# AUTORIDAD PORTUARIA DE PUERTO BOLIVAR

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

**Elaborado por:**

Ing. Aida García González

**Oficial de Seguridad de la Información**

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

**Revisado por:**

Comité de Seguridad de la Información

**Aprobado por:**

Abg. Carlos Guzmán Solano
**GERENTE GENERAL**

**Fecha:**

Puerto Bolívar, 12 de junio de 2025

# Tabla de contenido

## 1. Antecedentes

Autoridad Portuaria de Puerto Bolívar (APPB), como empresa pública y enfocada en ofrecer facilidades para el embarque y desembarque de pasajeros y mercancías, reconoce la importancia de identificar y proteger sus activos de información. La información es un activo estratégico que respalda las operaciones, el proceso de toma de decisiones y la provisión de servicios y control a la Alianza Público Privada. Es vital la confidencialidad, integridad y disponibilidad de los datos con el fin de mantener la confianza con usuarios, cumplir con las obligaciones legales, normativas y regulaciones, y asegurar la continuidad del negocio.

Actualmente, las amenazas cibernéticas están en constante evolución, por lo cual, APPB se enfoca en protegerse ante posibles escenarios a los que podría enfrentarse como son ataques de phishing, malware, robo de datos, ataques de fuerza bruta, y vulnerabilidades en servidores, infraestructura y redes. Estos ciberataques pueden poner en riesgo la información financiera, personal, usuarios, comprometer los sistemas y activos críticos de APPB, generando perdidas económicas, daños a la reputación y el incumplimiento de las obligaciones legales.

La falta de una política de seguridad de la información sólida y actualizada, o su incorrecta implementación, pone a APPB en peligro considerable lo que puede ocasionar que sus operaciones estén comprometidas y no se realicen de manera eficiente y segura, comprometiendo los recursos. Por ende, es crucial que la entidad implemente un marco de seguridad integral que establezca las directrices y controles requeridos para salvaguardar la información, los sistemas y la infraestructura tecnológicas frente a las amenazas internas como externas.

Esta política de Seguridad de la Información busca establecer el objetivo, orientación, principios y normas fundamentales para la administración de la seguridad de la información en APPB. El presente documento representa una política de alto nivel, diseñada con el propósito de regular los elementos más relevantes de la seguridad de la información, con una validez a largo plazo.

La política establece las directrices y el compromiso de la máxima autoridad y los miembros del CSI de APPB para salvaguardar la información asegurando la confidencialidad, integridad y disponibilidad. Además, tiene como objetivo prevenir y mitigar los riesgos que pueden comprometer la información y activos de la entidad, incluyendo la aplicación del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, Ley Orgánica de Protección de Datos Personales, de las Normas ISO 27001, ISO 27005 de Gestión de Riesgos e ISO 27002.

El Gerente General de APPB, se compromete con el cumplimiento de la política y con el Esquema de Seguridad Gubernamental (EGSI). La alta dirección y el CSI comprenden la importancia de identificar y proteger los activos de información, evitando la destrucción, divulgación, modificación y utilización no autorizada de la información relacionada con la ejecución de los procesos y actividades de la Entidad, para el éxito y la sostenibilidad de APPB. La máxima autoridad se compromete a aportar los recursos requeridos para su puesta en marcha y conservación.

El Gerente General de APPB tiene la obligación de aprobar esta política y permitir su publicación y difusión entre los servidores de la Entidad. El Oficial de Seguridad de la Información y CSI se comprometen a fomentar una cultura de protección de la información en toda la institución, garantizando que los servidores se comprometan y respeten las políticas y procedimientos establecidos.

La política de Seguridad de la Información de APPB es un factor clave en la gestión de riesgos y en la protección de los activos de información. La implementación efectiva, permite que la entidad proteja los recursos de información, cumpla con la normativa legal y las regulaciones, así como la confidencialidad, integridad y disponibilidad de la información para dar continuidad al negocio.

## 2. Propósito General de la Política

Establecer un marco estratégico de Seguridad de la información que permita a Autoridad Portuaria de Puerto Bolívar salvaguardar sus activos de información, reducir el número de incidentes de seguridad, garantizando el cumplimiento normativo (incluyendo el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, Ley Orgánica de Protección de Datos, las Normas ISO 27001, ISO 27005 Gestión de Riesgos, e ISO 27002), la continuidad de los servicios que brinda la Entidad y fortalecer la confianza de sus usuarios y partes interesadas.

## 3. Política de Seguridad de la Información

### 3.1. Descripción de la Política

El Gerente General y el Comité de Seguridad de la Información de Autoridad Portuaria de Puerto Bolívar, entendiendo la importancia del tratamiento, procesamiento y almacenamiento de los activos de información, se comprometen a cumplir con la misión de proteger la información crítica y sensible asegurando su confidencialidad, integridad y disponibilidad. Establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de los procedimientos legales aplicables, en concordancia con la misión y visión de la institución.

Para APPB, proteger la información implica reducir el impacto generado en sus activos primarios y de soporte, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

## 3.2. Declaración de los objetivos de seguridad de la información

Autoridad Portuaria de Puerto Bolívar define los objetivos de seguridad de la información siguientes, en concordancia con el Plan Estratégico Institucional, con el fin de asegurar la salvaguarda de los recursos de información y la realización de sus metas organizativas:

- Implementar un sistema de seguridad de la información basado en el EGSI V3.
- Fortalecer la cultura de Seguridad de la Información en la que sea primordial la protección de la información, capacitando y evaluando la formación de los servidores y los incidentes reportados, a través de un programa de capacitaciones y evaluaciones internas semestrales.
- Determinar, valorar y manejar de manera proactiva los riesgos de seguridad, evaluando los riesgos gestionados y los incidentes asociados, a través de evaluaciones anuales con revisiones trimestrales.
- Garantizar el acceso a la información publica de acuerdo a los términos de la LOTAIP, en la parte que corresponda.
- Proteger los datos personales según la Ley Orgánica de los Datos Personales
- Desarrollar e implementar un procedimiento eficiente para la respuesta ante incidentes, valorando los tiempos de identificación, reporte y solución, por medio de un plan de revisiones y simulacro de ataques.



## 3.3. Roles y Responsabilidades

APPB establece los siguientes roles y responsabilidades con el fin de garantizar y salvaguardar los activos de información de la entidad:

1. **Gerente General (Máxima Autoridad):**
    a. Velar que la seguridad de la información se gestione adecuadamente en toda la institución, a través del Comité de Seguridad de la Información (CSI).
    b. Aprobar la Política de Seguridad de la Información y proporcionar los recursos necesarios para su implementación y mantenimiento.

2. **Comité de Seguridad de la Información (CSI):**
    a. Supervisar la implementación y cumplimiento de la Política de Seguridad de la Información.
    b. Evaluar los riesgos y aprobar estrategias de mitigación.
    c. Analizar la efectividad del Sistema de Administración de Seguridad de la Información (SGSI).
    d. Evaluar y proponer mejoras para el cumplimiento de la política
    e. Reportar a la máxima autoridad sobre riesgos, hallazgos y necesidades

3. **Oficial de Seguridad de la Información (OSI):**
    a. Ejecutar y monitorear la implementación de la política y los controles del EGSI V3
    b. Reportar los incidentes a MINTEL y coordinar las actividades de respuesta.
    c. Elaborar reportes periódicos para revisión del Comité de Seguridad de la Información sobre el cumplimiento de la política, incidentes y riesgos.
    d. Proponer mejoras de la política basados en hallazgos operativos
    e. Asesorar al Gerente General y a las diferentes áreas en materia de seguridad de la información

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

4. **Jefes o Responsables de Área/Departamento:**
    a. Garantizar que los servidores a su cargo resguarden la información que generan y almacenan de acuerdo con las normas establecidas en la Entidad.
    b. Implementar los controles de seguridad definidos en el EGSI correspondientes a sus áreas
    c. Reportar los incidentes de seguridad a OSI, relacionados a los requisitos y controles de seguridad de la información
    d. Fomentar la cultura de seguridad de la información entre sus colaboradores.
    e. Coordinar las capacitaciones con los servidores de la Entidad con respecto a la Seguridad de la Información, en coordinación con el Responsable de la Unidad de Tecnologías de la Información y la Unidad de Administración de Talento Humano.

5. **Personal de APPB, Contratistas y Terceros:**
    a. Salvaguardar la información que generan, almacenan y a la que tienen acceso en los activos de información.

b. Cumplir con los controles y procedimientos de seguridad de la información establecidos en la Entidad.
c. Participar en capacitaciones o actividades de concienciación en seguridad de la información de manera obligatoria
d. Firmar acuerdos de confidencialidad
e. Reportar los incidentes de seguridad relacionados a los activos de información tecnológicos

### 3.4. Alcance de los activos de información y asociados

El alcance de la implementación del Esquema Gubernamental de la Información versión 3.0 en Autoridad Portuaria de Puerto Bolívar, se aplicará a todos los tipos de activos de información y asociados considerados como críticos, incluyendo, pero no limitándose a:

- Sistemas de información (hardware y software).
- Equipos de Redes de comunicación.
- Información en la nube y credenciales de accesos
- Bases de datos.
- Documentos (físicos y electrónicos)
- Infraestructura donde se genere, procese, almacene y transmita información.



Quedan excluidos los sistemas informáticos cuyas fuentes no sean administradas por la entidad y los procesos externos que no sean controlados por APPB. Así mismo, esta política abarca todas las acciones vinculadas con la generación, recepción, tratamiento, almacenaje, difusión y eliminación de la información de APPB.

**Asociados**: Son elementos que no contienen información directamente, pero son esenciales para su gestión o protección, incluyendo:

- Todo el personal de APPB
- Proveedores externos
- Procesos operativos que involucren información (visitantes, pasantes, etc)

### 3.5. Comunicación y Difusión de la Política

La Política de Seguridad de la Información se comunicará a todos los servidores de la institución, con el fin de garantizar que todos estén informados y comprometidos con las mejores prácticas en lo que respecta a protección de la información.

La comunicación y difusión de la política se realizará a través de los siguiente medios y actividades:

1. **Difusión por correo electrónico:** Se enviará un correo a todos los servidores, con el documento completo de la política aprobada.
2. **Material gráfico y visual:** Se pondrá en cartelera un volante informativo con un resumen de las principales acciones de seguridad de la información que deben seguirse.
3. **Portal web:** la política estará disponible en el portal web de la entidad.

### 3.6. Excepciones y sanciones

La Política de Seguridad de la Información se aplicará a todos los servidores de la entidad de forma general. No obstante, podrán surgir algunas excepciones, que necesitarán ser adecuadamente justificadas y aprobadas por las autoridades pertinentes. Las circunstancias en las que esta política podría no ser efectiva comprenden, aunque no se restringen a:

1. **Casos de fuerza mayor o circunstancias excepcionales:** Cuando surjan eventos de emergencias o imprevistos (tales como catástrofes naturales, interrupciones del servicio en masa, etc.) que perjudiquen la aplicabilidad de la política y el Sistema Gubernamental de Seguridad de la Información (EGSI)
2. **Excepciones técnicas o de funcionamiento:** En situaciones excepcionales técnicas u operativas que lo requieran, y con la aprobación del Responsable de la Unidad de Tecnología de la Información y Oficial de Seguridad de la Información, se podrán aplicar medidas de seguridad alternativas. Estas acciones deberán lograr el propósito de salvaguardar la información institucional, sin poner en riesgo la integridad y operatividad de los procesos implicados.
3. **Actividades o proyectos particulares:** En determinados proyectos o actividades, si las necesidades técnicas o estratégicas lo permiten, se podrán modificar protocolos especiales que no cumplan fielmente con algunas de las estipulaciones de esta política. No obstante, estas modificaciones siempre necesitarán la aprobación del Oficial de la Seguridad de la Información.

**Sanciones por Incumplimiento**

El cumplimiento de la política de Seguridad de la Información es obligatorio para todo el personal, contratistas, proveedores y terceros que manejen activos de información de la Entidad. El incumplimiento de esta politica, ya sea por acción, omisión, negligencia o dolo, tendrá consecuencias disciplinarias, administrativas y/o legales, según la gravedad de la infracción y normas aplicables.

Las sanciones se clasifican:

- **Sanción leve:** Si ocurren incumplimientos menores o negligencias involuntarias, como ingresar a sistemas sin autorización o acceder a información clasificada, se aplicará una advertencia, se capacitará sobre la política de la entidad y se evaluará el acceso y permisos a los sistemas.

- **Sanción moderada:** en el caso de identificar una sanción más grave como la pérdida de información delicada o el acceso a datos confidenciales, se tomarán medidas como la suspensión temporal a los activos de información, la renovación de permisos y la imposición de sanción económica o disciplinaria de acuerdo a las normativas internas de la entidad.

- **Sanción severa:** En el caso de infracciones deliberadas, como el mal uso de la información o la explotación de vulnerabilidades para propósitos personales o externos, se podrá aplicar sanciones rigurosas que abarcan la interrupción temporal o definitiva del funcionario implicado, la comunicación a las autoridades correspondientes y, en caso de ser necesario, la acción legal correspondiente.

Para la aplicación de estas sanciones, la institución elaborará un Reglamento Interno de Sanciones en materia de seguridad de la información.



## 4. Glosario de términos

| Término | Definición |
|---|---|
| APPB | Autoridad Portuaria de Puerto Bolívar |
| CSI | Comité de Seguridad de la Información |
| OSI | Oficial de Seguridad de la Información |
| Activos de información | Cualquier elemento valioso para una organización que debe ser protegido del acceso no autorizado, uso, divulgación, modificación, destrucción o compromiso |
| Amenaza | Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización. |
| Confidencialidad | Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados. |
| Disponibilidad | Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada. |
| Integridad | Propiedad de proteger la precisión y completitud de los activos. |
| EGSI | Esquema Gubernamental de Seguridad de la Información |
| Activos primarios | Son considerados activos primarios las actividades, procesos e información del negocio |
| Activos de soporte | (de los cuales dependen los elementos primarios del alcance) de todos los tipos: Son considerados activos secundarios los siguientes: Hardware, Software, Redes, Personal, Ubicación y |

| | |
|---|---|
| | Estructura de la organización. |
| Acceso No Autorizado | Ingreso a sistemas, aplicaciones o datos por parte de individuos o entidades que no tienen los permisos o la autorización necesarios para hacerlo. |
| Incidente de Seguridad | Cualquier evento que pueda poner en riesgo la seguridad de la información, como ataques cibernéticos, accesos indebidos, pérdidas de datos, entre otros. |
| Protección de Datos Personales | Medidas y prácticas que se implementan para garantizar la privacidad y seguridad de la información relacionada con personas identificadas o identificables, de acuerdo con las normativas de protección de datos aplicables. |
| Gestión de Riesgos | Proceso mediante el cual se identifican, evalúan y gestionan los riesgos potenciales que puedan afectar la seguridad de la información, implementando controles y medidas adecuadas para mitigar dichos riesgos. |
| Autenticación | Proceso mediante el cual se verifica la identidad de un usuario, sistema o entidad, asegurando que solo las personas o procesos autorizados puedan acceder a recursos protegidos. |
| Autorización | Proceso de conceder permiso o acceso a los usuarios a sistemas, aplicaciones o datos, basándose en su identidad y roles predefinidos. |
| Vulnerabilidad | Debilidad en un sistema, aplicación o red que puede ser aprovechada por un atacante para comprometer la seguridad de la información. |
| Copia de Seguridad (Backup) | Proceso de hacer una copia de los datos importantes para garantizar que puedan ser recuperados en caso de pérdida o daño. |
| Evaluación de Seguridad | Proceso de revisión y análisis de los sistemas, redes y prácticas de seguridad de la información con el fin de identificar vulnerabilidades, riesgos y posibles áreas de mejora. |
| Protocolo de Seguridad | Conjunto de reglas y procedimientos que determinan cómo se deben manejar y proteger los datos dentro de un sistema o red para garantizar su seguridad. |
| LOTAIP | Ley Orgánica de Transparencia y Acceso a la Información Pública |



## 5. Documentos de referencia

- Acuerdo Ministerial MINTEL-2024 0003
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27002
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27005
- Resolución Administrativa Nro. APPB-APPB-2024-0065-R
- Resolución Administrativa Nro. APPB-APPB-2024-0039-R
- Plan Estratégico Institucional

- Reglamento Interno del Comité de Seguridad de la Información
- Ley Orgánica Transparencia y Acceso a la Información Publica
- Ley Orgánica de Protección de Datos Personales

## 6. Firmas de responsabilidad

| | Nombre/Cargo | Firma |
|---|---|---|
| **Elaborado por:** | Mgs. Aída García González<br>**Oficial Seguridad de la Información** | Firmado electrónicamente por: AIDA RAQUEL GARCIA GONZALEZ<br>Validar únicamente con FirmaEC |
| **Revisado por:** | Ing. Andrea Nieto Rodríguez<br>**Responsable de Gestión de Planificación (CSI)** | Firmado electrónicamente por: ANDREA ROSIBELL NIETO RODRIGUEZ<br>Validar únicamente con FirmaEC |
| | Ing. Álvaro Minuche Hermida<br>**Jefe Administrativo (CSI)** | Firmado electrónicamente por: ALVARO JAVIER MINUCHE HERMIDA<br>Validar únicamente con FirmaEC |
| | Ing. Gladys Feijoo Feijoo<br>**Responsable Unidad de Administración de Talento Humano (CSI)** | Firmado electrónicamente por: GLADYS ROCIO FEIJOO FEIJOO<br>Validar únicamente con FirmaEC |
| | Abg. Elaine Ramón Montenegro<br>**Responsable Comunicación Social (CSI)** | Firmado electrónicamente por: ELAINE CAROL RAMON MONTENEGRO<br>Validar únicamente con FirmaEC |
| | Ing. Daniela Romero Quezada<br>**Responsable Tecnologías de la Información (CSI)** | Firmado electrónicamente por: DANIELA ALEXANDRA ROMERO QUEZADA<br>Validar únicamente con FirmaEC |
| | Abg. Francisco Gómez Ayora<br>**Responsable de Unidad de Asesoría Jurídica (CSI)** | FRANCISCO JAVIER GOMEZ AYORA<br>Firmado digitalmente por FRANCISCO JAVIER GOMEZ AYORA<br>Fecha: 2025.06.13 10:26:43 -05'00' |
| **Aprobado por:** | Abg. Carlos Guzmán Solano<br>**Gerente General** | Firmado electrónicamente por: CARLOS ALEJANDRO GUZMAN SOLANO<br>Validar únicamente con FirmaEC |



## Control de versiones del formato referencial

| | |
|---|---|
| **Versión**: | 2.0 |
| **Fecha de la versión**: | 12-06-2025 |
| **Creado por**: | Oficial de Seguridad de la Información |
| **Aprobado por**: | Gerente General |
| **Nivel de confidencialidad**: | Bajo |

## Historial de cambios del formato referencial

| Versión | Fecha | Detalle del cambio |
|---|---|---|
| 1.0 | 15/11/2024 | Emisión inicial del documento |
| 2.0 | 12/06/2025 | Segunda emisión del documento |

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN