EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

SUBSECRETARÍA DE GOBIERNO ELECTRÓNICO Y REGISTRO CIVIL

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	*Angel Dionicio Franco Calixto*
Fecha de Inicio:	*14/7/2025*
Fecha de Fin:	*6/7/2026*

2. CONTEXTUALIZACIÓN DEL PROYECTO

a) Problema:

Los sistemas desarrollados y aplicaciones utilizadas en la institución no cuentan con una política de seguridad de la información, ni requerimientos básicos para su parametrización a nivel de seguridad informática y de la información. Las reglas establecidas espontáneamente por la Dirección de Planificación, Procesos y Tecnología aún no han sido socializadas y avaladas por la Máxima Autoridad, dejando a la institución inmersa en un proceso improvisado para asignar permisos, accesos y restricciones a la infraestructura, paquetes y sistemas informáticos, así como a la información siendo una gran debilidad para la Dirección de Planificación, Procesos y Tecnología. Actualmente no se cuenta con una política de seguridad de la información aprobada que permita establecer los parámetros apropiados para salvaguardar la confidencialidad, disponibilidad e integridad de la infraestructura tecnológica, aplicaciones e información institucional.

b) Justificación:

La implementación del EGSI V3.0 reducirá significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física como electrónica, que procesa la institución. Así mismo, contribuirá a establecer un proceso de mejora continua de la gestión de la seguridad de la información y crear cultura y conciencia en los/as servidores/as públicos/as en cuanto al manejo de la información que utilizan para cumplir sus funciones, sea esta, institucional o de la ciudadanía.

3. DATOS GENERALES

a) Descripción del Proyecto

El presente proyecto tiene como objetivo cumplir con los 108 hitos establecidos en GPR que corresponde a los requisitos y controles que comprende la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI V3) conforme se establece en el Acuerdo Ministerial No. MINTEL-MINTEL-2024-003 publicado en el registro oficial del 1 de marzo de 2024.

Los requisitos y controles a implementar y que han sido homologadas como hitos del proyecto tienen un plazo de ejecución de 12 meses.

La implementación del EGSI V3.0 reducirá significativamente amenazas, riesgos y vulnerabilidades relacionadas a la gestión de la información, tanto física como electrónica, que procesa la institución. Así mismo, contribuirá a establecer un proceso de mejora continua de la gestión de la seguridad de la información e incrementar la cultura de los servidores públicos en cuanto al manejo de la información que utilizan para cumplir sus funciones sea esta institucional o de la ciudadanía.

b) Beneficios:

• Identificar, cuantificar y priorizar las amenazas, riesgos y vulnerabilidades que puedan afectar la seguridad de la información de la institución.
• Proporcionar a autoridades de la entidad soporte para la gestión de la seguridad de la información, en concordancia con la constitución, las leyes y demás normativa legal vigente.
• Contar con estructuras de evaluación y gestión de riesgos de la organización, así como la definición de las responsabilidades individuales de cada miembro a nivel de seguridad con los respectivos acuerdos de confidencialidad.
• Aplicar los estándares internacionales (ISO/IEC 27000) adoptados como normas técnicas ecuatorianas para la gestión de la seguridad de la información.
• Incrementar el conocimiento y cultura de los servidores públicos en cuanto a la gestión de la seguridad de la información que utilizan.
• Implementar medidas para evitar problemas y consecuencias no deseadas de un manejo no adecuado de la gestión de la seguridad de la información.
• Compartir información y poner en conocimiento incidentes de seguridad de la información que afecten a la institución o al gobierno en su conjunto, en coordinación con el MINTEL.

3. OBJETIVOS

a) Objetivo general:

Implementar el Esquema Gubernamental de Seguridad de la información EGSI V3, apegados a las disposiciones emitidas en el Acuerdo Ministerial MINTEL-MINTEL-2024-003 en la Empresa Pública de Comunicación del Ecuador EP, para minimizar los riesgos de los activos de información críticos de la institución.

b) Beneficiarios

Empresa Pública de Comunicación del Ecuador EP, entidades públicas o privadas, servidores públicos, Gobierno, Ciudadanía.

c) Plazo de ejecución

Se ha iniciado la ejecución de algunas actividades relacionadas a seguridad de la información, con la finalidad de dar fiel cumplimiento a lo estipulado por el ente de control, por lo que se han llevado a cabo varias acciones durante los años 2021, 2022, 2023, 2024 y 2025. Se planifica la ejecución del presente proyecto en dos partes, las fases de definición y planeación desde julio de 2025 y las fases de ejecución y cierre desde diciembre de 2025 hasta julio de 2026, el cronograma de principales hitos detalla la fecha de cumplimiento, los entregables y medios de verificación.

d) Cronograma de Ejecución – Actividades

Hitos de control	Fecha comprometida	Fecha estimada	% de avance físico
DEFINICIÓN: 0.1 Perfil de Proyecto EGSI v3, documentado y aprobado	*14/7/2025*	*14/7/2025*	2,00
PLANEACIÓN: 0.2 Definición del Alcance, documentado y aprobado	*22/8/2025*	*22/8/2025*	6,00
PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado	*4/9/2025*	*4/9/2025*	4,00
PLANEACIÓN: 0.4 Plan de evaluación Interna, documentado y aprobado	*10/9/2025*	*10/9/2025*	4,00
PLANEACIÓN: 0.5 Política de Seguridad de la información (alto nivel), documentado y aprobado	*20/9/2025*	*20/9/2025*	7,00
PLANEACIÓN: 0.6 Metodología de evaluación y tratamiento del riesgo, documentado y aprobado	*3/10/2025*	*3/10/2025*	10,00
PLANEACIÓN: 0.7 Informe de la Evaluación de los Riesgos, documentado y aprobado	*5/12/2025*	*5/12/2025*	12,00
PLANEACIÓN: 0.8 Declaración de Aplicabilidad (SoA), documentado y aprobado	*15/12/2025*	*15/12/2025*	2,00
PLANEACIÓN: 0.9 Plan de Tratamiento de los riesgos, documentado y aprobado	*19/12/2025*	*19/12/2025*	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 22/12/2025 y el 04/4/2026*	*En esta sección se debe planificar la implementación de los controles entre el 22/12/2025 y el 04/4/2026*	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			0,43
EJECUCIÓN:1.9 Inventario de información y otros activos asociados, documentado e implementado			0,43
EJECUCIÓN:1.10 Uso aceptable de la información y otros activos asociados, documentado e implementado			0,43
EJECUCIÓN:1.11 Devolución de activos, documentado e implementado			0,43
EJECUCIÓN:1.12 Clasificación de la información, documentado e implementado			0,43
EJECUCIÓN:1.13 Etiquetado de la información, documentado e implementado			0,43
EJECUCIÓN:1.14 Transferencia de información, documentado e implementado			0,43
EJECUCIÓN:1.15 Control de Acceso, documentado e implementado			0,43
EJECUCIÓN:1.16 Gestión de Identidad, documentado e implementado			0,43
EJECUCIÓN:1.17 Información de autenticacion, documentado e implementado			0,43
EJECUCIÓN:1.18 Derechos de acceso, documentado e implementado			0,43
EJECUCIÓN:1.19 Seguridad de la información en las relaciones con proveedores, documentado e implementado			0,43
EJECUCIÓN:1.20 Seguridad de la información en los acuerdos con proveedores, documentado e implementado			0,43
EJECUCIÓN:1.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC, documentado e implementado			0,43
EJECUCIÓN:1.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores, documentado e implementado			0,43
EJECUCIÓN:1.23 Seguridad de la información para el uso de servicios en la nube, documentado e implementado			0,43
EJECUCIÓN:1.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, documentado e implementado			0,43
EJECUCIÓN:1.25 Evaluación y decisión sobre eventos de seguridad de la información, documentado e implementado			0,43
EJECUCIÓN:1.26 Respuesta a incidentes de seguridad de la información, documentado e implementado			0,43
EJECUCIÓN:1.27 Aprendiendo de los incidentes de seguridad de la información, documentado e implementado			0,43
EJECUCIÓN:1.28 Recopilación de evidencias, documentado e implementado			0,43
EJECUCIÓN:1.29 Seguridad de la Información durante la interrupción, documentado e implementado			0,43
EJECUCIÓN:1.30 Preparación de las TIC para la continuidad del Negocio, documentado e implementado			0,43
EJECUCIÓN:1.31 Requisitos legales, estatutarios, reglamentarios y contractuales, documentado e implementado			0,43
EJECUCIÓN:1.32 Derechos de propiedad intelectual, documentado e implementado			0,43
EJECUCIÓN:1.33 Protección de los registros, documentado e implementado			0,43
EJECUCIÓN:1.34 Privacidad y protección de PII, documentado e implementado			0,43

EJECUCIÓN:1.35 Revisión independiente de seguridad de la información, documentado e implementado			0,43
EJECUCIÓN:1.36 Cumplimiento de políticas, reglas y normas de seguridad de la información, documentado e implementado			0,43
EJECUCIÓN:1.37 Procedimientos operativos, documentado e implementado			0,43
EJECUCIÓN:2.1 Selección de personas, documentado e implementado			0,43
EJECUCIÓN:2.2 Términos y condiciones de empleo, documentado e implementado			0,43
documentado e implementado			0,43
EJECUCIÓN:2.4 Proceso disciplinario, documentado e implementado			0,43
EJECUCIÓN:2.5 Responsabilidades después de la terminación o cambio de empleo, documentado e implementado			0,43
EJECUCIÓN:2.6 Acuerdo de confidenciliadad o no divulgación, documentado e implementado			0,43
EJECUCIÓN:2.7 Trabajo remoto, documentado e implementado			0,43
EJECUCIÓN:2.8 Reporte de eventos de seguridad de la información, documentado e implementado			0,43
EJECUCIÓN:3.1 Perímetros de seguridad física, documentado e implementado			0,43
EJECUCIÓN:3.2 Entrada física, documentado e implementado			0,43
EJECUCIÓN:3.3 Seguridad de oficinas, despachos e instalaciones, documentado e implementado			0,43
EJECUCIÓN:3.4 Monitoreo de seguridad física, documentado e implementado			0,43
EJECUCIÓN:3.5 Protección contra las amenazas externas y ambientales, documentado e implementado			0,43
EJECUCIÓN:3.6 Trabajo en áreas seguras, documentado e implementado			0,43
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 Proteccion 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	*6/5/2026*	*6/5/2026*	2,00
EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado	*20/5/2026*	*20/5/2026*	1,00

EJECUCIÓN: 0.12 Informe de los resultados de la revisión de la gestión del EGSI v3, documentado y aprobado	*5/6/2026*	*5/6/2026*	2,00
EJECUCIÓN: 0.13 Informe de los resultados de las medidas correctivas aplicadas al EGSI v3, documentado y aprobado	*22/6/2026*	*22/6/2026*	2,00
EJECUCIÓN: 0.14 Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información, documentado y aporbado	*1/7/2026*	*1/7/2026*	2,00
CIERRE: 0.0.15 Informe de cierre del proyecto EGSI v3, documentado y aprobado	*6/7/2026*	*6/7/2026*	1,00
		TOTAL	*100,00*

4. FIRMAS DE RESPONSABILIDAD - EQUIPO DEL PROYECTO

Nombre del funcionario	Puesto	Unidad	Firma
Andrea Soledad Benavides Peñafiel	*Directora de Planificación, Procesos y Tecnología*	*Dirección de Planificación, Procesos y Tecnología*	Firmado electrónicamente por: ANDREA SOLEDAD BENAVIDES PENAFIEL Validar únicamente con FirmaEC
Ana Lizbeth Brito Figueroa	*Directora Administrativo y Talento Humano*	*Dirección Administrativa y Talento Humano*	Firmado electrónicamente por: ANA LIZBETH BRITO FIGUEROA Validar únicamente con FirmaEC
Grace Vanessa Cordero Loor	*Coordinadora General de Medios*	*Coordinación General de Medios*	Firmado electrónicamente por: GRACE VANESSA CORDERO LOOR Validar únicamente con FirmaEC
Jose Gabriel Estrella Lopez	*Jefe de Asesoría Jurídica*	*Coordinación General de Asesoria Jurídica*	Firmado electrónicamente por: JOSE GABRIEL ESTRELLA LOPEZ Validar únicamente con FirmaEC
Omar Guillermo Barrera Romero	*Especialista de Planificación y Desarrollo Tecnológico (Delegado de Protección de Datos)*	*Dirección de Planificación, Procesos y Tecnología*	Firmado electrónicamente por: OMAR GUILLERMO BARRERA ROMERO Validar únicamente con FirmaEC
Angel Dionicio Franco Calixto	*Especialista de Infraestructura, Soporte Técnico y Seguridad de la Información (Oficial de Seguridad de la Información)*	*Dirección de Planificación, Procesos y Tecnología*	Firmado electrónicamente por: ANGEL DIONICIO FRANCO CALIXTO Validar únicamente con FirmaEC