

PLAN DE EVALUACIÓN INTERNA
ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA
INFORMACIÓN (EGSI V3)

Tabla de contenido

1. ANTECEDENTES.....	3
2. OBJETIVO DEL DOCUMENTO.....	3
3. PLAN DE EVALUACIÓN INTERNA DEL EGS V3.....	4
3.1. ALCANCE.....	4
3.2. CRITERIOS	6
3.3. METODOLOGÍA.....	9
3.4. CRONOGRAMA	9
3.5. RECURSOS NECESARIOS	9
3.6. DOCUMENTACIÓN DE HALLAZGOS.....	10
3.7. RESULTADOS	11
4. GLOSARIO DE TÉRMINOS	12
5. DOCUMENTOS DE REFERENCIA	12
6. FIRMAS DE RESPONSABILIDAD	13
CONTROL DE VERSIONES DEL FORMATO REFERENCIAL.....	14
HISTORIAL DE CAMBIOS DEL FORMATO REFERENCIAL	14



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



1. Antecedentes

El Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), en cumplimiento del Acuerdo Ministerial 2024-003 y el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), se encuentra en proceso de implementación de su Sistema de Gestión de Seguridad de la Información.

Considerando que la institución gestiona información crítica relacionada con:

- Operaciones de emergencias
- Comunicaciones operativas
- Gestión administrativa y financiera
- Talento humano
- TIC y seguridad

Se hace necesario evaluar periódicamente el cumplimiento, eficacia y madurez del EGSÍ.

2. Objetivo del documento

Objetivo General

El presente documento tiene como objetivo establecer las directrices, actividades y lineamientos necesarios para la ejecución de la evaluación interna del Esquema Gubernamental de Seguridad de la Información (EGSI v3.0) en el Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), con la finalidad de evaluar el grado de cumplimiento, efectividad y adecuación del sistema implementado, conforme a la normativa vigente, el Acuerdo Ministerial No. 2024-003 del Ministerio de Telecomunicaciones y de la Sociedad de la Información y las normas ISO/IEC 27001, 27002 y 27005.

Objetivos Específicos

- Planificar el proceso de evaluación interna del EGSÍ, definiendo el alcance, cronograma, recursos y metodología a utilizar.
- Verificar el cumplimiento de los requisitos establecidos en el EGSÍ v3 y la normativa aplicable en materia de seguridad de la información.
- Evaluar la implementación y eficacia de las políticas, procedimientos y controles de seguridad de la información adoptados por la institución.
- Validar la gestión de riesgos de seguridad de la información, incluyendo su identificación, análisis, tratamiento y seguimiento.

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

- Identificar no conformidades, debilidades y oportunidades de mejora en el sistema de gestión de seguridad de la información.
- Generar información relevante que permita a la alta dirección y al Comité de Seguridad de la Información tomar decisiones orientadas a la mejora continua del EGSi.

3. Plan de Evaluación interna del EGSi V3

3.1. Alcance

El alcance de la presente evaluación interna del Esquema Gubernamental de Seguridad de la Información (EGSI v3.0) en el Benemérito Cuerpo de Bomberos de Guayaquil (BCBG) comprende todas las áreas, procesos, unidades organizativas y activos de información definidos dentro del alcance institucional del EGSi, con el fin de verificar el grado de cumplimiento, implementación y efectividad de los controles de seguridad de la información.

La evaluación se aplicará a los procesos institucionales que intervienen en la generación, procesamiento, almacenamiento, transmisión y protección de la información, tanto en medios físicos como digitales.

Procesos y áreas incluidas en la evaluación

Procesos misionales (agregadores de valor)

- Combate y Extensión de Incendios.
- Prevención de incendios
- Ingeniería y Proyectos
- Control y Vigilancia

Procesos Habilitantes - De Asesoría

- Asesoría Legal
- Auditoría Interna
- Planificación Institucional
- Comunicación Social
- Del Despacho y Vinculación Operacional Interinstitucional

Procesos Habilitantes - De Apoyo

- Financiera
- Administrativa
- Contratación Pública
- Talento Humano
- Tecnologías de la Información y Comunicaciones (TIC)
- Equipos e Insumos de Emergencias Médicas y Atención Pre-Hospitalaria
- Evaluación Técnica del Mantenimiento y Control de Equipos de Emergencias
- Operaciones de Emergencias y Seguridad Física
- Gestión documental y archivo

Infraestructura y activos incluidos

La evaluación abarcará los activos de información definidos en el alcance del EGSÍ, incluyendo:

- Información digital e impresa
- Sistemas de información institucionales
- Infraestructura tecnológica (servidores, redes, equipos)
- Plataforma de correo y colaboración (Office 365)
- Dispositivos institucionales
- Registros operativos, administrativos y técnicos

Ubicaciones incluidas

- Primera Jefatura
- Cuarteles y compañías
- Central de Alarmas y Comunicaciones
- Áreas administrativas y operativas
- Academia de Bomberos
- Bodegas, talleres y logística
- Entornos de teletrabajo autorizados

Aspectos a evaluar

La evaluación interna comprenderá la validación del cumplimiento de:

- Requisitos del EGSÍ v3
- Políticas de seguridad de la información
- Gestión de riesgos de seguridad de la información
- Control de accesos e identidades
- Gestión de activos de información
- Seguridad física y ambiental
- Seguridad tecnológica y de redes
- Gestión de incidentes de seguridad
- Continuidad del negocio
- Cumplimiento legal, normativo y contractual
- Concienciación y capacitación del personal
- Monitoreo y mejora continua del sistema

Exclusiones del alcance

Quedan excluidos de la evaluación interna aquellos elementos que no son administrados directamente por el BCBG, tales como:

- Infraestructura y redes de proveedores externos
- Servicios tecnológicos tercerizados (nivel operativo del proveedor)
- Redes no corporativas (internet doméstico en cuarteles y compañías)
- Sistemas y plataformas de otras instituciones



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- Dispositivos personales no autorizados (BYOD)

No obstante, se evaluarán los controles establecidos por la institución para gestionar los riesgos asociados a estos elementos externos.

Cierre nivel experto

El alcance de la evaluación se encuentra alineado con los límites organizacionales, físicos y tecnológicos definidos en el EGSi, garantizando una revisión integral del sistema de gestión de seguridad de la información, orientada a la mejora continua y fortalecimiento de la seguridad institucional.

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 v3.0) en el Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), 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

Este criterio permitirá confirmar el cumplimiento de la normativa vigente aplicable a la seguridad de la información, incluyendo el Acuerdo Ministerial No. 2024-003 del Ministerio de Telecomunicaciones y de la Sociedad de la Información, el Esquema Gubernamental de Seguridad de la Información (EGSI v3.0), así como las normas ISO/IEC 27001, 27002 y 27005 u otros estándares adoptados por la institución.

Se verificará que los requisitos legales, regulatorios y normativos se encuentren identificados, documentados y cumplidos dentro de la organización.

Políticas y procedimientos internos

Este criterio permitirá revisar las políticas, procedimientos y lineamientos internos relacionados con la seguridad de la información, con el fin de garantizar que estén

alineados con los objetivos del EGSi y que se encuentren adecuadamente implementados en toda la institución.

Se validará:

- Su formalización (aprobación y firmas)
- Su actualización y control de versiones
- Su difusión y socialización
- Su aplicación en los procesos institucionales

Controles de seguridad

Este criterio permitirá validar, conjuntamente con los propietarios de los activos de información, la existencia, implementación y efectividad de los controles de seguridad establecidos para proteger la confidencialidad, integridad y disponibilidad de la información.

Se considerarán controles:

- Organizacionales
- Físicos
- Tecnológicos
- Procedimentales

Gestión de riesgos

Este criterio permitirá validar la correcta aplicación de la gestión de riesgos de seguridad de la información dentro del EGSi, asegurando que los riesgos sean identificados, analizados, evaluados y tratados de manera adecuada.

Se verificará la existencia de:

- Metodología de gestión de riesgos
- Matriz de riesgos
- Plan de tratamiento
- Seguimiento y actualización de riesgos

Acceso y gestión de la identidad

Este criterio permitirá examinar los controles relacionados con el acceso a los sistemas y la gestión de identidades, asegurando la aplicación del principio de mínimo privilegio y la adecuada protección de la información sensible.

Se evaluará:

- Gestión de usuarios
- Accesos privilegiados
- Autenticación
- Control de accesos

Capacitación y concienciación en seguridad

Este criterio permitirá evaluar la efectividad de los programas de capacitación y sensibilización en seguridad de la información implementados en la institución, asegurando que los funcionarios cuenten con los conocimientos necesarios para identificar, prevenir y responder a amenazas de seguridad.

Se verificará:

- Ejecución del plan de capacitación
- Nivel de conocimiento del personal
- Participación en actividades de sensibilización

Monitoreo y mejora continua

Este criterio permitirá evaluar los procesos de monitoreo, medición y mejora continua del EGSI, asegurando que se identifiquen oportunamente las debilidades y se implementen acciones correctivas.

Se evaluará:

- Monitoreo de eventos e incidentes
- Indicadores de desempeño
- Auditorías internas previas
- Acciones correctivas y preventivas
- Mejora continua del sistema

Cierre nivel auditor

Los criterios definidos permiten evaluar de manera integral tanto el cumplimiento documental como la efectividad operativa del EGSI, asegurando un enfoque basado en riesgos y orientado a la mejora continua del sistema de gestión de seguridad de la información.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



3.3. Metodología

La evaluación interna se llevará a cabo mediante una metodología estructurada y basada en riesgos, considerando las siguientes etapas:

Revisión documental: análisis de la documentación relacionada con el EGSÍ v3.0, incluyendo políticas, procedimientos, registros y demás documentos pertinentes. Se verificará su formalización, actualización y difusión.

Entrevistas: reuniones con responsables de procesos, propietarios de activos de información y personal clave, con el fin de evaluar el conocimiento y aplicación de los lineamientos de seguridad.

Inspección física: verificación de las condiciones de seguridad física y ambiental en las instalaciones de la institución.

Pruebas técnicas: validación de los controles tecnológicos implementados para la protección de la información.

Análisis de resultados: revisión de la información recopilada para determinar el nivel de cumplimiento, identificar hallazgos y establecer oportunidades de mejora.

3.4. Cronograma

Para la ejecución de la evaluación interna del EGSÍ v3.0 en el Benemérito Cuerpo de Bomberos de Guayaquil, se ha definido el siguiente cronograma en coordinación con las áreas involucradas:

Fecha de inicio: [día/mes/año]

Fecha de fin: [día/mes/año]

Lugar: Instalaciones del Benemérito Cuerpo de Bomberos de Guayaquil

Unidad Organizativa: Áreas y procesos relacionados con la gestión de seguridad de la información

El detalle de las actividades a realizar, así como los tiempos establecidos para cada fase de la evaluación, se encuentran definidos en el cronograma adjunto (ANEXO 1).

3.5. Recursos necesarios

Para la ejecución de la evaluación interna del EGSÍ v3.0 en el Benemérito Cuerpo de Bomberos de Guayaquil, la máxima autoridad y/o el Comité de Seguridad de la Información deberá garantizar la disponibilidad de los siguientes recursos:



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



- **Herramientas:** equipos de cómputo, sistemas de información institucionales, correo electrónico, herramientas ofimáticas y demás recursos tecnológicos necesarios.
- **Materiales:** listas de verificación, matrices de evaluación, formatos de levantamiento de información y documentos de apoyo.
- **Humanos:** equipo auditor responsable de la ejecución de la evaluación interna, así como la participación del personal de las diferentes áreas involucradas.
- **Financieros:** no se contempla un presupuesto adicional específico, al ser una actividad ejecutada con recursos institucionales disponibles.

Para la ejecución de la evaluación se utilizarán listas de verificación que permitirán validar el cumplimiento de los requisitos y controles establecidos en el Esquema Gubernamental de Seguridad de la Información (ANEXOS correspondientes).

3.6. Documentación de Hallazgos

Durante la ejecución de la evaluación interna del Esquema Gubernamental de Seguridad de la Información (EGSI v3.0) en el Benemérito Cuerpo de Bomberos de Guayaquil (BCBG), se deberá garantizar que todos los hallazgos identificados sean documentados de manera clara, objetiva, verificable y alineada a los criterios definidos en el presente plan.

La documentación de hallazgos permitirá evidenciar el nivel de cumplimiento del sistema de gestión, así como identificar no conformidades, riesgos y oportunidades de mejora que contribuyan al fortalecimiento del EGSi institucional.

Para la adecuada documentación de los hallazgos, se deberá considerar lo siguiente:

Evidencia recopilada: Se deberá registrar toda la evidencia objetiva que sustente los hallazgos identificados, tales como documentación revisada, registros, configuraciones de sistemas, entrevistas realizadas, inspecciones físicas y resultados de pruebas técnicas. La evidencia deberá ser suficiente, confiable y verificable.

Valoración del cumplimiento: Cada hallazgo deberá ser evaluado conforme a la tabla de valoración del cumplimiento definida en el presente documento, determinando el grado de implementación y efectividad de los controles de seguridad de la información.

Descripción de no conformidades: En los casos en que se evidencie incumplimiento de los requisitos del EGSi, se deberá documentar la no conformidad de manera detallada, incluyendo:

- Requisito o control evaluado
- Situación encontrada
- Criterio de evaluación incumplido
- Evidencia asociada
- Impacto potencial para la institución



Priorización de hallazgos: Los hallazgos deberán ser clasificados de acuerdo con su nivel de cumplimiento y criticidad, permitiendo establecer un orden de atención para la implementación de acciones correctivas, preventivas y de mejora continua.

Registro en matrices y listas de verificación: La documentación de los hallazgos deberá realizarse utilizando las listas de verificación y matrices definidas en los anexos del presente documento, asegurando la trazabilidad entre los requisitos evaluados, la evidencia recopilada y la valoración asignada.

TABLA DE VALORACIÓN DEL CUMPLIMIENTO REQUISITOS Y CONTROLES DE SEGURIDAD

CUMPLIMIENTO	DESCRIPCIÓN PARA EL NIVEL/ ESTADO DEL SISTEMA DE GESTIÓN	VALORACIÓN
0%	No se establecen medidas de seguridad de la información. No existe conciencia institucional ni reconocimiento de la información como activo estratégico.	NO CONFORMIDAD MAYOR
1% - 20%	Existe intención de implementar el EGSi, pero no está formalizado. No se identifican adecuadamente los activos ni se realiza gestión de riesgos.	
21% - 40%	Se evidencian procesos básicos, con bajo compromiso institucional. La gestión es principalmente reactiva y parcial.	NO CONFORMIDAD MENOR
41% - 60%	La gestión está documentada y difundida. Existe participación institucional y avances en mejora continua.	OPORTUNIDAD DE MEJORA
61% - 80%	Se monitorea y mide el cumplimiento mediante indicadores. Se evalúa la efectividad de controles y se gestionan incidentes.	
81% - 100%	El EGSi se encuentra en mejora continua, con evidencia de madurez y compromiso institucional.	CONFORME

3.7. Resultados

Los resultados de la evaluación interna del Esquema Gubernamental de Seguridad de la Información (EGSi v3.0) serán comunicados a la alta dirección, representada por la máxima autoridad y el Comité de Seguridad de la Información, así como a las partes interesadas que correspondan, asegurando que la información presentada sea clara, objetiva y orientada a la toma de decisiones.

Como resultado de la ejecución de la evaluación interna, se generará el Informe de Evaluación Interna del EGSi, documento oficial que consolida los resultados obtenidos y refleja el estado del sistema de gestión de seguridad de la información en la institución.



EGSI

ESQUEMA
GUBERNAMENTAL
DE SEGURIDAD
DE LA INFORMACIÓN



El informe contendrá el nivel de cumplimiento de los requisitos y controles establecidos en el EGSi, así como los hallazgos identificados durante la evaluación, incluyendo no conformidades y oportunidades de mejora, debidamente sustentadas en evidencia objetiva. Asimismo, se incluirá el análisis de las debilidades del sistema, las potenciales situaciones de riesgo y las conclusiones generales sobre el grado de madurez del EGSi institucional.

La presentación de los resultados se realizará de manera formal ante la alta dirección, garantizando su comprensión, relevancia y alineación con los objetivos institucionales.

Cuando se identifiquen no conformidades, se establecerá un plan de acción orientado a su tratamiento, el cual será elaborado por el Oficial de Seguridad de la Información y acordado con el líder del equipo evaluador y los responsables de los procesos evaluados.

El plan de acción incluirá, como mínimo:

- Descripción de la no conformidad detectada
- Análisis de las causas que la originaron
- Definición de acciones de corrección y acciones correctivas
- Plazos para su implementación
- Responsables de su ejecución

El seguimiento al cumplimiento del plan de acción se realizará de manera periódica, con el fin de verificar la implementación efectiva de las medidas definidas y asegurar la mejora continua del EGSi en la institución.

4. Glosario de términos

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

5. Documentos de referencia

Para la elaboración del presente Plan de Evaluación Interna del Esquema Gubernamental de Seguridad de la Información (EGSi v3.0), se han considerado las siguientes referencias normativas y documentales, las cuales establecen los

lineamientos y criterios aplicables para la gestión de la seguridad de la información en la institución:

- Acuerdo Ministerial No. 2024-0003 del Ministerio de Telecomunicaciones y de la Sociedad de la Información.
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0).
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001.
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27002.
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27005.
- Políticas de Seguridad de la Información del BCBG.
- Reglamento Interno del Comité de Seguridad de la Información.
- Procedimientos y lineamientos internos relacionados con la gestión de tecnologías de la información y seguridad de la información.

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

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

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
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:	24-07-2026
Creado por:	Oficial de Seguridad de la Información del Benemerito Cuerpo de Bomberos de Guayaquil
Aprobado por:	Comité de Seguridad de la Información del Benemerito Cuerpo de Bomberos de Guayaquil
Nivel de confidencialidad:	Bajo

Historial de cambios del formato referencial

Versión	Fecha	Detalle del cambio
1.0	24/07/2026	Emisión inicial del documento



ANEXO 1

EJEMPLO - CRONOGRAMA DE TRABAJO

Evaluación Interna de Cumplimiento EGSi v3

N.	Actividades a ejecutar	Agosto 2026														
		Semana 1					Semana 2					Semana 3				
		D1	D2	D3	D4	D5	D1	D2	D3	D4	D5	D1	D2	D3		
1	Revisión y recopilación de información básica, política, normativa, otras; en la que se basa la evaluación.															
2	Reunión previa para aprobación del Plan y Cronograma de trabajo.															
3	Reunión de Inicio y presentación de actividades a realizar															
4	Ejecución de entrevistas a funcionarios claves en la implementación															
5	Revisión de cumplimiento de los requisitos del sistema de gestión															
6	Revisión del Proceso de evaluación de riesgos															
7	Revisión de controles de seguridad de la información y evidencia de su funcionamiento															
8	Revisión de acciones de monitoreo e informes de cumplimiento															
9	Documentación detallada de los hallazgos y las no conformidades encontradas															
10	Análisis y generación de Resultados															
11	Elaboración del Informe Final															

NOTA IMPORTANTE:

Levantamiento de la información: para levantar la información y determinar la valoración de los hallazgos, se podrían realizar: verificaciones en sitio, entrevistas, encuestas, otros.

Revisión y recopilación de información básica: tomar conocimiento de la normativa externa e interna en la que se basa la implementación y evaluación del Sistema de Gestión (EGSI V3).

Reunión aprobación Plan y cronograma de trabajo: reunión de trabajo para dar a conocer el cronograma de trabajo y su posterior aprobación.

Reunión de inicio y presentación de actividades a realizar: reunión formal del inicio de la evaluación y presentación de actividades que se van a desarrollar durante el transcurso del proceso de evaluación.

Revisión del Proceso de evaluación de riesgos: revisión de la metodología documentada y la aplicación en el levantamiento de la matriz de riesgos.

Revisión de controles de seguridad de la información: verificación de la existencia y aplicación correcta de los controles de seguridad de acuerdo al resultado de la evaluación de riesgos.

Revisión de acciones de monitoreo e informes de cumplimiento: verificación de la implementación adecuada y alineada a los procedimientos, manuales, políticas establecidas. La documentación debe estar actualizada.

Elaboración del Informe de Evaluación: documentar los resultados de la evaluación, hallazgos, no conformidades, mismas que serán presentados y revisados por las autoridades para el seguimiento y mejora continua.

ANEXO 2

LISTA DE VERIFICACIÓN - REQUISITOS DEL SISTEMA DE GESTIÓN (ANEXO - EGSÍ 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 EGSÍ?	<i>Ejemplo: Se verificó que existe un documento de Perfil de Proyecto actualizado, no especifica los objetivos de la implementación del EGSÍ; no tiene firmas de responsabilidad y no ha sido socializado. Los tiempos planificados no se están cumpliendo en su totalidad, existe un retraso.</i>	30	0	20	50
0.2	Definición del Alcance del EGSÍ versión 2.0					
	¿Se ha determinado el alcance del EGSÍ y se conserva información documentada?					
0.3	Plan de Comunicación y Sensibilización del EGSÍ					
	¿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 EGSÍ? ¿El documento contiene las acciones de tratamiento a las no conformidades que permitan garantizar la mejora continua del EGSÍ?					
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 EGSÍ?					

ANEXO 3

LISTA DE VERIFICACIÓN - CONTROLES DE SEGURIDAD (ANEXO - EGS 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					