PLAN DE EVALUACIÓN INTERNA

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI versión 3.0)

SEPTIEMBRE 2025

Dirección: San Salvador E6-49 y Eloy Alfaro
Código Postal: 170518 / Quito - Ecuador
Cel: (+593) 987 777 778
www.comunica.ec

Tabla de contenido

1. Antecedentes

El Ministerio de Telecomunicaciones y de la Sociedad de la Información, mediante Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 expidió el Esquema Gubernamental de Seguridad de la Información – EGSI, el cual es el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información y es de implementación obligatoria en las entidades, organismos e instituciones del sector público, de conformidad con lo establecido en el artículo 225 de la Constitución de la República del Ecuador.

El presente plan de evaluación interna se desarrolla en el contexto de la evaluación del Esquema Gubernamental de Seguridad de la Información (EGSI) en la Empresa Pública de Comunicación del Ecuador EP. El EGSI se estableció con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información crítica de la Empresa Pública de Comunicación del Ecuador EP, así como de los activos relacionados con la información.

La Empresa Pública de Comunicación del Ecuador EP opera en el sector de las comunicaciones, proporcionando los siguientes servicios: radiodifusión, televisión y noticias web. La dependencia de los sistemas de información y la sensibilidad de la información gestionada en la institución han llevado a la implementación del EGSI conforme a lo establecido en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, el cual está basado en las normas ISO/IEC 27001:2022, ISO/IEC 27005:2022 e ISO/IEC 27002:2022.

La Empresa Pública de Comunicación del Ecuador EP reconoce la importancia de mantener un Sistema de Gestión robusto y efectivo para proteger sus activos de información y mantener la confianza de sus partes interesadas, incluidos: ciudadanos, instituciones públicas, empresas privadas, otras.

En el presente plan de evaluación interna, se hará referencia a definiciones clave establecidas en el Esquema Gubernamental de Seguridad de la Información, así como a documentación interna pertinente, como políticas, procedimientos y registros de implementación del EGSI V3.

2. Objetivo del documento

El objetivo de este plan de evaluación interna del Esquema Gubernamental de Seguridad de la Información (EGSI) es establecer las actividades a realizar en el proceso de evaluación interna, con el fin de identificar no conformidades, riesgos y oportunidades, que permitan evaluar la efectividad, eficiencia y adecuación del EGSI implementado en la Empresa Pública de Comunicación del Ecuador EP en cumplimiento con los requisitos de seguridad de la información establecidos por EGSI, las normas ISO relacionadas y otros estándares relevantes.

Objetivos específicos:

- Planificar las actividades que se deben seguir para realizar el proceso de evaluación interna del EGSI en la institución que contemple: Definir recursos (personal y económicos) que va a auditar, áreas que serán auditadas, infraestructura, alcance de la auditoría, cronograma para la ejecución de la auditoría, fases en las que se realizará la

evaluación, revisión de los requisitos del sistema de gestión así como evaluar la implementación y el funcionamiento de los controles de seguridad de acuerdo con las políticas y procedimientos establecidos en el EGSI. La documentación interna pertinente, como políticas, procedimientos y registros de implementación del EGSI V3.

3. Plan de Evaluación interna del EGSI V3

3.1 Alcance

El alcance de esta evaluación interna cubrirá todas las áreas y procesos relacionados con la implementación del EGSI V3 en la Empresa Pública de Comunicación del Ecuador EP, incluyendo, pero no limitado a:

Jefatura de Asesoría Jurídica

- Elaboración de contratos y convenios

Dirección Administrativa y de Talento Humano

- Administración y coordinación de la gestión archivística
- Registro, despacho y seguimiento documental
- Administración del programa de seguros
- Movilización vehicular
- Inventario y matriculación vehicular
- Mantenimiento preventivo y correctivo vehicular
- Elaboración y reforma al PAC
- Capacitación
- Cultura organizacional
- Desvinculación y liquidación de haberes
- Elaboración, ejecución y evaluación del plan de vigilancia de salud
- Evaluación de desempeño
- Gestión de requerimientos de actos administrativos de la dirección de talento humano
- Nómina
- Reclutamiento, selección, vinculación e inducción de personal
- Seguridad industrial y responsabilidad social
- Seguridad y salud ocupacional
- Viáticos y movilización de personal

Dirección Financiera

- Administración de Caja Chica
- Fondos a Rendir Cuentas
- Cierre contable y generación de estados financieros
- Cuentas por Cobrar
- Etapas del ciclo presupuestario

- Facturación

Dirección de Planificación, Procesos y Tecnología

- Acciones correctivas
- Análisis de contexto y partes interesadas
- Medición, seguimiento y control de indicadores
- Seguimiento a recomendaciones emitidas por entes de control
- Identificación, análisis y evaluación de riesgos
- Levantamiento, diseño y mejoramiento de procesos
- Administración y monitoreo
- Desarrollo y mantenimiento de aplicativos
- Gobierno de tecnología de la información
- Infraestructura
- Soporte a usuarios

Jefatura de Comercialización

- Autopautas y autopromociones
- Canjes
- Venta de avisos judiciales
- Venta de espacios publicitarios
- Tráfico

Jefatura de Operaciones

- Generación de material Audiovisual
- Mantenimiento preventivo y correctivo de equipos y sistemas de la gestión de planta
- Contingencia ante fallas de energía eléctrica
- Alquiler de infraestructura y equipos con personal técnico especializado

Jefatura de Contenidos

- Producción y programación de noticias
- Producción y Programación de deportes
- Planificación y programación de medios digitales
- Producción y programación de programas de radio

Jefatura de Producción

- Producción de Televisión
- Promoción de Televisión

Jefatura de Programación y Transmisión

- Programación de televisión de señal internacional

- Programación de televisión de señal nacional
- Recepción, análisis e ingesta de contenidos audiovisuales

La evaluación interna comprenderá la validación del cumplimiento de:

- Requisitos de implementación del EGIS V3
- Política de seguridad de la información
- Evaluación de riesgos
- Planificación y control de acceso
- Gestión de activos de información
- Seguridad física y ambiental
- Gestión de incidentes de seguridad
- Gestión de la continuidad del negocio
- Cumplimiento legal y contractual

3.2 Criterios

Los criterios definidos y considerados para la ejecución de la evaluación interna de la implementación del Esquema Gubernamental de Seguridad de la Información – EGSI v3 en la Empresa Pública de Comunicación del Ecuador EP, se detallan a continuación:

- Normativas y estándares de seguridad
- Políticas y procedimientos internos
- Controles de seguridad
- Gestión de riesgos
- Acceso y gestión de la identidad
- Capacitación y concienciación en seguridad
- Monitoreo y mejora continua

Normativas y estándares de seguridad: permitirá confirmar el cumplimiento del Acuerdo Ministerial Nro. 2024-003, los artículos, disposiciones; además de la Norma Técnica – EGSI V3 y estándares relevantes de seguridad de la información que la organización haya adoptado.

Políticas y procedimientos internos: permitirá revisar las políticas y procedimientos internos relacionados con la seguridad de la información para garantizar que estén alineados con los objetivos del EGSI y que se estén implementando adecuadamente en toda la institución. Validad la formalización, actualización y difusión de estos documentos.

Controles de seguridad: permitirá validar conjuntamente con los propietarios de los activos, la efectividad de los controles de seguridad de la información implementados, para proteger los activos de información de la institución. Esto puede incluir controles físicos, lógicos y de procedimientos.

Gestión de riesgos: permitirá validar la gestión de riesgos aplicada en el EGSI, para asegurarse de que se estén identificando, evaluando y tratando adecuadamente los riesgos de seguridad de la información de la institución.

Acceso y gestión de la identidad: permitirá examinar los controles relacionados con el acceso y la gestión de la identidad para garantizar que se estén aplicando adecuadamente los principios de mínimos privilegios y que se estén protegiendo adecuadamente los datos confidenciales.

Capacitación y concienciación en seguridad: permitirá evaluar la efectividad de los programas de capacitación y concienciación en seguridad para el personal de la institución, asegurándose de que tengan la capacidad para identificar y responder adecuadamente a las amenazas de seguridad.

Monitoreo y mejora continua: permitirá evaluar los procesos de monitoreo y mejora continua del EGSI para asegurarse de que se estén identificando y abordando proactivamente las áreas de mejora en la seguridad de la información.

3.3 Metodología

La evaluación interna se llevará a cabo con la metodología establecida en la Empresa Pública de Comunicación del Ecuador EP y en las siguientes etapas:

Revisión documental: revisión de la documentación relacionada con el EGSI V3, incluyendo políticas, procedimientos, registros y otros documentos pertinentes; estos documentos deberán al menos tener evidencias de formalización (firmas de responsabilidad), actualización (versionamiento), socialización (registro de publicación, compartición a las partes interesadas)

Entrevistas: entrevista con los propietarios de los activos de información y el personal clave, para evaluar el conocimiento y la aplicación de las políticas y procedimientos de seguridad de la información.

Inspección física: inspección física de las instalaciones para evaluar la seguridad física y ambiental.

Pruebas técnicas: validación y/o evaluación de controles técnicos implementados para proteger la información.

3.4 Cronograma

En la Empresa Pública de Comunicación del Ecuador EP para la ejecución de la evaluación interna se ha planificado con las partes interesadas/involucradas el siguiente cronograma:

Fecha de inicio: 12/septiembre/2025

Fecha de fin: 31/diciembre/2025

Lugar: San Salvador E6-49 y Eloy Alfaro

Unidades Organizativas: Jefatura de Asesoría Jurídica, Dirección Administrativa y Talento Humano, Dirección Financiera, Dirección de Planificación, Procesos y Tecnología, Jefatura de Comercialización, Jefatura de Operaciones, Jefatura de Contenidos, Jefatura de Producción, Jefatura de Programación y Transmisión.

El detalle de las actividades a realizar y los tiempos establecidos se encuentran en el siguiente cronograma: (ANEXO 1).

3.5 Recursos necesarios

La máxima autoridad y/o Comité de Seguridad de la Información de la Empresa Pública de Comunicación del Ecuador EP, para ejecutar las respectivas evaluaciones deberá proveer los siguientes recursos:

- Herramientas: Equipos de cómputo, sistemas de información, impresoras, correo electrónico institucional, otros
- Materiales: Listas de verificación, presentaciones, otros
- Humanos: Equipo de trabajo para ejecutar la evaluación interna.
- Financieros: Presupuesto asignado $0.00

Para la ejecución de la evaluación interna se ha elaborado listas de verificación para la revisión del cumplimiento de los requisitos y controles de seguridad del Esquema Gubernamental de Seguridad de la Información (ANEXO 2, ANEXO 3).

3.6 Documentación de Hallazgos

Durante el proceso de evaluación interna en la Empresa Pública de Comunicación del Ecuador EP, se deberá documentar los hallazgos identificados en cada una de las revisiones, para lo cual se debe considerar:

- *Evidencia Recopilada*: documentar la evidencia recopilada que respalda los hallazgos identificados
- *Valoración del cumplimiento*: establecer la valoración respectiva de acuerdo a la tabla de valoración definida.
- *No Conformidades*: documentar detalladamente las no conformidades encontradas durante la evaluación interna
- *Priorización de Hallazgos*: Clasificación de hallazgos según su valoración, con el fin de establecer recomendaciones para mejorar el sistema de gestión de seguridad de la información (EGSI).

TABLA DE VALORACIÓN DEL CUMPLIMIENTO REQUISITOS Y CONTROLES DE SEGURIDAD		
CUMPLIMIENTO	**DESCRIPCIÓN PARA EL NIVEL/ ESTADO DEL SISTEMA DE GESTIÓN**	**VALORACIÓN**
0%	No establecen medidas de seguridad de la información: no se tiene conciencia de la importancia de la seguridad de la información en la institución y no se reconoce la información como un activo importante para su misión y el cumplimiento de los objetivos estratégicos.	**NO CONFORMIDAD MAYOR**
1% - 20%	Se tiene la iniciativa y necesidad de implementar el Esquema Gubernamental de Seguridad de la información, pero no se encuentra formalizado: no se ha identificado activos de información (o se tiene de manera general) y la evaluación de riesgos, que permita determinar el grado de criticidad de la información.	
21% - 40%	Se tiene procesos básicos para la Gestión de la Seguridad de la información: los funcionarios de la institución tienen conciencia sobre la seguridad de la información, pero no se identifica un compromiso real. No participa toda la institución en el proceso, se deja la responsabilidad a cada funcionario. La gestión de la institución es reactiva. El proceso de mejora continua se realiza paulatinamente.	**NO CONFORMIDAD MENOR**
41% - 60%	La Gestión de la Seguridad de la Información se ha estandarizado, documentado y ha sido difundida: toda la institución participa en el proceso y la gestión es más proactiva que reactiva. Existe avances en el proceso de mejora continua.	**OPORTUNIDAD DE MEJORA**
61% - 80%	La Gestión de la Seguridad de la Información se monitorea y mide su cumplimiento. Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. El proceso de mejora continua es adecuado y formalizado.	
81% - 100%	La Gestión de la Seguridad de la Información se encuentra en continua mejora: existe evidencia de la mejora continua, se ha establecido que la seguridad de la información es un valor agregado para la institución. Los funcionarios apoyan y contribuyen al mejoramiento de la seguridad de la información.	**CONFORME**

Tabla 1: Valoración del cumplimiento, requisitos y controles de seguridad

3.7 Resultados

Una vez ejecutado el proceso de evaluación o revisión, el "equipo evaluador" deberá elaborar

El Informe de la Evaluación Interna, que tendrá como objetivo informar el resultado de la evaluación interna ejecutada, en donde se evidencie las insuficiencias en el sistema de gestión, las potenciales situaciones de riesgo, las oportunidades de mejora, el cumplimiento de los requisitos y controles establecidos en el Esquema Gubernamental de Seguridad, a través de los hallazgos y no conformidades identificadas; esto con el fin de proporcionar a las autoridades, información útil y valiosa, que permita adoptar las acciones de mejora necesarias.

Si el resultado de la evaluación interna incluye no conformidades, el Oficial de Seguridad de la Información deberá preparar un plan de acción.

Plan de acción para cada no conformidad que se deberá acordar con el "Líder del equipo evaluador". Un plan de acción de monitoreo que incluya:

- Descripción de la no conformidad detectada;
- Descripción de la (s) causa (s) de la no conformidad;
- Descripción de la corrección a corto plazo y la acción correctiva a más largo plazo para eliminar una "no conformidad" detectada dentro de un plazo definido; y
- Las personas responsables de la ejecución del plan.

4. Glosario de términos

Término	Definición
EGSI	Esquema Gubernamental de Seguridad de la Información
CSI	Comité de Seguridad de la Información
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información
PAC	Plan Anual de Contratación
OSI	Oficial de Seguridad de la Información

5. Documentos de referencia

- Acuerdo Ministerial MINTEL-MINTEL-2024-003.
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, NTE INEN-ISO/IEC 27002, NTE INEN-ISO/IEC 27005
- Reglamento Interno del Comité de Seguridad de la Información.

6. Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	**Mgs. Angel Franco Calixto** Oficial de Seguridad de la Información	Firmado electrónicamente por: ANGEL DIONICIO FRANCO CALIXTO Validar únicamente con FirmaEC
Revisado y aprobado por:	**Eco. Mónica Salas Herrera** Presidente del Comité de Seguridad de la Información	Firmado electrónicamente por: MONICA KATIUSCA SALAS HERRERA Validar únicamente con FirmaEC
Aprobado por:	**Lcda. Ana Lizbeth Brito Figueroa** Integrante del Comité de Seguridad de la Información	Firmado electrónicamente por: ANA LIZBETH BRITO FIGUEROA Validar únicamente con FirmaEC
Aprobado por:	**Mgs. Grace Cordero Loor** Integrante del Comité de Seguridad de la Información	Firmado electrónicamente por: GRACE VANESSA CORDERO LOOR Validar únicamente con FirmaEC
Aprobado por:	**Espc. José Estrella Lopez** Integrante del Comité de Seguridad de la Información	Firmado electrónicamente por: JOSE GABRIEL ESTRELLA LOPEZ Validar únicamente con FirmaEC
Aprobado por:	**Mgs. Omar Barrera Romero** Integrante del Comité de Seguridad de la Información	Firmado electrónicamente por: OMAR GUILLERMO BARRERA ROMERO Validar únicamente con FirmaEC

Control de versiones

Versión:	1.0
Fecha de la versión:	11-09-2025
Creado por:	Oficial de Seguridad de la Información de la Empresa Pública de Comunicación del Ecuador EP
Revisado por:	Comité de Seguridad de la Información de la Empresa Pública de Comunicación del Ecuador
Aprobado por:	Empresa Pública de Comunicación del Ecuador
Nivel de confidencialidad:	Bajo

Historial de modificaciones

Versión	Fecha	Detalle del cambio
1.0	11/09/2025	Emisión inicial del documento

ANEXO 1

CRONOGRAMA DE TRABAJO
Evaluación Interna de Cumplimiento EGSI v3

N.	Actividades a ejecutar	Septiembre 2025																			
		Semana1					Semana 2					Semana 3					Semana 4				
		D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3	D4	D5
1	Revisión y recopilación de información básica, política, normativa, otras; en la que se basa la evaluación.																				
2	Ejecución de entrevistas a funcionarios claves: Procesos de la Jefatura de Asesoría Jurídica																				
3	Ejecución de entrevistas a funcionarios claves: Procesos de la Dirección Administrativa y Talento Humano																				
4	Revisión de cumplimiento de los requisitos del sistema de gestión																				-
5	Revisión del Proceso de evaluación de riesgos																				
6	Revisión de controles de seguridad de la información y evidencia de su funcionamiento																				
7	Revisión de acciones de monitoreo e informes de cumplimiento																				
8	Documentación detallada de los hallazgos y las no conformidades encontradas																				
9	Análisis y generación de Resultados																				

CRONOGRAMA DE TRABAJO
Evaluación Interna de Cumplimiento EGSI v3

N.	Actividades a ejecutar	Octubre 2025																			
		Semana1					Semana 2					Semana 3					Semana 4				
		D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3	D4	D5
1	Ejecución de entrevistas a funcionarios claves: Procesos de la Dirección Financiera																				
2	Ejecución de entrevistas a funcionarios claves: Procesos de la Dirección de Planificación, Procesos y Tecnología																				

3	Ejecución de entrevistas a funcionarios claves: Procesos de la Jefatura de Comercialización																				
4	Revisión de cumplimiento de los requisitos del sistema de gestión																				-
5	Revisión del Proceso de evaluación de riesgos																				
6	Revisión de controles de seguridad de la información y evidencia de su funcionamiento																				
7	Revisión de acciones de monitoreo e informes de cumplimiento																				
8	Documentación detallada de los hallazgos y las no conformidades encontradas																				
9	Análisis y generación de Resultados																				

CRONOGRAMA DE TRABAJO
Evaluación Interna de Cumplimiento EGSI v3

N.	Actividades a ejecutar	Noviembre 2025																			
		Semana1					Semana 2					Semana 3					Semana 4				
		D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3	D4	D5
1	Ejecución de entrevistas a funcionarios claves: Procesos de la Jefatura de Operaciones																				
2	Ejecución de entrevistas a funcionarios claves: Procesos de la Jefatura de Contenidos																				
3	Ejecución de entrevistas a funcionarios claves: Procesos de la Jefatura de Producción																				
4	Revisión de cumplimiento de los requisitos del sistema de gestión																				-
5	Revisión del Proceso de evaluación de riesgos																				
6	Revisión de controles de seguridad de la información y evidencia de su funcionamiento																				
7	Revisión de acciones de monitoreo e informes de cumplimiento																				
8	Documentación detallada de los hallazgos y las no conformidades encontradas																				

9	Análisis y generación de Resultados																			

CRONOGRAMA DE TRABAJO
Evaluación Interna de Cumplimiento EGSI v3

N.	Actividades a ejecutar	Diciembre 2025																		
		Semana1					Semana 2					Semana 3					Semana 4				
		D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3	D4	D5
1	Ejecución de entrevistas a funcionarios claves: Procesos de la Jefatura de Programación y Transmisión																			
2	Revisión de cumplimiento de los requisitos del sistema de gestión																			-
3	Revisión del Proceso de evaluación de riesgos																			
4	Revisión de controles de seguridad de la información y evidencia de su funcionamiento																			
5	Revisión de acciones de monitoreo e informes de cumplimiento																			
6	Documentación detallada de los hallazgos y las no conformidades encontradas																			
7	Análisis y generación de Resultados																			
8	Elaboración del Informe Final																			

ANEXO 2

LISTA DE VERIFICACIÓN - REQUISITOS DEL SISTEMA DE GESTIÓN (ANEXO - EGSI V3.0) Ref. ISO/IEC 27001:2022

Sección (# de Hito del Proyecto)	Descripción	Descripción de hallazgos identificados	¿Vigente?	¿Formalizado?	¿Implementado?	Porcentaje Total Cumplimiento
			30	30	40	100
0.1	**Perfil del Proyecto**		30	0	20	50
	¿Se ha determinado el Perfil del Proyecto para la implementación del EGSI?	*Ejemplo: Se verificó que existe un documento de Perfil de Proyecto actualizado, no especifica los objetivos de la implementación del EGSI; no tiene firmas de responsabilidad y no ha sido socializado. Los tiempos planificados no se están cumpliendo en su totalidad, existe un retraso.*	30	0	20	50
0.2	**Definición del Alcance del EGSI versión 2.0**					
	¿Se ha determinado el alcance del EGSI y se conserva información documentada?					
0.3	**Plan de Comunicación y Sensibilización del EGSI**					
	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?					

	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?					
	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?					
0.4	**Plan de Evaluación Interna**					
	¿Se ha documentado un Plan para la ejecución de la evaluación interna, que contemple las herramientas, metodología, recursos y equipo?					
0.5	**Política de la Seguridad de la Información (alto nivel)**					
	¿Se ha definido una Política de la Seguridad de la Información (alto nivel)?					
	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la institución?					
	¿Están identificados los objetivos de seguridad de la información estratégicos?					
0.6	**Metodología de evaluación y tratamiento de riesgos**					
	¿Se ha documentado un proceso en donde se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?					
0.7	**Informe de la Evaluación de los Riesgos**					

	¿Se ha documentado el proceso de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia					
0.8	**Declaración de Aplicabilidad (SoA)**					
	¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?					
0.9	**Plan de Tratamiento de los riesgos**					
	¿Se ha implementado un plan de tratamiento de riesgos?, dónde: -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados					
0.10	**Informe del monitoreo del desempeño y los indicadores de la gestión**					
	¿Se ha documentado formalmente en un informe? ¿El informe describe los indicadores y la metodología utilizada para el monitoreo del desempeño? ¿Se evidencia los cambios y progreso en la implementación?					
0.11	**Informe de la evaluación interna del EGSI V3**					

	¿Se ha documentado formalmente en un informe? ¿El documento informa el resultado de la evaluación interna ejecutada? ¿Se evidencia las insuficiencias en el sistema de gestión, las potenciales situaciones de riesgo, el cumplimiento de los requisitos y controles establecidos en el Esquema Gubernamental de Seguridad? ¿Se incluyen hallazgos y no conformidades?					
0.12	**Informe de los resultados de la revisión de la gestión del EGSI V3**					
	¿Se ha documentado formalmente en un informe? ¿Se detalla las gestiones y revisiones realizadas por la Alta Dirección (Comité de Seguridad de la Información)? ¿Existe evidencias de las gestiones realizadas por el CSI que permitan a la máxima autoridad de la institución tomar decisiones estratégicas?					
0.13	**Informe de los resultados de las medidas correctivas aplicadas**					
	¿Se ha documentado formalmente en un informe? ¿El informe de medidas correctivas se ha redactado en base a los resultados obtenidos de las no conformidades en las evaluaciones internas realizadas al EGSI? ¿El documento contiene las acciones de tratamiento a las no conformidades que permitan garantizar la mejora continua del EGSI?					

0.14	**Informe de cumplimiento de la Gestión de Riesgos**					
	¿Se ha documentado formalmente en un informe? ¿El informe cumple con el formato obligatorio dispuesto por el ente rector (MINTEL)? ¿El documento resume todas las actividades realizadas durante el proceso de la gestión de riesgos de seguridad de la información, es decir, la metodología definida y los criterios establecidos; el análisis, la evaluación, el tratamiento, la aceptación de los riesgos y el plan de acción a ejecutarse durante el proceso de mejora continua del EGSI?					

ANEXO 3

LISTA DE VERIFICACIÓN - CONTROLES DE SEGURIDAD (ANEXO - EGSI V3.0) Ref. ISO/IEC 27002:2022

Ítem	Sección (# de Hito del Proyecto)	Descripción	Descripción de los hallazgos identificados	¿Vigente?	¿Formalizado?	¿Implementado?	Porcentaje Total Cumplimiento
				30	30	40	100
	1	**Controles Organizacionales**					
1	1.1	Políticas de seguridad de la información (específicas)					
2	1.2	Roles y Responsabilidades de Seguridad de la Información					
3	1.3	Separación de Funciones					
4	1.4	Responsabilidades de la dirección					
5	1.5	Contacto con las autoridades					
6	1.6	Contacto con grupos de interés especial					
7	1.7	Inteligencia de amenazas					
8	1.8	Seguridad de la información en la Gestión de proyectos					
9	1.9	Inventario de información y otros activos asociados					
10	1.10	Uso aceptable de la información y otros activos asociados					
11	1.11	Devolución de activos					

12	1.12	Clasificación de la información					
13	1.13	Etiquetado de la información					
14	1.14	Transferencia de información					
15	1.15	Control de Acceso					
16	1.16	Gestión de Identidad					
17	1.17	Información de autenticación					
18	1.18	Derechos de acceso					
19	1.19	Seguridad de la información en las relaciones con proveedores					
20	1.20	Abordar la seguridad de la información en los acuerdos con proveedores					
21	1.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC					
22	1.22	Monitoreo, revisión y gestión de cambios de servicios de proveedores.					
23	1.23	Seguridad de la información para el uso de servicios en la nube					
24	1.24	Planificación y preparación de la gestión de incidentes de seguridad de la información					
25	1.25	Evaluación y decisión sobre eventos de seguridad de la información					
26	1.26	Respuesta a incidentes de seguridad de la información					
27	1.27	Aprendiendo de los incidentes de seguridad de la información					

28	1.28	Recopilación de evidencias					
29	1.29	Seguridad de la Información durante la interrupción					
30	1.30	Preparación de la TIC para la continuidad del Negocio					
31	1.31	Requisitos legales, estatutarios, reglamentarios y contractuales					
32	1.32	Derechos de propiedad intelectual					
33	1.33	Protección de los registros					
34	1.34	Privacidad y protección de PII					
35	1.35	Revisión independiente de seguridad de la información					
36	1.36	Cumplimiento de políticas, reglas y normas de seguridad de la información					
37	1.37	Procedimientos operativos documentados					
	2	**Controles de Personas**					
38	2.1	Selección					
39	2.2	Términos y condiciones de empleo					
40	2.3	Concienciación, educación y formación en seguridad de la información					
41	2.4	Proceso disciplinario					
42	2.5	Responsabilidades después de la terminación o cambio de empleo					
43	2.6	Acuerdo de confidencialidad o no divulgación					

44	2.7	Trabajo remoto					
45	2.8	Reporte de eventos de seguridad de la información					
	3	**Controles Físicos**					
46	3.1	Perímetros de seguridad física					
47	3.2	Entrada física					
48	3.3	Seguridad de oficinas, despachos e instalaciones					
49	3.4	Monitoreo de seguridad física					
50	3.5	Protección contra las amenazas externas y ambientales					
51	3.6	Trabajo en áreas seguras					
52	3.7	Puesto de trabajo despejado y pantalla limpia					
53	3.8	Ubicación y protección de equipos					
54	3.9	Seguridad de los activos fuera de las instalaciones					
55	3.10	Medios de almacenamiento					
56	3.11	Servicios de Soporte					
57	3.12	Seguridad del cableado					
58	3.13	Mantenimiento de equipo					
59	3.14	Eliminación segura o reutilización de equipos					
	4	**Controles Tecnológicos**					

60	4.1	Dispositivos de usuario final					
61	4.2	Derechos de acceso privilegiado					
62	4.3	Restricción de acceso a la información					
63	4.4	Acceso al código fuente					
64	4.5	Autenticación Segura					
65	4.6	Gestión de la capacidad					
66	4.7	Protección contra malware					
67	4.8	Gestión de vulnerabilidades técnicas					
68	4.9	Gestión de la Configuración					
69	4.10	Eliminación de información					
70	4.11	Enmascaramiento de datos					
71	4.12	Prevención de fuga de datos					
72	4.13	Copia de seguridad de la información					
73	4.14	Redundancia de las instalaciones de tratamiento de información					
74	4.15	Registros de eventos					
75	4.16	Actividades de monitoreo					
76	4.17	Sincronización de reloj					
77	4.18	Uso de programas de utilidad privilegiados					
78	4.19	Instalación de software en sistemas operativos					

79	4.20	Seguridad de redes					
80	4.21	Seguridad de los servicios de red.					
81	4.22	Separación en las redes					
82	4.23	Filtrado web					
83	4.24	Uso de criptografía					
84	4.25	Ciclo de vida de desarrollo seguro					
85	4.26	Requisitos de seguridad de la aplicación					
86	4.27	Arquitectura del sistema seguro y principios de ingeniería					
87	4.28	Codificación Segura					
88	4.29	Pruebas de seguridad en el desarrollo y la aceptación					
89	4.30	Desarrollo subcontratado					
90	4.31	Separación de los entornos de desarrollo, prueba y producción					
91	4.32	Gestión de cambios					
92	4.33	Información de pruebas					
93	4.34	Protección de los sistemas de información durante las pruebas de auditoría					