la gestión adecuada de derechos de propiedad intelectual, enfatizando la responsabilidad de cada miembro de la organización.

5.2.3 Protección de los registros

La protección de los registros es un componente fundamental del Sistema de Gestión de Seguridad de la Información en la EPSI Anas Wayuu. Este control tiene como objetivo asegurar que los registros críticos, tanto físicos como digitales, estén protegidos contra pérdida, alteración, acceso no autorizado y destrucción, cumpliendo con los requisitos legales, regulatorios y operativos aplicables.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	14 de 32		

Para garantizar la protección efectiva de los registros, la EPSI Anas Wayuu implementa las siguientes directrices:

- Los registros se clasifican en función de su nivel de sensibilidad, importancia operativa y requisitos legales.
- Esta clasificación permite establecer controles específicos para cada categoría de registro.
- Los registros físicos se almacenan en instalaciones seguras con acceso restringido, como archivos protegidos por cerraduras o áreas de almacenamiento controladas.
- Los registros digitales se almacenan en sistemas que cuentan con mecanismos de seguridad avanzados, incluyendo el cifrado y controles de acceso basados en roles.
- Solo el personal autorizado puede acceder a los registros, siguiendo un esquema de permisos definido y documentado.
- Se implementan mecanismos de autenticación para acceder a los registros digitales, como contraseñas seguras y autenticación multifactor (MFA).
- Los registros se mantienen durante el tiempo especificado en las políticas de retención de la organización, cumpliendo con los requisitos legales y contractuales.
- Una vez que un registro ha cumplido su ciclo de vida útil, se elimina de manera segura, utilizando procedimientos aprobados para el borrado seguro de datos.
- Los registros críticos son respaldados periódicamente para prevenir su pérdida en caso de incidentes. Los respaldos se almacenan en ubicaciones seguras, separadas de los registros originales.
- Se realizan pruebas regulares de recuperación para garantizar que los respaldos sean efectivos y puedan restaurarse en caso de necesidad.

Estas medidas garantizan la integridad, confidencialidad y disponibilidad de los registros, fortaleciendo la postura de seguridad de la EPSI Anas Wayuu y asegurando el cumplimiento con los requisitos normativos y operativos.

5.2.4 Protección de los sistemas de información durante las pruebas de auditoría

Durante la ejecución de pruebas de auditoría, es fundamental garantizar que los sistemas de información mantengan su integridad, confidencialidad y disponibilidad en todo

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	15 de 32		

momento. Este control establece directrices para proteger los activos de información durante estas actividades en la EPSI Anas Wayuu.

Para implementar este control, la EPSI Anas Wayuu adopta las siguientes medidas:

- Se limita el acceso a los sistemas de información únicamente a los auditores y personal autorizado involucrado en el proceso, siguiendo estrictos esquemas de autenticación y control de acceso.
- Se documentan todos los accesos realizados durante las auditorías para garantizar transparencia y trazabilidad.
- Antes de iniciar cualquier prueba, se garantizan los respaldos de los sistemas afectados para prevenir la pérdida o alteración de datos durante la auditoría.
- Cuando sea posible, las auditorías se ejecutan en entornos de prueba o simulación, minimizando riesgos para los sistemas en producción.
- Se asegura que los datos sensibles utilizados en las pruebas estén anonimizados o cifrados para proteger su confidencialidad.
- El área de tecnología supervisa las pruebas para garantizar que se ejecuten dentro de los acuerdos establecidos.
- Se establecen canales claros de comunicación entre los auditores y el área de tecnología, para coordinar cualquier intervención o ajuste necesario sin afectar la estabilidad de los sistemas.
- Al finalizar la auditoría, se realiza una revisión para identificar posibles impactos en los sistemas y se asegura la corrección de cualquier vulnerabilidad detectada.
- Se documentan los hallazgos y aprendizajes para fortalecer futuras auditorías.

5.2.5 Cumplimiento de las políticas, reglas y normas de seguridad de la información

El cumplimiento de las políticas, reglas y normas de seguridad de la información es un principio fundamental en la EPSI Anas Wayuu para garantizar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) y el alineamiento con los objetivos organizacionales.

La EPSI Anas Wayuu establece las siguientes directrices:

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	16 de 32		

1. Difusión de políticas y normas:

- Las políticas, reglas y normas de seguridad de la información son comunicadas de manera efectiva a todos los empleados, contratistas y terceros relevantes.
- Se realizan sesiones periódicas de sensibilización y formación para garantizar la comprensión y aplicación de estas normas.

2. Supervisión y monitoreo:

- La aplicación de las políticas y normas es monitoreada a través de auditorías internas regulares, verificando el cumplimiento en todas las áreas de la organización.
- Se utilizan herramientas de monitoreo y registro para rastrear actividades y detectar posibles incumplimientos.

3. Gestión de incumplimientos:

- Se establecen procedimientos específicos para abordar y corregir incumplimientos de políticas o normas, incluyendo la realización de análisis de causas raíz y la implementación de acciones correctivas.
- Las violaciones graves se gestionan de acuerdo con el reglamento interno de la organización y las disposiciones legales aplicables.

4. Responsabilidad y revisión:

- La alta dirección asume la responsabilidad última del cumplimiento de las políticas y normas, supervisando el desempeño del SGSI y asegurando los recursos necesarios.
- Las políticas y normas se revisan periódicamente para garantizar su vigencia y alineación con los cambios en el contexto normativo o del entorno de la organización.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	17 de 32		

Estas medidas reflejan el compromiso de la EPSI Anas Wayuu con la mejora continua y el cumplimiento normativo, asegurando que sus procesos operativos y estratégicos se realicen bajo un marco de seguridad estructurado y transparente.

5.2.6 Revisión independiente de la seguridad de la información

La revisión independiente de la seguridad de la información debe garantizar que el Sistema de Gestión de Seguridad de la Información (SGSI) sea eficaz, cumpla con los requisitos establecidos y se alinee con los objetivos estratégicos de la organización.

La EPSI Anas Wayuu establece las siguientes directrices:

1. Periodicidad de las revisiones:

- Las revisiones independientes se realizan con una frecuencia definida (por ejemplo, anual o semestral) o en función de eventos clave, como cambios significativos en el SGSI, auditorías internas o incidentes de seguridad relevantes.

2. Rol de los revisores:

- Las revisiones deben ser realizadas por auditores internos que no estén directamente involucrados en la operación del SGSI o por entidades externas especializadas en seguridad de la información.
- Los revisores deben poseer las competencias necesarias y un conocimiento adecuado de los estándares aplicables, como la norma ISO/IEC 27001.

3. Objetivos de la revisión:

- Verificar el cumplimiento de las políticas, controles y procedimientos de seguridad de la información.
- Evaluar la eficacia de las medidas de control implementadas.
- Identificar brechas de seguridad y oportunidades de mejora.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	18 de 32		

4. Metodología de la revisión:

- Se aplica un enfoque sistemático basado en estándares como ISO/IEC 27001 de 2022.
- La revisión abarca entrevistas, análisis de documentación, pruebas de controles y evaluación del cumplimiento con las políticas internas.

5. Gestión de resultados:

- Los hallazgos de la revisión se documentan en un informe detallado que incluye observaciones, recomendaciones y acciones correctivas necesarias.

6. POLÍTICAS

Anas Wayuu EPSI establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los colaboradores, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

6.1 POLÍTICA USO DE CIFRADO

La política de uso de cifrado, establece directrices claras para proteger la confidencialidad, integridad y autenticidad de la información mediante el uso adecuado de técnicas criptográficas. Aplica a todos los actores de la organización e incorpora lineamientos normativos como la ISO/IEC 27001, 27002 y 27005, así como el modelo de seguridad y privacidad del MinTIC. Se definen criterios para el uso de cifrado en dispositivos, almacenamiento y transmisión de datos, y se abordan aspectos como la gestión, revocación, recuperación y destrucción de claves, asegurando su protección frente a accesos no autorizados.

6.2 POLÍTICA PARA LA GESTIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

La política PO-860-14 Política de Gestión de Continuidad de la Seguridad de la Información, establece estrategias y procedimientos para garantizar la operación continua de los

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	19 de 32		

procesos críticos frente a interrupciones. Fundamentado en las normas ISO 22301 e ISO/IEC 27001, contempla un análisis integral del negocio en el contexto de la seguridad de la información, identificando procesos esenciales, riesgos asociados, infraestructura crítica, y personal clave. El objetivo principal es minimizar el impacto ante incidentes y asegurar la prestación ininterrumpida de servicios a clientes internos y externos.

La política incluye herramientas como el Catálogo de Continuidad y disponibilidad y la evaluación de riesgos para establecer prioridades de recuperación. También contempla estrategias de recuperación, roles y responsabilidades, así como esquemas de organización en equipos. Además, define procedimientos específicos para cada fase del incidente: alerta, transición, recuperación y retorno a la normalidad, asegurando trazabilidad y control.

Herramientas que apoyan la Política:

- PD-860-10 Procedimiento de Gestión de la Capacidad.
- PL-860-01 Plan de Gestión de la Capacidad.
- FO-860-26 Catálogo De Continuidad y Disponibilidad.

6.3 GESTIÓN DE ACTIVOS

6.3.1 Política de gestión de activos

La PO-860-05 Política de Activos de Información tiene como finalidad asegurar que toda la información y los activos asociados sean identificados, clasificados, protegidos y gestionados de manera adecuada durante su ciclo de vida. Esta política aplica a colaboradores y terceros que accedan o administren activos informativos de la organización, sin importar su formato (físico, digital, voz, etc.). Se establece la obligación de mantener un inventario actualizado, preciso y clasificado de activos, gestionado por propietarios designados, quienes son responsables de su protección, uso y control, según lo definido en la GA-860-01 Guía de Identificación y Clasificación de Activos. Asimismo, se abordan aspectos como el uso aceptable, la devolución de activos, el marcado, el almacenamiento seguro, la eliminación controlada y la trazabilidad documental.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	20 de 32		

La política también enfatiza que toda clasificación debe considerar la confidencialidad, integridad y disponibilidad de la información, con base en su valor, sensibilidad y criticidad. Se exige el cumplimiento de protocolos definidos para el etiquetado, devolución y eliminación de información, incluyendo dispositivos físicos, credenciales, copias impresas y soportes digitales. Las responsabilidades están claramente asignadas a los propietarios, custodios y usuarios de los activos, quienes deben cumplir con los lineamientos establecidos y reportar cualquier irregularidad a las autoridades competentes.

Herramientas que apoyan la Política de Activos de Información:

- GA-860-01 Guía de Identificación y Clasificación de Activos.
- MT-860-06 Matriz de Activos de Información.
- FO-860-03 Formato de Entrega y Devolución de Activos.
- MT-860-08 Matriz de Roles, Responsabilidades y Autoridades.
- PD-860-11 Procedimiento para la Eliminación Segura de Datos y Activos.

6.3.2 Política de transferencia de información

La PO-860-07 Política de Transferencia de Información establece las medidas necesarias para garantizar la protección de la información durante su transmisión, independientemente del medio utilizado: electrónico, físico o verbal. Esta política es de cumplimiento obligatorio para todos los colaboradores, contratistas y terceros que participen en procesos que impliquen intercambio de datos. El objetivo principal es salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información conforme a su clasificación y nivel de criticidad, tal como lo exige el Sistema de Gestión de Seguridad de la Información (SGSI).

En cuanto a las transferencias electrónicas, la política establece controles técnicos específicos, como la segmentación de redes, el uso de dispositivos perimetrales y la separación entre redes internas y externas. También se prohíbe expresamente el uso de canales inseguros como mensajes SMS o mensajería instantánea para la transmisión de información sensible. Se exige la autenticación del usuario y la protección contra malware mediante herramientas institucionales, además de restringir los puertos de diagnóstico y exigir el monitoreo activo de accesos y comunicaciones.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	21 de 32		

Respecto a las transferencias físicas y verbales, la política requiere el cumplimiento de los procedimientos de archivo para el manejo documental y promueve prácticas seguras para la comunicación oral de datos confidenciales. Por ejemplo, se recomienda evitar conversaciones en lugares públicos, no dejar mensajes sensibles en contestadores automáticos y advertir a los asistentes de reuniones sobre el carácter reservado de la información que se va a compartir. Estas disposiciones buscan prevenir accesos indebidos, filtraciones accidentales y garantizar que toda transferencia esté protegida bajo principios de seguridad digital.

6.3.3 Política de uso aceptable de la información y otros activos asociados

La política PO-860-06 Política de Uso Aceptable de la Información y Activos Asociados, establece las reglas y responsabilidades para el uso adecuado de los activos de información y recursos tecnológicos en la organización. Se definen prácticas obligatorias relacionadas con el uso de hardware y software, donde se prohíbe expresamente la modificación, intercambio o instalación no autorizada de dispositivos, y se requiere que toda instalación sea gestionada por el área de Tecnología. Solo se permite el uso de software previamente licenciado y aprobado por la organización, aplicando el principio de mínimo privilegio y preservando los derechos de propiedad intelectual.

En cuanto al uso del correo electrónico, la política establece que su uso debe estar orientado exclusivamente al cumplimiento de funciones laborales. Las cuentas de correo son personales e intransferibles, y su uso indebido —como el envío de correos masivos no autorizados, cadenas, SPAM o contenido ofensivo— está estrictamente prohibido. Se requiere protección de las credenciales de acceso y cifrado de la información clasificada como reservada. Adicionalmente, se exige revisar constantemente el buzón institucional durante la jornada laboral y seguir lineamientos específicos durante ausencias prolongadas.

El uso de internet también está regulado para garantizar la seguridad de los activos de información. Se prohíbe el acceso a sitios inapropiados, ilegales o que puedan comprometer la seguridad institucional. Los usuarios deben evitar divulgar información confidencial en entornos públicos, y se restringe el uso de plataformas de mensajería o correos alternos no autorizados. El acceso a internet debe realizarse desde segmentos controlados y con base en los perfiles definidos por la organización. Toda actividad es monitoreada por el área de Tecnología, quien está facultada para restringir accesos y

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	22 de 32		

aplicar medidas disciplinarias ante usos indebidos. Para más información, consultar el documento completo: “PO-860-06 Política de Uso Aceptable de la Información y Activos Asociados”.

6.4 GESTIÓN DE AMENAZAS Y VULNERABILIDADES

6.4.1 Procedimiento para la gestión de vulnerabilidades técnicas

El procedimiento PD-860-13 Procedimiento para la Gestión de Vulnerabilidades Técnicas, tiene como objetivo establecer lineamientos claros para la identificación, análisis, clasificación y remediación de vulnerabilidades técnicas en la infraestructura tecnológica con el fin de proteger la confidencialidad, integridad y disponibilidad de la información institucional. Aplica a todo el personal con acceso autorizado a los activos de información y establece responsabilidades específicas para los jefes de tecnología, el oficial de seguridad de la información y el coordinador de servicios tecnológicos. Se exige la realización de escaneos de vulnerabilidades al menos una vez al año o por requerimiento, el mantenimiento de un listado actualizado con planes de remediación y la priorización obligatoria de vulnerabilidades críticas y altas, salvo justificación técnica formal.

Toda acción correctiva en ambientes productivos debe seguir el procedimiento de gestión de cambios tecnológicos, y los resultados de los análisis deben ser comunicados en informes ejecutivos a la Alta Dirección. El procedimiento también incluye pasos para supervisar la ejecución del plan de remediación, evaluar su efectividad, y asegurar su alineación con las políticas del SGSI. Aunque el documento no menciona anexos formales, se apoya funcionalmente en herramientas como el mapa de riesgos institucional, los planes de trabajo de escaneo, el procedimiento de gestión de cambios y los informes técnicos de remediación, los cuales actúan como insumos operativos para su aplicación efectiva.

6.4.2 Política de inteligencia contra amenazas y protección contra malware

La política PO-860-17 Política de Inteligencia Contra Amenazas y Protección Contra Malware, establece el marco estratégico, táctico y operativo para gestionar la inteligencia contra amenazas y garantizar una protección integral contra software malicioso. Aplica a todos los sistemas, redes, dispositivos y personal involucrado en la gestión de seguridad de la información. La organización debe implementar procesos de inteligencia en tiempo

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	23 de 32		

real, análisis de amenazas, automatización de detección y fuentes confiables de información sobre ataques. Se promueve una visión de ciberseguridad proactiva, mediante la evaluación continua de amenazas y la integración de inteligencia en los procesos de monitoreo, detección y respuesta a incidentes.

En cuanto a la protección contra malware, se establecen controles como el uso de soluciones antimalware en toda la infraestructura, la actualización de motores de detección, escaneos periódicos, control de dispositivos extraíbles y restricción de software no autorizado. También se definen filtros avanzados en correo electrónico y navegación web, campañas de concienciación para usuarios, y protocolos claros de respuesta ante incidentes de infección. La política es gestionada por el Coordinador de Seguridad de la Información, e involucra a todos los usuarios con acceso a sistemas críticos como corresponsables en la detección y reporte de amenazas.

6.5 GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Esta guía establece un modelo integral para gestionar los incidentes de seguridad de la información, desde la preparación hasta las actividades post-incidente. Se estructura en cuatro fases: preparación, detección y análisis, contención y recuperación, y lecciones aprendidas, alineándose con las mejores prácticas del NIST, la ISO/IEC 27035:2013 y la Resolución 500 de 2021 del MSPI. Se definen claramente los roles (usuarios, agentes, administradores, analistas, líderes) y procedimientos para asegurar una respuesta coordinada, oportuna y eficaz ante incidentes como accesos no autorizados, código malicioso, denegación de servicio o vandalismo digital. Se contempla también la clasificación, priorización, escalamiento y documentación de los incidentes.

La guía detalla los tiempos de respuesta según nivel de prioridad, los criterios de evaluación del impacto y los canales de notificación. Asimismo, establece protocolos rigurosos para la recolección de evidencia digital, análisis forense, medidas de contención, documentación de eventos y retroalimentación continua mediante lecciones aprendidas. Se enfatiza la necesidad de sensibilización del personal, aseguramiento de plataformas, gestión de parches y monitoreo constante como medidas preventivas clave. La aplicación efectiva de esta guía contribuye a la continuidad operativa, la mejora del SGSI y la preparación frente a ciberamenazas críticas.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	24 de 32		

6.6 POLÍTICA DE CONTROL DE ACCESO Y GESTIÓN DE LA IDENTIDAD

La PO-860-19 Política de Control de Acceso establece los lineamientos para proteger los sistemas de información y activos digitales de la organización mediante la implementación de controles de autenticación, autorización, monitoreo y restricción de accesos físicos y lógicos. Aplica a todos los usuarios internos y externos con acceso a los sistemas institucionales, y se basa en los principios de menor privilegio, segregación de funciones y acceso explícitamente autorizado. Define reglas claras para la creación, modificación, desactivación y eliminación de cuentas, tanto personales como privilegiadas, así como condiciones para el uso de cuentas genéricas bajo justificación y aprobación especial. También regula el acceso a redes, VPN, plataformas tecnológicas y dispositivos, estableciendo mecanismos como el uso obligatorio de MFA, bloqueo tras inactividad, y prohibición de almacenamiento automático de credenciales.

La política aborda además la gestión de accesos a la infraestructura, sistemas operativos, aplicaciones y código fuente, incluyendo prácticas como el monitoreo de sesiones, asignación de usuarios únicos, restricciones geográficas y de protocolo, rotación automática de contraseñas privilegiadas y bloqueo de estaciones de trabajo. Se integra con otras políticas como la de desarrollo seguro, la de contraseñas y la de uso aceptable, y prevé sanciones en caso de incumplimiento.

Herramientas que apoyan la política:

- PO-860-15 Política de Administración de Contraseñas.
- PO-860-06 Política de Uso Aceptable de la Información y Activos Asociados.
- GA-860-01 Guía de Identificación y Clasificación de Activos.

6.7 PROTECCION DE LA INFORMACION

6.7.1 Política de dispositivos del usuario

La Política PO-860-08 Política de Dispositivos Finales del Usuario, establece los controles y requisitos para el uso seguro de dispositivos finales utilizados por empleados, contratistas y terceros, asegurando la protección de la información que estos dispositivos procesan, almacenan o transmiten. Esta política aplica a portátiles, estaciones de trabajo, teléfonos

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	25 de 32		

móviles, tabletas y dispositivos extraíbles, estableciendo lineamientos en aspectos como autenticación multifactor (MFA), protección antimalware, gestión de parches y cifrado de datos. También se abordan el uso obligatorio de VPN para conexiones remotas, la prohibición del almacenamiento de información sensible en dispositivos personales no autorizados y la gestión ante pérdidas o robos de equipos, incluyendo bloqueo remoto.

La política exige el uso de software aprobado por la organización, controles centralizados para instalación y eliminación de programas, y mecanismos para detectar software no autorizado. Además, regula estrictamente el uso de dispositivos de almacenamiento extraíbles, imponiendo análisis antivirus, cifrado obligatorio y restricciones físicas en puertos. Se definen responsabilidades específicas para todos los usuarios, incluyendo el bloqueo de sesiones, custodia física de equipos, y reportes inmediatos ante incidentes. Esta política contribuye a preservar la confidencialidad, integridad y disponibilidad de la información institucional y debe ser conocida y aplicada por todos los actores de la organización que utilicen dispositivos finales.

Herramientas que apoyan la política:

- PO-860-15 Política de Administración de Contraseñas.
- PD-860-11 Procedimiento para la eliminación segura de datos y activos.
- FO-860-27 Formato de reporte de incidentes de Seguridad de la Información.

6.7.2 Política de trabajo y acceso remoto

La política PO-860-10 Política de Trabajo y Acceso Remoto, establece las directrices para proteger el acceso a los sistemas de información de la empresa, desde ubicaciones remotas o mediante dispositivos móviles. Su propósito es reducir los riesgos derivados del trabajo remoto, controlando el uso de conexiones externas, VPN, estaciones personales y dispositivos móviles. Aplica a todo el personal autorizado a acceder fuera de la red interna, definiendo condiciones de acceso como la autenticación multifactor (MFA), el principio de mínimo privilegio, la restricción por origen de conexión y el monitoreo continuo. Todo acceso remoto debe ser autorizado formalmente por la Gerencia del área solicitante y ejecutarse bajo estándares definidos, incluyendo la prohibición del almacenamiento automático de contraseñas y el uso de herramientas sin controles de seguridad.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	26 de 32		

Respecto al uso de VPN, se exige que solo se utilicen equipos autorizados o, en caso de excepción, que se acceda únicamente mediante escritorio remoto a estaciones corporativas. Además, los dispositivos móviles como portátiles, tabletas o celulares deben cumplir con controles específicos como el cifrado de medios de almacenamiento, custodia física segura, bloqueo con contraseña, y ausencia de datos sensibles o etiquetas corporativas visibles. Se establece que toda actividad debe ser monitoreada y que cualquier incumplimiento podrá ser sancionado disciplinariamente. Esta política debe revisarse cada doce meses o ante cambios relevantes en la organización o su entorno de amenazas.

6.8 POLÍTICA PARA EL DESARROLLO SEGURO

La PO-860-20 Política de Desarrollo Seguro de Software y Sistemas establece las directrices para garantizar que todo el software y los sistemas creados o adquiridos por la organización integren medidas de seguridad desde las etapas más tempranas del ciclo de vida de desarrollo (SDLC). Se fundamenta en los controles de la norma ISO/IEC 27001, e incluye prácticas clave como separación de entornos (desarrollo, pruebas y producción), codificación segura, arquitectura de sistemas robusta, validación continua de requisitos de seguridad, y pruebas técnicas rigurosas antes del paso a producción. Asimismo, busca minimizar vulnerabilidades, asegurar la protección de la información procesada por las aplicaciones y alinear el desarrollo con los requisitos regulatorios y de negocio.

La política exige evaluaciones de riesgos para definir requisitos de seguridad, incorporación de controles de entrada y salida, cifrado de comunicaciones, monitoreo de errores, validación de datos y autenticación reforzada. También establece lineamientos específicos para pruebas de aceptación, registros de pruebas, control de versiones, gestión de configuraciones y tratamiento de la información sensible usada en ambientes no productivos.

Herramientas que apoyan la política:

- GA-860-02 Guía De Codificación Segura.
- PD-860-14 Procedimiento De Pruebas.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	27 de 32		

6.9 SEGURIDAD DE LAS RELACIONES CON LOS PROVEEDORES

6.9.1 Política de seguridad de la información de los servicios en la nube

La política PO-860-18 Política de Seguridad de la Información de los Servicios en la Nube de la EPSI Anas Wayuu define los lineamientos para garantizar la seguridad de la información almacenada, procesada o transmitida a través de servicios en la nube. Aplica a modelos como IaaS, PaaS y SaaS, e involucra a todo el personal y terceros con acceso a estos servicios. Establece que, previo a la adopción de cualquier solución en la nube, se deben identificar los riesgos mediante una evaluación formal, definir los requisitos de seguridad aplicables y verificar que los proveedores cuenten con certificaciones. La selección de proveedores debe considerar aspectos como localización de datos, cifrado, soporte técnico y cumplimiento legal. Se promueve una responsabilidad compartida entre la organización y el proveedor, asignando roles específicos al área de Tecnología, el responsable de Seguridad de la Información y los usuarios.

Asimismo, la política establece controles para la gestión de incidentes en la nube, el monitoreo continuo de accesos y configuraciones, auditorías periódicas, y la planificación segura del cambio o terminación de servicios. Se exige que los proveedores garanticen el acceso a registros de auditoría cuando sea necesario y que los datos sean eliminados de forma segura al finalizar el contrato. Esta política refuerza la trazabilidad, la protección de activos digitales críticos y la continuidad de negocio en entornos híbridos o completamente virtualizados.

6.9.2 Política para la seguridad de las relaciones con los proveedores

La Política PO-860-09 Política para la Seguridad de las relaciones con los Proveedores, establece un marco de acción para la adquisición de bienes, servicios, insumos y equipos, con criterios técnicos, de seguridad y cumplimiento normativo. Aplica tanto a la selección inicial como a la evaluación y reevaluación periódica de proveedores y contratistas críticos, en conformidad con los requisitos de los sistemas de gestión ISO/IEC 27001 (Seguridad de la Información), ISO 9001 (Calidad) e ISO 45001 (SST). La política busca garantizar que los proveedores cumplan con condiciones mínimas técnicas, legales, financieras y contractuales, alineadas con los objetivos del Sistema Integrado de Gestión (SIG). También exige validar compromisos de seguridad de la información mediante acuerdos formales firmados por la Alta Dirección y los proveedores involucrados.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	28 de 32		

El procedimiento cubre todo el ciclo de contratación, desde la solicitud, cotización, evaluación técnica y legal, hasta la recepción, verificación y archivo documental de los productos o servicios. Incluye controles específicos para proveedores TIC y de servicios críticos. También contempla una reevaluación anual y un mecanismo de retroalimentación para establecer acciones de mejora. Este enfoque integral fortalece la trazabilidad, el cumplimiento normativo y la reducción de riesgos operacionales vinculados a la cadena de suministro.

6.10 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

Esta política define los lineamientos para garantizar la protección de la información institucional desde la vinculación, permanencia y desvinculación de colaboradores y contratistas. Establece controles en procesos como selección, validación de antecedentes, verificación de referencias y requisitos contractuales relacionados con la confidencialidad. La política aplica a todos los empleados y terceros, exigiendo el cumplimiento de cláusulas contractuales de seguridad, acuerdos de confidencialidad y revisión de roles críticos. También regula el proceso disciplinario ante incumplimientos y dispone medidas específicas para garantizar el tratamiento adecuado de la información tras el retiro del personal, incluyendo la inactivación de accesos y la devolución de activos.

Se establece un programa formal de sensibilización, formación y apropiación en seguridad de la información que debe aplicarse desde el ingreso del colaborador y mantenerse actualizado. Se promueve la evaluación periódica del conocimiento adquirido y la actualización de contenidos a partir de incidentes reales. Asimismo, la política contempla requisitos específicos para el trabajo remoto, asegurando controles físicos, lógicos y de autenticación para entornos virtuales. Estas disposiciones se alinean con los controles de la norma ISO/IEC 27001 y promueven un enfoque integral de corresponsabilidad entre la organización y sus colaboradores en la protección de los activos de información.

6.10.1 Seguridad física

La política PO-860-13 Política Controles Físicos de Seguridad de la Información, establece los lineamientos generales para proteger los activos físicos e instalaciones contra accesos no autorizados, daños, robos, interferencias ambientales y amenazas externas. Define controles específicos para el acceso físico a oficinas, salas, centros de datos y zonas

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	29 de 32		

críticas, mediante mecanismos como autenticación biométrica, credenciales temporales, monitoreo con CCTV, sensores de movimiento, alarmas, rondas de vigilancia, doble verificación y zonas de seguridad perimetral. También se contemplan prácticas de identificación visible del personal, acompañamiento a visitantes y separación de zonas de entrega para prevenir accesos indebidos.

La política incluye directrices detalladas sobre el monitoreo continuo de instalaciones, la ubicación discreta de salas con información sensible, la supervisión del trabajo en zonas seguras, y la protección contra amenazas físicas y ambientales como fuego, inundaciones, armas o sobretensiones eléctricas. Se establecen además directrices para la disposición y reutilización segura de equipos, la custodia de dispositivos fuera de la empresa y el respeto de la privacidad en inspecciones. Todas estas medidas buscan reforzar la confidencialidad, integridad y disponibilidad de la información bajo un enfoque preventivo, conforme a la norma ISO/IEC 27001.

7. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad es un documento que lista los objetivos y controles implementados en la empresa, así como las justificaciones de aquellos controles que no van a ser implementados. Este análisis se hizo evaluando el cumplimiento de la norma NTC ISO/IEC 27001, para cada uno de los controles establecidos en los dominios o temas relacionados con la gestión de la seguridad de la información que este estándar especifica.

8. MATERIALES NECESARIOS

- ✓ Oficinas administrativas al interior de la entidad.
- ✓ Muebles de oficina.
- ✓ Herramientas de oficina (grapadora, saca grapas, perforadora, entre otros).
- ✓ Teléfono o celular.
- ✓ Archivadores.
- ✓ Computadores.
- ✓ Aplicaciones de apoyo.
- ✓ Internet.
- ✓ Conexiones periféricas.
- ✓ Impresora.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	30 de 32		

- ✓ Papelería (hojas, notas adhesivas, bloc de notas, agenda, entre otros).

9. DOCUMENTOS Y REGISTROS ASOCIADOS

- ✓ PO-860-05 Política de Activos de Información.
- ✓ PO-860-06 Política de Uso Aceptable de la Información y Activos Asociados.
- ✓ PO-860-07 Política de Transferencia de Información.
- ✓ PO-860-09 Política para la Seguridad de las relaciones con los Proveedores.
- ✓ PO-860-10 Política de Trabajo y Acceso Remoto.
- ✓ PO-860-13 Política Controles Físicos de Seguridad de la Información.
- ✓ PO-860-14 Política de Gestión de Continuidad de la Seguridad de la Información.
- ✓ PO-860-15 Política de Administración de Contraseñas.
- ✓ PO-860-17 Política de Inteligencia Contra Amenazas y Protección Contra Malware.
- ✓ PO-860-18 Política de Seguridad de la Información de los Servicios en la Nube de la EPSI Anas Wayuu.
- ✓ PO-860-19 Política de Control de Acceso.
- ✓ PO-860-20 Política de Desarrollo Seguro de Software y Sistemas.
- ✓ PD-860-10 Procedimiento de Gestión de la Capacidad.
- ✓ PD-860-11 Procedimiento para la Eliminación Segura de Datos y Activos.
- ✓ PD-860-13 Procedimiento para la Gestión de Vulnerabilidades Técnicas.
- ✓ PD-860-14 Procedimiento De Pruebas.
- ✓ PL-860-01 Plan de Gestión de la Capacidad.
- ✓ FO-860-03 Formato de Entrega y Devolución de Activos.
- ✓ FO-860-26 Catálogo De Continuidad y Disponibilidad.
- ✓ FO-860-27 Formato de reporte de incidentes de Seguridad de la Información.
- ✓ GA-860-01 Guía de Identificación y Clasificación de Activos.
- ✓ GA-860-02 Guía De Codificación Segura.
- ✓ MT-860-06 Matriz de Activos de Información.
- ✓ MT-860-08 Matriz de Roles, Responsabilidades y Autoridades.

10. RESPONSABLE DE SOCIALIZACIÓN

- ✓ Responsable del SGSI.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	31 de 32		

11. RESPONSABLE DE EJECUCIÓN

- ✓ Los colaboradores, contratistas y terceros de Anas Wayuu EPSI.

12. 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
6.1	Cuarenta (40)	14/11/2024	Actualización en la denominación de cargos.
7.0	Cuarenta (40)	27/01/2025	Actualización en logo vigilado Super Salud - Circular Externa 2024151000000013-5 de 2024
8.0	Treinta y dos (32)	02/05/2025	Se eliminan los ítems de introducción, propósito, sustento legal y normativo técnico, política, lineamientos, política para los dispositivos móviles,

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo

Código:	MP-860-01	MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
Versión:	8.0-02-05-25		
Página:	32 de 32		

VERSIÓN	PAGINAS	FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN DEL CAMBIO
			política de teletrabajo, políticas del sistema de gestión de seguridad de la información de los usuarios, políticas de seguridad física y ambiental, políticas de gestión de seguridad de la información y administración de operaciones de cómputo, políticas de controles de acceso lógico (sistemas operativos y de información), políticas de uso de controles criptográficos y control de llaves, política de escritorios limpios, política de copia de respaldo, políticas y estándares de cumplimiento de seguridad informática, Se actualizan los ítems de objetivo, alcance, definiciones, políticas, se anexa el ítem de marco de políticas, directrices generales y declaración de aplicabilidad.

Elabora:	Revisa:	Aprueba:
Líder de Gestión Tecnológica	Director de Aseguramiento y Tecnología	Consejo Directivo