

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

Tabla de contenido

1. ANTECEDENTES	3
2. OBJETIVO DE LA POLÍTICA	4
3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	5
3.1. DESCRIPCIÓN DE LA POLÍTICA	5
3.2. DECLARACIÓN DE LOS OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN	5
3.3. ROLES Y RESPONSABILIDADES	8
3.4. ALCANCE Y USUARIOS	10
3.5. COMUNICACIÓN DE LA POLÍTICA	11
3.6. EXCEPCIONES Y SANCIONES	13
4. GLOSARIO DE TÉRMINOS	14
5. DOCUMENTOS DE REFERENCIA	16
6. FIRMAS DE RESPONSABILIDAD	17



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



1. Antecedentes

El Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), en su condición de institución estratégica encargada de la prevención, protección, socorro y respuesta oportuna ante incendios, emergencias médicas y rescates en el cantón Guayaquil, genera, administra y custodia un volumen significativo de información de alta criticidad. Estos activos de información —que abarcan desde los datos operativos en tiempo real de la Central de Alarmas y Comunicaciones hasta los registros administrativos, financieros, logísticos y de talento humano— constituyen el pilar fundamental para asegurar la continuidad de los servicios misionales y salvaguardar la vida y los bienes de la ciudadanía.

La presente Política General de Seguridad de la Información se crea ante la imperiosa necesidad de establecer un marco de gobernanza robusto y formalizado que regule y proteja estos activos contra las crecientes y sofisticadas amenazas del entorno digital y físico. Si bien la adopción tecnológica y la digitalización optimizan de forma exponencial la capacidad de respuesta y la eficiencia institucional, también introducen riesgos complejos como el acceso no autorizado, el secuestro de datos (ransomware), la fuga de información sensible, la alteración de registros críticos y la denegación de servicios informáticos.

No contar con una política de alto nivel formalizada, aprobada y periódicamente actualizada expone al BCBG a riesgos institucionales de alto impacto. La ausencia de lineamientos claros propicia la vulnerabilidad ante incidentes de seguridad causados por el factor humano o la falta de concienciación, debilita la implementación de salvaguardas tecnológicas uniformes y atomiza los esfuerzos de defensa. Las consecuencias de estas brechas no solo comprometen la confidencialidad, integridad y disponibilidad de los datos, sino que exponen a la institución a severas sanciones legales, pérdida de la confianza pública, afectación reputacional y, de forma crítica, a la interrupción potencial de los sistemas de despacho y operaciones de emergencia, lo que impactaría de manera directa en la seguridad ciudadana.

Por consiguiente, el propósito fundamental de esta política de alto nivel es definir con absoluta claridad el objetivo, la dirección estratégica, los principios rectores y las reglas básicas que gobernarán el Sistema de Gestión de Seguridad de la Información (SGSI), en estricta alineación con el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0) y el Acuerdo Ministerial Nro. 0003-2024. Este documento se constituye con una visión y vigencia de largo plazo, consolidándose como la norma matriz y la piedra angular directiva de la cual se desprenderán, de manera jerárquica, las políticas específicas, estándares técnicos y procedimientos operativos que la infraestructura requiera.

La Máxima Autoridad del Benemérito Cuerpo de Bomberos de Guayaquil, consciente de su responsabilidad legal, operativa y social, declara e instrumenta a través de la emisión de este documento su compromiso absoluto e inquebrantable con el diseño, implementación, mantenimiento, dotación de recursos y mejora continua del EGSi v3.0. Las autoridades de la institución asumen formalmente la responsabilidad de respaldar las funciones del Comité de Seguridad de la Información y del Oficial de Seguridad de la Información (OSI), impulsando activamente una cultura organizacional donde la seguridad de la información no sea vista como un esfuerzo técnico aislado, sino como una responsabilidad compartida y obligatoria para todos los servidores y funcionarios públicos de esta benemérita institución así como



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



terceras partes vinculadas, garantizando un entorno institucional resiliente, seguro y transparente.

2. Objetivo de la Política

El objetivo fundamental de la presente Política General de Seguridad de la Información es establecer las directrices estratégicas, principios rectores y lineamientos corporativos de alto nivel que regulen la gestión integral de la seguridad de la información dentro del Benemérito Cuerpo de Bomberos de Guayaquil (BCBG). Este instrumento define el marco normativo y el compromiso institucional necesarios para garantizar la adecuada protección de todos los activos de información de la entidad, minimizando la vulnerabilidad de la infraestructura tecnológica y operativa frente a amenazas internas o externas, deliberadas o accidentales.

A través de la formalización de esta política de alto nivel, el BCBG persigue un propósito multidimensional orientado a los siguientes fines:

- **Preservar la Triada de la Seguridad:** Asegurar de manera permanente la confidencialidad (garantizando que la información sea accesible únicamente por el personal formalmente autorizado), la integridad (salvaguardando la exactitud, completitud y no alteración de los datos y sistemas); y, la disponibilidad (asegurando el acceso oportuno a la información y a los recursos tecnológicos cuando la operación misional o administrativa lo requiera).
- **Prevenir y Mitigar Riesgos Institucionales:** Institucionalizar la gestión proactiva de riesgos para identificar de forma temprana las amenazas y vulnerabilidades que afecten a los activos de información, ejecutando controles proporcionales que impidan incidentes de seguridad, fugas de datos, accesos no autorizados o interrupciones en los servicios de la entidad.
- **Garantizar la Continuidad de los Servicios de Emergencia:** Proteger con especial énfasis los sistemas de información, redes de comunicación y plataformas tecnológicas críticas que sustentan la atención inmediata de emergencias, prevención de incendios y salvamento, asegurando que la capacidad de respuesta operativa del BCBG hacia la ciudadanía no se vea comprometida en ninguna circunstancia.
- **Alinear el Cumplimiento Legal y Normativo:** Proveer la base jurídica interna indispensable para cumplir con el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), el Acuerdo Ministerial Nro. 0003-2024, la Ley Orgánica de Protección de Datos Personales, la Ley Orgánica de Transparencia y Acceso a la Información Pública; y, demás normativas emitidas por los órganos de control del Estado ecuatoriano.
- **Guiar la Normativa Específica:** Servir como el documento matriz y eje conductor del cual se desprenderán de forma jerárquica y obligatoria las políticas específicas,

**EGSI**ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN

manuales, estándares técnicos, directrices de configuración y procedimientos operativos de seguridad de la información que requieran implementarse en las distintas áreas del BCBG

3. Política de Seguridad de la Información

3.1. Descripción de la Política

La Máxima Autoridad y el Comité de Seguridad de la Información del Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), reconociendo el valor estratégico de la información en el cumplimiento de sus funciones misionales de prevención, protección, socorro y respuesta a emergencias, formalizan su compromiso inquebrantable con el diseño, despliegue y mantenimiento continuo de un Sistema de Gestión de Seguridad de la Información robusto.

Este sistema tiene como fin primordial consolidar un marco de absoluta confianza y transparencia en las interacciones y servicios que la institución mantiene con el Estado ecuatoriano, la ciudadanía de Guayaquil; y, los diversos grupos de interés, asegurando que cada proceso se ejecute bajo el más estricto cumplimiento legal y técnico en concordancia directa con la misión institucional.

Para el BCBG, la protección integral de la información se concibe como un proceso dinámico y transversal que busca la mitigación y reducción sistemática del impacto generado sobre sus activos informáticos, operativos y administrativos. A través de la identificación, evaluación y tratamiento continuo de los riesgos tecnológicos y humanos, la entidad mantendrá un nivel de exposición controlado y aceptable. Esto garantiza la preservación de la confidencialidad, integridad y disponibilidad de los datos sensibles de la ciudadanía y de las operaciones de emergencia, respondiendo de manera oportuna a las demandas de seguridad exigidas por los entes de control y la sociedad.

En virtud de lo expuesto, la presente política establece las directrices fundamentales que guiarán el comportamiento personal y profesional dentro y fuera de la infraestructura tecnológica de la entidad. Su observancia, aplicación y cumplimiento riguroso son de carácter obligatorio para todas las áreas que componen la estructura orgánica del BCBG según el alcance definido, vinculando de forma directa e inderogable a los servidores, funcionarios y trabajadores públicos de esta benemérita institución, contratistas, consultores, proveedores externos y terceras partes que, por razones de su función o relación jurídica, tengan acceso, custodien, generen o procesen información de propiedad o bajo la responsabilidad de la institución.

3.2. Declaración de los objetivos de seguridad de la información

Para materializar las directrices de la presente Política General y asegurar su alineación estratégica con el Plan Estratégico Institucional (PEI) del Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), se establecen los siguientes objetivos estratégicos de seguridad de la información. Estos objetivos son coherentes con el marco normativo, técnicamente medibles,



EGSÍ

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



vinculados directamente a la gestión de riesgos y serán comunicados y actualizados de forma periódica por el Comité de Seguridad de la Información.

- **Objetivo 1:** Fortalecer la Cultura de Seguridad y Concientización Institucional
 - **Descripción:** Desarrollar, promover y consolidar una cultura organizacional orientada a la seguridad de la información, transformando las buenas prácticas en hábitos cotidianos para todo el personal operativo, administrativo y terceras partes.
 - **Planificación Operativa:** Se diseñará e implementará un Plan Anual de Comunicación y Sensibilización que abarque talleres, simulacros de ingeniería social y boletines informativos.
 - **Recursos Requeridos:** Plataformas de aprendizaje virtual, material didáctico, canales de difusión institucionales y horas de capacitación asignadas.
 - **Responsables:** Dirección General de Talento Humano en coordinación directa con el Oficial de Seguridad de la Información (OSI).
 - **Plazo de Cumplimiento:** Ejecución continua con evaluaciones e informes semestrales.
 - **Evaluación de Resultados:** Medido a través del indicador de cobertura de capacitación (porcentaje de personal concientizado) y la reducción en la tasa de vulnerabilidad en los simulacros de incidentes (ej. campañas de phishing simuladas).
- **Objetivo 2:** Institucionalizar la Gestión Proactiva de Riesgos de Seguridad de la Información
 - **Descripción:** Identificar, valorar, priorizar y mitigar sistemáticamente los riesgos tecnológicos, físicos y humanos que afecten a los activos de información críticos, previniendo o reduciendo los impactos operativos y legales no deseados.
 - **Planificación Operativa:** Realizar el Análisis y Valoración de Riesgos integral de la institución, definiendo e implantando las salvaguardas y controles de seguridad técnica y organizativa dictados por el EGSÍ v3.0.
 - **Recursos Requeridos:** Metodologías estándar de análisis de riesgos (ej. Magerit o ISO/IEC 27005), herramientas de inventario de activos y herramientas de evaluación técnica.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



Responsables: Oficial de Seguridad de la Información (OSI) con el soporte técnico de la Dirección General de Tecnologías de la Información y Comunicaciones y la aprobación del Comité de Seguridad de la Información.

- **Plazo de Cumplimiento:** Actualización anual formal, o ante cambios significativos en la infraestructura tecnológica.
- **Evaluación de Resultados:** Medido mediante el índice de mitigación de riesgos críticos y el porcentaje de controles del EGSi v3.0 efectivamente implementados y operativos.
- **Objetivo 3:** Optimizar la Respuesta a Incidentes y Garantizar la Continuidad Operativa
 - **Descripción:** Garantizar una administración eficaz, integrada y oportuna de los eventos, debilidades e incidentes de seguridad de la información, minimizando el impacto negativo en los servicios misionales, especialmente en los sistemas de despacho y la Central de Alarmas y Comunicaciones.
 - **Planificación Operativa:** Establecer y documentar el Procedimiento de Gestión de Incidentes de Seguridad, configurando alertas tempranas, planes de contingencia, respaldos de información cifrados y mecanismos de alta disponibilidad.
 - **Recursos Requeridos:** Herramientas de monitoreo y detección, soluciones de copia de seguridad (backups) físicas y en la nube, y canales de comunicación redundantes.
 - **Responsables:** La Dirección General de Tecnologías de la Información y Comunicaciones en coordinación operativa con el Oficial de Seguridad de la Información (OSI).
 - **Plazo de Cumplimiento:** Implementación del protocolo de respuesta inmediata y revisión permanente.
 - **Evaluación de Resultados:** Evaluado a través del Tiempo Medio de Detección (MTTD) y Tiempo Medio de Respuesta/Resolución (MTTR) ante incidentes, así como el porcentaje de efectividad en las pruebas de restauración de copias de seguridad.
- **Objetivo 4:** Asegurar el Cumplimiento Legal, Normativo y de Auditoría
 - **Descripción:** Velar por que todas las operaciones, sistemas y tratamientos de datos dentro del BCBG se ejecuten en estricto cumplimiento del marco legal informático del Ecuador y las directrices de los órganos de control.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- **Planificación Operativa:** Ejecutar auditorías y evaluaciones internas periódicas del SGSI, asegurando la trazabilidad de los accesos, la retención segura de bitácoras (logs); y, la alineación con las disposiciones de la Contraloría General del Estado y el Ministerio de Telecomunicaciones y de la Sociedad de la Información.
- **Recursos Requeridos:** Herramientas de auditoría de sistemas, marcos de cumplimiento del EGSi v3.0 y asesoría legal institucional.
- **Responsables:** Oficial de Seguridad de la Información (OSI) en conjunto con la Dirección General de Auditoría Interna.
- **Plazo de Cumplimiento:** Evaluaciones programadas de forma previa a los cortes y reportes oficiales exigidos por los entes de regulación.
- **Evaluación de Resultados:** Medido mediante el nivel de madurez obtenido en las evaluaciones del EGSi v3.0 y el porcentaje de hallazgos o no conformidades solventadas oportunamente.

Para el seguimiento y control de estos objetivos, el Oficial de Seguridad de la Información mantendrá una Matriz de Indicadores de Gestión que será presentada semestralmente ante el Comité de Seguridad de la Información, asegurando que el desempeño del sistema se mantenga en un ciclo de mejora continua.

3.3. Roles y Responsabilidades

Para garantizar la adecuada gobernanza, uso y protección de los activos de información del Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), se establece una estructura formal de roles y responsabilidades. La seguridad de la información se gestiona como un compromiso transversal y una responsabilidad compartida en todos los niveles de la organización, estructurada de la siguiente manera:

- **Primer Jefe / Máxima Autoridad**
 - **Responsabilidad:** Ostenta la máxima responsabilidad legal y estratégica sobre la seguridad de la información en la institución. Se encarga de aprobar formalmente la Política General y las políticas específicas del Sistema de Gestión de Seguridad de la Información (SGSI), emitir directrices de alto nivel y asegurar la asignación oportuna de los recursos financieros, tecnológicos y humanos necesarios para la correcta implementación y mejora continua del EGSi v3.0.
- **Comité de Seguridad de la Información (CSI)**
 - **Responsabilidad:** Órgano colegiado de carácter directivo encargado de supervisar, alinear y validar la estrategia de seguridad con los objetivos



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



misionales del BCBG. Es responsable de revisar periódicamente el desempeño del EGSi, aprobar los planes de tratamiento de riesgos, validar las políticas complementarias antes de su promulgación y tomar decisiones ejecutivas ante incidentes de seguridad de alto impacto o desviaciones normativas detectadas en las evaluaciones internas.

- **Oficial de Seguridad de la Información (OSI)**

- **Responsabilidad:** Rol especializado e independiente encargado de coordinar, ejecutar y supervisar la implementación operativa del EGSi v3.0 en la institución. Actúa como el principal asesor técnico y estratégico del Comité de Seguridad de la Información y de la Máxima Autoridad en materia de ciberseguridad y protección de datos.

Sus funciones incluyen la realización de análisis de riesgos, la formulación de políticas y estándares, el monitoreo del cumplimiento normativo, la gestión de la matriz de indicadores y la entrega periódica de informes ejecutivos sobre el estado de la seguridad de la información del BCBG.

- **Dirección General de Tecnologías de la Información y Comunicaciones**

- **Responsabilidad:** Custodio tecnológico del ecosistema digital del BCBG. Es responsable de diseñar, implementar y mantener operativos los controles y salvaguardas técnicas necesarias en la infraestructura de red, servidores, bases de datos y sistemas operativos institucionales. Debe asegurar la aplicación de mecanismos de cifrado, segregación de redes, parches de seguridad, gestión de vulnerabilidades y la administración técnica de identidades y accesos, garantizando en todo momento la alta disponibilidad y redundancia de las plataformas que soportan la atención de emergencias.

- **Dirección General de Talento Humano**

- **Responsabilidad:** Responsable de gestionar la seguridad de la información desde la perspectiva del recurso humano. Debe asegurar que todo el personal de nuevo ingreso (administrativo y operativo) firme obligatoriamente los Acuerdos de Confidencialidad y Uso Aceptable de Activos antes de acceder a los sistemas. Asimismo, coordinará con el OSI la ejecución de los planes anuales de capacitación y sensibilización, y aplicará los procesos disciplinarios o sanciones administrativas correspondientes en caso de violaciones o incumplimientos a las políticas de seguridad vigentes, de acuerdo con la normativa legal vigente y reglamentos internos.

- **Directores, Jefes de Unidad y Líderes de Proceso**



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- **Responsabilidad:** Actúan como los propietarios y custodios directos de la información generada o procesada dentro de sus áreas de competencia. Son responsables de identificar y clasificar sus activos de información según su nivel de criticidad, y de garantizar que los servidores públicos y colaboradores bajo su control directo conozcan, comprendan y apliquen rigurosamente las normas y procedimientos de seguridad establecidos, reportando de inmediato al OSI cualquier evento o debilidad detectada en sus operaciones diarias.
- **Servidores Públicos, Personal Operativo y Terceras Partes**
 - **Responsabilidad:** Todo usuario con acceso a los recursos de información del BCBG (incluyendo servidores, funcionarios, trabajadores, consultores, proveedores externos, pasantes y contratistas) tiene la obligación personal e inderogable de mantener la confidencialidad, integridad y disponibilidad de la información relacionada con sus funciones de trabajo. Deben dar un uso estrictamente institucional y seguro a las credenciales de acceso, dispositivos asignados y canales de comunicación oficiales, cumpliendo fielmente con la presente política y notificando oportunamente cualquier sospecha de incidente de seguridad.

3.4. Alcance y usuarios

La presente Política General de Seguridad de la Información es de aplicación transversal y cumplimiento obligatorio para toda la estructura orgánica y funcional del Benemérito Cuerpo de Bomberos de Guayaquil (BCBG). El alcance y el universo de usuarios obligados se delimitan de la siguiente manera:

- **Alcance Institucional y Tecnológico:** Esta política se aplica de forma vinculante a todos los activos de información, tangibles e intangibles, que forman parte del Sistema de Gestión de Seguridad de la Información, de acuerdo con lo especificado y delimitado en el documento oficial de Definición del Alcance del EGS de la institución. Esto comprende:
 - **Procesos Misionales y de Apoyo:** Todas las actividades relacionadas con la misión principal del BCBG, incluyendo la gestión, despacho y atención operativa de emergencias, la prevención y seguridad contra incendios, la Central de Alarmas y Comunicaciones, la Academia de Bomberos, así como los procesos logísticos, administrativos, financieros, legales y de talento humano.
 - **Límites Físicos y Geográficos:** La totalidad de las instalaciones bajo la responsabilidad del BCBG, que incluyen la Primera Jefatura, cuarteles, compañías, bodegas, dependencias operativas y/o administrativas; y, entornos autorizados para la ejecución de funciones institucionales.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- **Infraestructura Tecnológica:** Redes de comunicación (datos y voz), servidores, bases de datos, sistemas de información propios o contratados (incluyendo la gestión de identidades y accesos en entornos de nube), computadoras de escritorio, dispositivos portátiles y cualquier medio físico o digital utilizado para crear, almacenar, procesar o transmitir información de la entidad.
- **Usuarios de la Política:** Los mandatos, prohibiciones y directrices contenidos en este documento y en las normativas específicas que de él se deriven, deben ser conocidos, comprendidos y acatados estrictamente por las siguientes personas o grupos de personas:
 - **Personal Interno:** Todos los servidores públicos sin distinción de su nivel jerárquico o modalidad de contratación, lo cual incluye a la Jefatura Máxima, miembros del Comité de Seguridad de la Información, directores generales, jefes de unidad, personal administrativo, oficiales, y el personal operativo en servicio activo.
 - **Terceras Partes y Relaciones Externas:** Todos los contratistas, consultores, asesores externos, pasantes, proveedores de bienes y servicios tercerizados (incluyendo soporte técnico, desarrollo de software y mantenimiento de infraestructura); y, cualquier persona natural o jurídica que, por motivos de una relación contractual, legal o de cooperación interinstitucional, requiera acceso a las instalaciones, redes o activos de información del BCBG.

La seguridad de la información constituye una condición indispensable para el desempeño de cualquier función dentro o para el BCBG; por lo tanto, ningún usuario está exento de la observancia y cumplimiento de esta política dentro de las actividades relacionadas con su gestión.

3.5. Comunicación de la Política

La eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) radica en el conocimiento y la comprensión de sus normativas por parte de todos los miembros de la institución. Por lo tanto, esta Política General no tiene carácter reservado y debe ser comunicada, socializada y asimilada por todos los servidores públicos, personal operativo, personal administrativo y terceras partes que interactúen con el Benemérito Cuerpo de Bomberos de Guayaquil (BCBG).

Para garantizar una difusión efectiva y permanente, el Oficial de Seguridad de la Información (OSI), en coordinación directa con la Dirección General de Talento Humano y la Dirección General de Comunicación (o quien haga sus veces), ejecutará las directrices establecidas en el Plan de Comunicación y Sensibilización del EGSi, a través de las siguientes estrategias y medios:

**EGSI**ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN

Estrategias de Difusión y Sensibilización:

Inducciones al Personal de Nuevo Ingreso: La Política General de Seguridad de la Información será un componente obligatorio en el proceso de inducción de todo nuevo servidor, bombero u oficial que se integre al BCBG. Durante este proceso, se explicarán los lineamientos básicos y se firmará el Acuerdo de Confidencialidad respectivo.

Talleres y Capacitaciones Periódicas: Se programarán talleres anuales teórico-prácticos adaptados a los diferentes perfiles de la institución (capacitaciones específicas para operadores de la Central de Alarmas, para personal administrativo/financiero y para bomberos en los cuarteles y compañías). Estos espacios permitirán resolver dudas y simular escenarios de riesgos reales (ej. correos fraudulentos, manejo de contraseñas).

Campañas de Concientización (Propaganda): Se diseñarán campañas visuales y digitales continuas con mensajes clave, directos y de fácil recordación sobre buenas prácticas de ciberseguridad, prevención de fuga de información y protección de los activos de la institución.

Medios y Canales de Comunicación Oficiales:

Correo Electrónico Institucional: Envío de boletines periódicos, infografías y comunicados oficiales (memorandos) recordando los principios de esta política y alertando sobre nuevas amenazas informáticas.

Portal Web e Intranet: La versión oficial y actualizada de la presente Política, así como de los manuales y procedimientos derivados, estará publicada permanentemente en la intranet o portal web del BCBG para consulta de todo el personal.

Carteleras Físicas y Pantallas Digitales: Colocación de afiches y reproducción de material audiovisual en las pantallas informativas ubicadas en la Primera Jefatura, dependencias administrativas, la Academia de Bomberos, cuarteles y compañías, asegurando que el mensaje llegue al personal operativo que no labora frente a un computador de manera continua.

Volantes y Trípticos (Material Impreso): Distribución de material impreso resumido tipo "guía de bolsillo" durante los talleres de capacitación o visitas técnicas a las distintas dependencias del BCBG.

Sistema de Gestión Documental: Notificación formal y obligatoria de la emisión de esta política (y sus futuras actualizaciones) a través del sistema de gestión documental institucional para dejar constancia de la recepción por parte de todas las direcciones y jefaturas.

La institución garantizará que los materiales de comunicación sean claros, concisos y utilicen un lenguaje accesible para todo el personal, independientemente de su nivel de conocimiento técnico.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



3.6. Excepciones y sanciones

Dada la naturaleza crítica de las operaciones del Benemérito Cuerpo de Bomberos de Guayaquil (BCBG) y la sensibilidad de la información que custodia, el cumplimiento de la presente Política General y de las normativas de seguridad que de ella se derivan es de carácter estricto y obligatorio. No obstante, se establecen los siguientes lineamientos para la gestión de casos excepcionales y el régimen disciplinario aplicable en caso de incumplimientos.

A. Gestión de Excepciones

Como regla general, no se admiten desviaciones a los controles de seguridad establecidos en el SGSI. Sin embargo, se reconoce que pueden existir escenarios operativos, limitaciones técnicas de sistemas heredados (legacy) o requerimientos de interoperabilidad institucional que hagan técnica o funcionalmente inviable el cumplimiento estricto de una directriz. Para estos casos, la política no será aplicable bajo el siguiente procedimiento formal:

Solicitud y Justificación: Toda excepción tecnológica o procedimental debe ser solicitada por escrito por el Director o Jefe de Área responsable del proceso. La solicitud debe incluir una justificación técnica u operativa detallada que demuestre la necesidad de la excepción para no afectar la operatividad de la institución.

Evaluación de Riesgos: El Oficial de Seguridad de la Información (OSI) evaluará la solicitud, identificando las vulnerabilidades y el riesgo residual que la excepción introduciría al entorno del BCBG, proponiendo controles compensatorios temporales.

Aprobación Formal: Ninguna excepción tendrá validez sin la aprobación formal y documentada del Comité de Seguridad de la Información.

Temporalidad y Revisión: Toda excepción aprobada tendrá un carácter temporal (con fecha de caducidad) y será registrada en el Inventario de Excepciones del SGSI, sujeta a auditoría y revisión periódica.

Excepción por Fuerza Mayor (Emergencia Operativa): En situaciones de fuerza mayor o emergencias operativas comprobadas donde la salvaguarda de vidas humanas o bienes dependa de saltar un control de seguridad (ej. acceso de urgencia a un sistema de despacho), el personal operativo podrá actuar según la necesidad del incidente. Sin embargo, este evento deberá ser reportado obligatoriamente al OSI y a la cadena de mando en un plazo no mayor a 24 horas tras finalizar la emergencia, para su respectiva auditoría y registro.

B. Régimen de Sanciones e Incumplimientos

La seguridad de la información es una obligación inherente al cargo y función de todo colaborador. El desconocimiento de esta política no exime de responsabilidad a ningún



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



usuario. En caso de detectarse un incumplimiento, vulneración intencional, negligencia o mal uso de los activos de información del BCBG, se aplicará el siguiente régimen de sanciones:

Proporcionalidad y Debido Proceso: Toda presunta infracción será investigada por el Oficial de Seguridad de la Información y reportada a la Dirección General de Talento Humano y a la Dirección General de Asesoría Legal (o quien haga sus veces). Las sanciones se aplicarán garantizando el debido proceso y en estricta proporcionalidad a la gravedad de la falta, el nivel de impacto causado a la institución, la afectación a la operatividad de emergencias y la intencionalidad del infractor.

Personal Sujeto a la Ley Orgánica de Servicio Público y Código de Trabajo: Para los servidores y funcionarios públicos, oficiales y personal operativo, las sanciones se ejecutarán en estricto apego al Régimen Disciplinario establecido en la Ley Orgánica del Servicio Público (LOSEP), el Código del Trabajo y a los reglamentos internos establecidos en la institución. Estas podrán ir desde una amonestación verbal o escrita, hasta la destitución del cargo o visto bueno, dependiendo de la tipificación de la falta (leve, grave o muy grave).

Terceras Partes y Contratistas: En el caso de proveedores, consultores externos o contratistas, el incumplimiento de esta política se considerará una violación directa a las cláusulas del Acuerdo de Confidencialidad y del contrato suscrito. El BCBG se reserva el derecho de dar por terminado el contrato de manera unilateral y anticipada; y, de ejecutar las garantías correspondientes o exigir compensaciones por daños y perjuicios.

Responsabilidad Legal y Penal: Si el incumplimiento constituye una violación a la Ley Orgánica de Protección de Datos Personales (fuga o comercialización de datos ciudadanos), o se tipifica como un delito informático según el Código Orgánico Integral Penal (COIP) (ej. sabotaje a sistemas de emergencia, interceptación ilegal de datos, destrucción de registros públicos), la Jefatura Máxima del BCBG, a través de su representante legal, iniciará inmediatamente las acciones administrativas, civiles y penales correspondientes ante las autoridades judiciales competentes.

4. Glosario de términos

Término	Definición
Activo de Información	Cualquier elemento valioso para la institución (datos, hardware, software, servicios, instalaciones, talento humano e intangibles como la reputación) que debe ser protegido del acceso no autorizado, uso, divulgación, modificación, destrucción o compromiso.

**EGSI**ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN

Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos que no cuenten con la autorización formal respectiva.
CSI	Comité de Seguridad de la Información. Órgano colegiado de carácter directivo dentro del BCBG encargado de la aprobación, dirección estratégica y evaluación del Sistema de Gestión de Seguridad de la Información.
Disponibilidad	Propiedad de que la información, los sistemas y los recursos tecnológicos sean accesibles y utilizables de manera oportuna por demanda de una entidad o usuario autorizado.
EGSI v3.0	Esquema Gubernamental de Seguridad de la Información. Marco técnico y normativo de cumplimiento obligatorio en Ecuador, emitido por el MINTEL, que establece las directrices para la protección de la información en las instituciones del Estado.
Incidente de Seguridad	Evento o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del BCBG y amenazar la confidencialidad, integridad o disponibilidad de la información.
Integridad	Propiedad de salvaguardar la exactitud, completitud y estado original de los activos de información, previniendo alteraciones o modificaciones no autorizadas, ya sean accidentales o malintencionadas.
OSI	Oficial de Seguridad de la Información. Funcionario especializado encargado de liderar, coordinar y supervisar la



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



	implementación, operación y mejora continua del EGSi dentro del BCBG.
Riesgo de Seguridad	La posibilidad de que una amenaza tecnológica, física o humana explote una vulnerabilidad de un activo de información, causando un impacto negativo en las operaciones o en el cumplimiento de los objetivos de la institución.
SGSI	Sistema de Gestión de Seguridad de la Información. Parte del sistema de gestión general del BCBG, basado en un enfoque de riesgos, destinado a establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
Vulnerabilidad	Debilidad en un activo de información o en los controles de seguridad que puede ser explotada por una o más amenazas.

5. Documentos de referencia

La presente Política General de Seguridad de la Información se fundamenta y complementa con los siguientes cuerpos legales, normativas técnicas y documentos internos institucionales:

Marco Legal Nacional:

- Constitución de la República del Ecuador.
- Ley Orgánica de Protección de Datos Personales y su Reglamento General.
- Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).
- Ley Orgánica para la Transformación Digital y Audiovisual.
- Ley Orgánica del Servicio Público (LOSEP) y su Reglamento General.
- Código Orgánico Integral Penal (COIP) - (En lo referente a delitos informáticos y protección de sistemas de la información).

Normativa Gubernamental y Estándares Técnicos:

- Acuerdo Ministerial Nro. 0003-2024, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL).
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0).
- Familia de Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC (27000, 27001, 27002 y 27005) referentes a los Sistemas de Gestión de Seguridad de la Información y la Gestión de Riesgos.

**EGSI**ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN**Documentación Interna Institucional (BCBG):**

- Plan Estratégico Institucional (PEI) del Benemérito Cuerpo de Bomberos de Guayaquil.
- Estatuto Orgánico de Gestión Organizacional por Procesos del BCBG.
- Documento formal de "Definición del Alcance del Esquema Gubernamental de Seguridad de la Información (EGSI)".
- Reglamento Interno disciplinario y normativas de Talento Humano vigentes en la institución.

6. Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	Ing. Juan Carlos Mena Molina Oficial de Seguridad de la Información	 Firmado electrónicamente por: JUAN CARLOS MENA MOLINA
Revisado por:	Ing. María Cielito Mejía Muñoz Directora General de Talento Humano (E)	 Firmado electrónicamente por: MARIA CIELITO
Revisado por:	Ing. Felipe Peralta Velasquez Director General Administrativo (E)	 Firmado electrónicamente por: FELIPE ANTONIO PERALTA VELASQUEZ
Revisado por:	Ing. Johnny Aguayo Aguirre Director General de Tecnologías de la Información y Comunicaciones	 Firmado electrónicamente por: JOHNNY ALBERTO AGUAYO AGUIRRE
Revisado por:	Abg. Eleana Lecaro Monroy Delegada de Protección de Datos Personales	 Firmado electrónicamente por: ELEANA GABRIELA LECARO MONROY
Aprobado por:	Abg. Camila Veloz Jaramillo Directora General de Asesoría Legal (E)	 Firmado electrónicamente por: CAMILA VICTORIA VELOZ JARAMILLO
Aprobado por:	Ing. Diana Tinoco Ajila Directora General de Comunicación Social	 Firmado electrónicamente por: DIANA CAROLINA TINOCO AJILA

**EGSI**ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN

Aprobado por:	Ing. Edwin Angulo Cardona Director General de Planificación Institucional (E)	 Firmado electrónicamente por: EDWIN JOHNNY ANGULO CARDONA
----------------------	--	--

Control de versiones del formato referencial

Versión:	1.1
Fecha de la versión:	31-07-2026
Creado por:	Oficial de Seguridad de la Información del Benemérito Cuerpo de Bomberos de Guayaquil
Aprobado por:	Comité de Seguridad de la Información del Benemérito Cuerpo de Bomberos de Guayaquil
Nivel de confidencialidad:	Bajo

Historial de cambios del formato referencial

Versión	Fecha	Detalle del cambio
1.0	31/07/2026	Emisión inicial del documento