

**EGSI**ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓNSUBSECRETARÍA DE GOBIERNO
ELECTRÓNICO Y REGISTRO CIVIL**FORMATO REFERENCIAL DEL PERFIL DE PROYECTO****1. NOMBRE DEL PROYECTO:**

Implementación del Esquema Gubernamental de Seguridad de la información (EGSI V3)

Programa relacionado:	Gestión de la Seguridad de la Información en las instituciones del sector público EGSi V3
Líder del Proyecto	Juan Carlos Mena Molina, Molina
Fecha de Inicio:	9/7/2026
Fecha de Fin:	17/4/2027

2. CONTEXTUALIZACIÓN DEL PROYECTO**a) Problema:**

El Benemérito Cuerpo de Bomberos de Guayaquil no cuenta actualmente con una política institucional formalizada que regule la clasificación, manejo, acceso, custodia, almacenamiento, difusión y desclasificación de la información generada y administrada por la institución. La ausencia de lineamientos claros incrementa el riesgo de exposición, fuga, alteración o pérdida de información confidencial, reservada y sensible, afectando potencialmente la continuidad operativa, la seguridad ciudadana y el cumplimiento normativo, especialmente respecto al EGSi V3, LOTAIP y la Ley Orgánica de Protección de Datos Personales.

b) Justificación:

La implementación de la Política Específica de Clasificación de la Información es fundamental para cumplir con los controles establecidos en el EGSi V3.0, los cuales demandan que las entidades públicas cuenten con lineamientos documentados y actualizados para proteger adecuadamente la información institucional.

Esta política permitirá establecer criterios uniformes y auditables para la clasificación de la información, garantizando la confidencialidad, integridad y disponibilidad, así como la protección de datos sensibles, reservados y personales. Además, fortalecerá el Sistema de Gestión de Seguridad de la Información del BCBG, reducirá riesgos operativos y facilitará el cumplimiento de obligaciones legales en materia de transparencia, manejo de datos y seguridad de la información.

3. DATOS GENERALES**a) Descripción del Proyecto**

El proyecto consiste en desarrollar, formalizar e implementar la Política Específica de Clasificación de la Información del BCBG, estableciendo criterios, responsabilidades, controles y procedimientos para la adecuada protección y manejo de la información institucional en sus diferentes categorías: pública, confidencial, reservada y sensible.

La política se construirá bajo los lineamientos del EGSi V3.0, la LOTAIP, la Ley de Protección de Datos Personales y la normativa archivística aplicable.

Como parte del proyecto se elaborará una matriz de clasificación, se definirán medidas técnicas y organizativas, se capacitará al personal y se integrará la política al SGSI institucional.

Su implementación permitirá mejorar la gestión de riesgos relacionados con la información, fortalecer la cultura de seguridad documental y reducir amenazas y vulnerabilidades que puedan comprometer activos críticos.

b) Beneficios:

- Disminuir riesgos de fuga, alteración o pérdida de información sensible y confidencial.
- Fortalecer el cumplimiento del EGSÍ V3.0, LOTAIP y la Ley de Protección de Datos Personales.
- Estandarizar el proceso de clasificación y manejo de la información en toda la institución.
- Incrementar la cultura de seguridad y conciencia del personal en el manejo de información.
- Mejorar la trazabilidad y auditoría respecto al tratamiento de la información institucional.
- Garantizar medidas proporcionales para proteger información crítica para la ciudadanía y la operación del BCBG.
- Facilitar procesos de interoperabilidad y coordinación con otras entidades públicas bajo lineamientos claros de clasificación.

3. OBJETIVOS

a) Objetivo general:

Implementar la Política Específica de Clasificación de la Información del Benemérito Cuerpo de Bomberos de Guayaquil para establecer criterios y controles que garanticen la confidencialidad, integridad y disponibilidad de la información institucional conforme al EGSÍ V3.0.

b) Beneficiarios

- Personal operativo y administrativo del BCBG.
- Direcciones responsables de gestión documental, TI y seguridad de la información.
- Ciudadanía que interactúa con los servicios del BCBG.
- Entidades de control y organismos públicos que reciben o intercambian información.

c) Plazo de ejecución

9 de julio de 2026 al 17 de abril de 2027

Incluye:

Elaboración técnica

Validación interdireccional

Aprobación institucional

Socialización

Capacitación

Integración al SGSÍ

d) Cronograma de Ejecución – Actividades

Hitos de control	Fecha comprometida	Fecha estimada	% de avance físico
DEFINICIÓN: 0.1 Perfil de Proyecto EGSÍ v3, documentado y aprobado	9/7/2026	9/7/2026	2,00
PLANEACIÓN: 0.2 Definición del Alcance, documentado y aprobado	10/7/2026	10/7/2026	6,00
PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado	17/7/2026	17/7/2026	4,00
PLANEACIÓN: 0.4 Plan de evaluación Interna, documentado y aprobado	24/7/2026	24/7/2026	4,00
PLANEACIÓN: 0.5 Política de Seguridad de la información (alto nivel), documentado y aprobado	31/7/2026	31/7/2026	7,00
PLANEACIÓN: 0.6 Metodología de evaluación y tratamiento del riesgo, documentado y aprobado	14/9/2026	14/9/2026	10,00
PLANEACIÓN: 0.7 Informe de la Evaluación de los Riesgos, documentado y aprobado	30/9/2026	30/9/2026	12,00
PLANEACIÓN: 0.8 Declaración de Aplicabilidad (SoA), documentado y aprobado	6/10/2026	6/10/2026	2,00
PLANEACIÓN: 0.9 Plan de Tratamiento de los riesgos, documentado y aprobado	12/10/2026	12/10/2026	3,00
EJECUCIÓN: 1.1 Políticas de seguridad de la información (específicas), documentado e implementado	En esta sección se debe planificar la implementación de los controles entre el 13/10/2026 y el 15/02/2027	En esta sección se debe planificar la implementación de los controles entre el 13/10/2026 y el 15/02/2027	0,43
EJECUCIÓN: 1.2 Roles y Responsabilidades de Seguridad de la Información, documentado e implementado			0,43
EJECUCIÓN: 1.3 Separación de Funciones, documentado e implementado			0,43
EJECUCIÓN: 1.4 Responsabilidades de la dirección, documentado e implementado			0,43
EJECUCIÓN: 1.5 Contacto con las autoridades, documentado e implementado			0,43
EJECUCIÓN: 1.6 Contacto con grupos de interés especial, documentado e implementado			0,43
EJECUCIÓN: 1.7 Inteligencia de amenazas, documentado e implementado			0,43

EJECUCIÓN:1.8 Seguridad de la información en la Gestión de proyectos, documentado e implementado
EJECUCIÓN:1.9 Inventario de información y otros activos asociados, documentado e implementado
EJECUCIÓN:1.10 Uso aceptable de la información y otros activos asociados, documentado e implementado
EJECUCIÓN:1.11 Devolución de activos, documentado e implementado
EJECUCIÓN:1.12 Clasificación de la información, documentado e implementado
EJECUCIÓN:1.13 Etiquetado de la información, documentado e implementado
EJECUCIÓN:1.14 Transferencia de información, documentado e implementado
EJECUCIÓN:1.15 Control de Acceso, documentado e implementado
EJECUCIÓN:1.16 Gestión de Identidad, documentado e implementado
EJECUCIÓN:1.17 Información de autenticación, documentado e implementado
EJECUCIÓN:1.18 Derechos de acceso, documentado e implementado
EJECUCIÓN:1.19 Seguridad de la información en las relaciones con proveedores, documentado e implementado
EJECUCIÓN:1.20 Seguridad de la información en los acuerdos con proveedores, documentado e implementado
EJECUCIÓN:1.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC, documentado e implementado
EJECUCIÓN:1.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores, documentado e implementado
EJECUCIÓN:1.23 Seguridad de la información para el uso de servicios en la nube, documentado e implementado
EJECUCIÓN:1.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, documentado e implementado
EJECUCIÓN:1.25 Evaluación y decisión sobre eventos de seguridad de la información, documentado e implementado
EJECUCIÓN:1.26 Respuesta a incidentes de seguridad de la información, documentado e implementado
EJECUCIÓN:1.27 Aprendiendo de los incidentes de seguridad de la información, documentado e implementado
EJECUCIÓN:1.28 Recopilación de evidencias, documentado e implementado
EJECUCIÓN:1.29 Seguridad de la Información durante la interrupción, documentado e implementado
EJECUCIÓN:1.30 Preparación de las TIC para la continuidad del Negocio, documentado e implementado
EJECUCIÓN:1.31 Requisitos legales, estatutarios, reglamentarios y contractuales, documentado e implementado
EJECUCIÓN:1.32 Derechos de propiedad intelectual, documentado e implementado
EJECUCIÓN:1.33 Protección de los registros, documentado e implementado
EJECUCIÓN:1.34 Privacidad y protección de PII, documentado e implementado
EJECUCIÓN:1.35 Revisión independiente de seguridad de la información, documentado e implementado
EJECUCIÓN:1.36 Cumplimiento de políticas, reglas y normas de seguridad de la información, documentado e implementado
EJECUCIÓN:1.37 Procedimientos operativos, documentado e implementado
EJECUCIÓN:2.1 Selección de personas, documentado e implementado
EJECUCIÓN:2.2 Términos y condiciones de empleo, documentado e implementado e implementado
EJECUCIÓN:2.4 Proceso disciplinario, documentado e implementado
EJECUCIÓN:2.5 Responsabilidades después de la terminación o cambio de empleo, documentado e implementado
EJECUCIÓN:2.6 Acuerdo de confidencialidad o no divulgación, documentado e implementado
EJECUCIÓN:2.7 Trabajo remoto, documentado e implementado
EJECUCIÓN:2.8 Reporte de eventos de seguridad de la información, documentado e implementado
EJECUCIÓN:3.1 Perímetros de seguridad física, documentado e implementado
EJECUCIÓN:3.2 Entrada física, documentado e implementado
EJECUCIÓN:3.3 Seguridad de oficinas, despachos e instalaciones, documentado e implementado
EJECUCIÓN:3.4 Monitoreo de seguridad física, documentado e implementado
EJECUCIÓN:3.5 Protección contra las amenazas externas y ambientales, documentado e implementado
EJECUCIÓN:3.6 Trabajo en áreas seguras, documentado e implementado

EJECUCIÓN:3.7 Puesto de trabajo despejado y pantalla limpia, documentado e implementado			0,43
EJECUCIÓN:3.8 Ubicación y protección de equipos, documentado e implementado			0,43
EJECUCIÓN:3.9 Seguridad de los activos fuera de las instalaciones, documentado e implementado			0,43
EJECUCIÓN:3.10 Medios de almacenamiento, documentado e implementado			0,43
EJECUCIÓN:3.11 Servicios de Soporte, documentado e implementado			0,43
EJECUCIÓN:3.12 Seguridad del cableado, documentado e implementado			0,43
EJECUCIÓN:3.13 Mantenimiento de equipo, documentado e implementado			0,43
EJECUCIÓN:3.14 Eliminación segura o reutilización de equipos, documentado e implementado			0,43
EJECUCIÓN:4.1 Dispositivos de usuario final, documentado e implementado			0,43
EJECUCIÓN:4.2 Derechos de acceso privilegiado, documentado e implementado			0,43
EJECUCIÓN:4.3 Restricción de acceso a la información, documentado e implementado			0,43
EJECUCIÓN:4.4 Acceso al código fuente, documentado e implementado			0,43
EJECUCIÓN:4.5 Autenticación Segura, documentado e implementado			0,43
EJECUCIÓN:4.6 Gestión de la capacidad, documentado e implementado			0,43
EJECUCIÓN:4.7 Protección contra malware, documentado e implementado			0,43
EJECUCIÓN:4.8 Gestión de vulnerabilidades técnicas, documentado e implementado			0,43
EJECUCIÓN:4.9 Gestión de la Configuración, documentado e implementado			0,43
EJECUCIÓN:4.10 Eliminación de información, documentado e implementado			0,43
EJECUCIÓN:4.11 Enmascaramiento de datos, documentado e implementado			0,43
EJECUCIÓN:4.12 Prevención de fuga de datos, documentado e implementado			0,43
EJECUCIÓN:4.13 Copia de seguridad de la información, documentado e implementado			0,43
EJECUCIÓN:4.14 Redundancia de las instalaciones de tratamiento de información			0,43
EJECUCIÓN:4.15 Registros de eventos, documentado e implementado			0,43
EJECUCIÓN:4.16 Actividades de monitoreo, documentado e implementado			0,43
EJECUCIÓN:4.17 Sincronización de reloj, documentado e implementado			0,43
EJECUCIÓN:4.18 Uso de programas de utilidad privilegiados, documentado e implementado			0,43
EJECUCIÓN:4.19 Instalación de software en sistemas operativos, documentado e implementado			0,43
EJECUCIÓN:4.20 Seguridad de redes, documentado e implementado			0,43
EJECUCIÓN:4.21 Seguridad de los servicios de red, documentado e implementado			0,43
EJECUCIÓN:4.22 Separación en las redes, documentado e implementado			0,43
EJECUCIÓN:4.23 Filtrado web, documentado e implementado			0,43
EJECUCIÓN:4.24 Uso de criptografía, documentado e implementado			0,43
EJECUCIÓN:4.25 Ciclo de vida de desarrollo seguro, documentado e implementado			0,43
EJECUCIÓN:4.26 Requisitos de seguridad de la aplicación, documentado e implementado			0,43
EJECUCIÓN:4.27 Arquitectura del sistema seguro y principios de ingeniería, documentado e implementado			0,43
EJECUCIÓN:4.28 Codificación Segura, documentado e implementado			0,43
EJECUCIÓN:4.29 Pruebas de seguridad en el desarrollo y la aceptación, documentado e implementado			0,43
EJECUCIÓN:4.30 Desarrollo subcontratado, documentado e implementado			0,43
EJECUCIÓN:4.31 Separación de los entornos de desarrollo, prueba y producción, documentado e implementado			0,43
EJECUCIÓN:4.32 Gestión de cambios, documentado e implementado			0,43
EJECUCIÓN:4.33 Información de pruebas, documentado e implementado			0,43
EJECUCIÓN:4.34 Protección de los sistemas de información durante las pruebas de auditoría, documentado e implementado			0,43
EJECUCIÓN: 0.10 Informe del monitoreo del desempeño y los indicadores de la gestión del EGSi v3, documentado y aprobado	26/2/2027	26/2/2027	2,00
EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSi v3, documentado y aprobado	8/3/2027	8/3/2027	1,00
EJECUCIÓN: 0.12 Informe de los resultados de la revisión de la gestión del EGSi v3, documentado y aprobado	18/3/2027	18/3/2027	2,00
EJECUCIÓN: 0.13 Informe de los resultados de las medidas correctivas aplicadas al EGSi v3, documentado y aprobado	28/3/2027	28/3/2027	2,00
EJECUCIÓN: 0.14 Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información, documentado y aprobado	7/4/2027	7/4/2027	2,00
CIERRE: 0.0.15 Informe de cierre del proyecto EGSi v3, documentado y aprobado	17/4/2027	17/4/2027	1,00
TOTAL			100,00

4. FIRMAS DE RESPONSABILIDAD - EQUIPO DEL PROYECTO

Nombre del funcionario	Puesto	Unidad	Firma
Ing. Juan Carlos Mena Molina	Oficial de Seguridad	Primera Jefatura	 Firmado electrónicamente por: JUAN CARLOS MENA MOLINA
Ing. María Cielito Mejía Muñoz	[miembro 1 - de Comité de Seguridad de la Información]	Dirección General de Talento Humano	 Firmado electrónicamente por: MARIA CIELITO
Ing. Felipe Peralta Velasquez	[miembro 2 - de Comité de Seguridad de la Información]	Dirección General Administrativa	 Firmado electrónicamente por: FELIPE ANTONIO PERALTA VELASQUEZ
Ing. Johnny Aguayo Aguirre	[miembro 3- de Comité de Seguridad de la Información]	Dirección General de Tecnologías de la Información y Comunicaciones	 Firmado electrónicamente por: JOHNNY ALBERTO AGUAYO AGUIRRE
Abg. Eleana Lecaro Monroy	[miembro 4 - de Comité de Seguridad de la Información]	Primera Jefatura	 Firmado electrónicamente por: ELEANA GABRIELA LECARO MONROY
Abg. Camila Veloz Jaramillo	[miembro 5 - de Comité de Seguridad de la Información]	Dirección General de Asesoría Legal	 Firmado electrónicamente por: CAMILA VICTORIA VELOZ JARAMILLO
Ing. Diana Tinoco Ajila	[miembro 6 - de Comité de Seguridad de la Información]	Dirección General de Comunicación Social	 Firmado electrónicamente por: DIANA CAROLINA TINOCO AJILA
Ing. Edwin Angulo Cardona	Presidente del Comité de Seguridad de la Información	Dirección General de Planificación Institucional	 Firmado electrónicamente por: EDWIN JOHNNY ANGULO CARDONA