INSTRUCTIVO

Control de los Avances en la Implementación del EGSI V3.0 – SECTOR PÚBLICO

En cumplimiento del Acuerdo Ministerial
Nro. MINTEL-MINTEL-2024-0003

EGSI ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

2024

QUITO – ECUADOR

[Versión 1.1]

Tabla de contenido

1. Propósito

Emitir los lineamientos específicos para el control de los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI v3), en cumplimiento del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003.

2. Audiencia

- Oficiales de Seguridad de la Información (OSI)
- Comité de Seguridad de la Información (CSI)
- Responsables de la Información

3. Alcance

El presente documento está dirigido a las instituciones del **Sector Público**[1], que gestionan internamente el proyecto de implementación del Esquema Gubernamental de Seguridad de la Información EGSI V3.

4. Control del cumplimiento de los hitos del proyecto EGSI V3.0

Para el control de los verificables de cumplimiento de cada uno de los hitos homologados, se debe utilizar la "Ficha de cumplimiento de hitos" que se encuentra como Anexo 1 en el presente documento.

La "Ficha de cumplimiento de hitos" debe ser validada y firmada en cada institución del sector público por parte de los siguientes funcionarios:

- Oficial de Seguridad de la Información
- Comité de Seguridad de la Información
- Responsable de la Información (relacionado con el hito a reportar).

Las instituciones deben llenar la ficha y **conservarla**[2], esta permitirá realizar el control y seguimiento de la implementación del EGSI V3.

Las instituciones deberán generar una "Ficha de cumplimiento de hitos" por cada hito homologado (Anexo 3), es decir ciento ocho (108) fichas.

De acuerdo a los plazos establecidos en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, disposición transitoria segunda, se ha distribuido el plazo en las siguientes etapas:

Primera Etapa: 6 meses

- 0.1 Perfil de Proyecto EGSI v3, documentado y aprobado
- 0.2 Definición del Alcance, documentado y aprobado
- 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado
- 0.4 Plan de evaluación Interna, documentado y aprobado
- 0.5 Política de Seguridad de la información (alto nivel), documentado y aprobado
- 0.6 Metodología de evaluación y tratamiento del riesgo, documentado y aprobado
- 0.7 Informe de la Evaluación de los Riesgos, documentado y aprobado
- 0.8 Declaración de Aplicabilidad (SoA), documentado y aprobado

[1] Instituciones del Sector Público, excepto las instituciones de la Función Ejecutiva.

[2] Cada institución deberá conservar la ficha con la documentación de implementación y esta podrá ser solicitada por el ente de control que así lo requiera.

- 0.9 Plan de Tratamiento de los riesgos, documentado y aprobado.

Segunda Etapa: 4 meses, a partir de la finalización de la primera etapa.

- Desde: 1.1 políticas de seguridad de la información (específicas), documentado e implementado
- Hasta: 4.34 Protección de los sistemas de información durante las pruebas de auditoría, documentado e implementado

Tercera Etapa: 2 meses, a partir de la finalización de la segunda etapa.

- 0.10 Informe del monitoreo del desempeño y los indicadores de la gestión del EGSI v3, documentado y aprobado
- 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado
- 0.12 Informe de los resultados de la revisión de la gestión del EGSI v3, documentado y aprobado
- 0.13 Informe de los resultados de las medidas correctivas aplicadas al EGSI v3, documentado y aprobado
- 0.14 Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información, documentado y aprobado
- 0.15 Informe de cierre del proyecto EGSI v3, documentado y aprobado

De manera adicional, se debe revisar el detalle de las fechas comprometidas en la "Plantilla de los hitos homologados" que se encuentra como Anexo 3 en el presente documento. Esta distribución de fechas se ha planteado con el fin de garantizar el cumplimiento de los plazos establecidos en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003.

Nota: Las fechas para el cumplimiento de los hitos 1.1.1 al 14.2.3, las debe definir cada institución considerando el periodo establecido en las fechas comprometidas del Anexo 3 y considerando también que durante este periodo se deberán reportar el cumplimiento de los 93 controles de seguridad a través de las fichas de cumplimiento.

4.1. Descripción de pasos para ejecutar el control del cumplimiento de los hitos del proyecto

PASO 1:

Utilizar la ficha de cumplimiento para detallar las actividades desarrolladas, en cumplimiento de lo solicitado en cada hito del proyecto. Esta ficha es el respaldo del cumplimiento de cada uno de los hitos del proyecto; a continuación, los criterios para el llenado de la mencionada ficha:

CRITERIOS PARA EL REGISTRO DE FICHAS	
No.	Descripción
1	Uso del formato establecido para reportar el cumplimiento de hitos.
2	Registro de actividades (coherentes) realizadas para el cumplimiento del hito reportado.
3	Registro del documento/verificable interno, como evidencia de cumplimiento del hito reportado.
4	Registro de las firmas de responsabilidad respectivas.

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SECTOR PUBLICO		
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE CUMPLIMIENTO DE HITOS **Implementación del EGSI v3**		
ENTIDAD / (SIGLAS):	*Ministerio de Telecomunicaciones y de la Sociedad de la Información / MINTEL*	
DESCRIPCIÓN DEL HITO:	*Acuerdos de confidencialidad o no divulgación, documentado e implementado.*	
NÚMERO DE HITO:	*2.6*	
No.	**RESUMEN ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO**
1	*Elaboración/actualización del acuerdo de confidencialidad, con las partes involucradas: Oficial de Seguridad, responsable de la Unidad de Talento Humano y delegado de Jurídico.*	*Acuerdos de confidencialidad o no divulgación firmados por todos los funcionarios.*
2	*Socialización del contenido del acuerdo de confidencialidad elaborado: derechos y responsabilidades legales de los funcionarios relacionados a la seguridad de la información.*	**UBICACIÓN**
3	*Recepción y registro de firmas de acuerdos de confidencialidad de parte de todos los funcionarios de la Institución.*	*Área de archivo de la Unidad de Talento Humano (expediente de funcionarios)*
PIE DE RESPONSABILIDAD		
FECHA ELABORACIÓN:	*15/02/2024*	
NOMBRE DEL OFICIAL DE SEGURIDAD: *[Nombres y Apellidos del Oficial de Seguridad nombrado]*	**FIRMA:**	
NOMBRE DEL REPRESENTANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: *[Nombres y Apellidos del funcionario que preside el Comité de Seguridad de la Información]*	**FIRMA:**	
NOMBRE DEL RESPONSABLE DE LA INFORMACIÓN: *[Nombres y Apellidos del responsable de la Unidad de Talento Humano (para el caso del presente ejemplo)]*	**FIRMA:**	
DECLARACIÓN DE RESPONSABILIDAD		
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3. *LOETA, Art. 10.- Veracidad de la información: "(...) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el período de tiempo inherente a dicho ejercicio (...)".*		

Es importante precisar que la persona designada como Oficial de Seguridad de la Información (OSI), es responsable de la información ingresada en cada una de las fichas, por lo que, dicha información debe ser verídica y validada por los miembros del Comité de Seguridad de la información (CSI), previo a estampar la firma electrónica; en cumplimiento de la **Declaración de Responsabilidad**[3].

PASO 2:

Por cada hito, las instituciones internamente deben elaborar la documentación respectiva y mantenerla actualizada, esto permitirá verificar el cumplimiento de cada hito. Esta información debe ser detallada en la ficha de cumplimiento, en el campo **VERIFICABLE INTERNO** (Los documentos verificables pueden ser, por ejemplo: políticas, procedimientos, instructivos,

[3] LOETA, Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, art. 10

memorandos, oficios, informes técnicos, otros); en el campo **UBICACIÓN** ingresar la ubicación, es decir el lugar en donde reposa la documentación, por ejemplo: repositorio digital o archivo físico. Se adjunta al presente el ejemplo de Ficha de cumplimiento de hitos (Anexo 2) como referencia para el ingreso de la información en la ficha.

Nota: las evidencias (verificable interno), serán validadas durante el proceso de evaluación en sitio que será coordinada e informada oportunamente con las instituciones.

PASO 3:

En caso de no ser posible la implementación de ciertos controles de seguridad establecidos en el EGSI V3.0 y se encuentre implícito en el documento Declaración de Aplicabilidad (SoA), la institución deberá realizar un **informe técnico**[4], en el cual se describa o registre la justificación técnica del no cumplimiento del hito del proyecto que corresponde al control de seguridad no aplicable.

Este informe técnico será el VERIFICABLE de los controles que no aplican a la institución y se registrará en la ficha de cumplimiento que corresponda al hito reportado.

PASO 4:

Con el objetivo de facilitar el control a las partes, se deberá seguir la siguiente nomenclatura para nombrar las Fichas de cumplimiento de hitos:

EGSIV3_SiglasEntidad_NroHito_SecArchivo_FechadeCump

en donde:

- **EGSIV3:** Esquema Gubernamental de Seguridad de la Información versión 3.0
- **SiglasEntidad:** Son las siglas o acrónimo de la institución pública.
- **NroHito:** Número de hito para el cual se registra el cumplimiento. El número es el que consta en la "Plantilla de los hitos homologados" (Anexo 3).
- **SecArchivo:** Número secuencial del verificable cargado. Para el caso de que exista más de un verificable, se deberá utilizar un secuencial con el que se reporte el cumplimiento del hito respectivo con un verificable adicional (casos excepcionales).
- **FechadeCump:** Fecha en la que se registra el cumplimiento. La fecha deberá estar en el formato "AAAAMMDD" (sin espacios ni guiones).

Nota: Estas fichas deberán ser firmadas electrónicamente para que tengan validez.

Ejemplo:

a) Nomenclatura de la ficha de cumplimiento del hito:
"2.6 Acuerdo de confidencialidad o no divulgación"

- EGSIV3_MINTEL_2.6_0**1**_20240211.pdf

[4] El formato referencial para la elaboración de este informe técnico se encuentra publicado en el portal web de gobierno electrónico www.gobiernoelectronico.gob.ec, sección Seguridad de la Información.

Para el **control interno**[5] se debe considerar que, por cada hito cumplido le corresponde un porcentaje de avance en la ejecución del proyecto. Esta distribución de pesos/porcentajes se encuentra detallada en el Anexo 4.

5. Contacto Soporte Técnico

Para preguntas o requerimientos de cómo aplicar o seguir el presente instructivo a continuación los contactos de soporte:

INSTITUCIÓN / UNIDAD	DIRECCIÓN DE CORREO ELECTRÓNICO
MINTEL / Subsecretaría de Gobierno Electrónico y Registro Civil	**servicios**@gobiernoelectronico.gob.ec

6. Control de cambios del Instructivo

Versión:	1.1
Fecha de la versión:	15-03-2024
Creado por:	Dirección de Infraestructura, Interoperabilidad, Seguridad de la Información y Registro Civil
Aprobado por:	Subsecretaría de Gobierno Electrónico y Registro Civil
Nivel de confidencialidad:	Bajo

7. Historial de cambios del Instructivo

Versión	Fecha	Detalle de la modificación
1.0	01/03/2024	Emisión inicial del documento
1.1	15/03/2024	Cambios en el contenido

[5] Para el control interno, si la institución así lo considera, podrá hacer uso de la Plantilla de Seguimiento del Proyecto de Implementación EGSI V3, publicada en el portal web de Gobierno Electrónico.

Anexo 1

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SECTOR PUBLICO		
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"		
FICHA DE CUMPLIMIENTO DE HITOS **Implementación del EGSI v3**		
ENTIDAD / (SIGLAS):		
DESCRIPCIÓN DEL HITO:		
NÚMERO DE HITO:		
No.	**RESUMEN DE ACTIVIDADES REALIZADAS**	**VERIFICABLE INTERNO (DOCUMENTO)**
N		
N+1		
N+3		**UBICACIÓN**
…..		
FIRMAS DE RESPONSABILIDAD		
FECHA ELABORACIÓN:	*dd/mm/aaaa*	
NOMBRE DEL OFICIAL DE SEGURIDAD: *[Nombres, Apellidos]*	**FIRMA:** *[**Firma electrónica** del funcionario (a)]*	
NOMBRE DEL REPRESENTANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: *[Nombres, Apellidos]*	**FIRMA:** *[**Firma electrónica** del funcionario (a)]*	
NOMBRE DEL RESPONSABLE DE LA INFORMACIÓN: *[Nombres, Apellidos]*	**FIRMA:** *[**Firma electrónica** del funcionario (a)]*	
DECLARACIÓN DE RESPONSABILIDAD		
Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3. *LOETA, Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".*		

Anexo 2

EJEMPLO de la Ficha de cumplimiento de hitos

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SECTOR PUBLICO	
PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI V3)"	
FICHA DE CUMPLIMIENTO DE HITOS **Implementación del EGSI v3**	
ENTIDAD / (SIGLAS):	*Ministerio de Telecomunicaciones y de la Sociedad de la Información / MINTEL*
DESCRIPCIÓN DEL HITO:	*Acuerdos de confidencialidad o no divulgación, **documentado e implementado**.*
NÚMERO DE HITO:	*2.6*

No.	RESUMEN ACTIVIDADES REALIZADAS	VERIFICABLE INTERNO
1	*Elaboración/actualización del acuerdo de confidencialidad, con las partes involucradas, Oficial de Seguridad, responsable de la Unidad de Talento Humano y delegado de Jurídico.*	*Acuerdos de confidencialidad o no divulgación **firmados** por todos los funcionarios.*
2	*Socialización del contenido del acuerdo de confidencialidad elaborado: derechos y responsabilidades legales de los funcionarios relacionados a la seguridad de la información.*	**UBICACIÓN** *Área de archivo de la Unidad de Talento Humano (expediente de funcionarios)*
3	*Recepción y registro de firmas de acuerdos de confidencialidad de parte de todos los funcionarios de la institución.*	

PIE DE RESPONSABILIDAD	
FECHA ELABORACIÓN:	*15/02/2024*
NOMBRE DEL OFICIAL DE SEGURIDAD: *[Nombres y Apellidos del Oficial de Seguridad nombrado]*	**FIRMA:** Firmado electrónicamente por: OFICIAL DE SEGURIDAD DE LA INFORMACIÓN
NOMBRE DEL REPRESENTANTE DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: *[Nombres y Apellidos del funcionario que preside el Comité de Seguridad de la Información]*	**FIRMA:** Firmado electrónicamente por: REPRESENTANTE DEL COMITÉ DE SEGURIDAD
NOMBRE DEL RESPONSABLE DE LA INFORMACIÓN: *[Nombres y Apellidos del responsable de la Unidad de Talento Humano (para el caso del presente ejemplo)]*	**FIRMA:** Firmado electrónicamente por: RESPONSABLE DE LA INFORMACIÓN

DECLARACIÓN DE RESPONSABILIDAD

Los firmantes declaran que la información registrada en el presente documento es verídica y podrá ser verificada cuando sea necesario, dando cumplimiento a lo dispuesto al Art. 10 de la Ley para la Optimización y Eficiencia de Trámites Administrativos (LOETA); por lo que se deberá cumplir a cabalidad con los criterios establecidos en la implementación del EGSI v3.

LOETA, Art. 10.- Veracidad de la información: "(…) A los efectos de esta Ley, se entenderá por declaración responsable el instrumento público suscrito por el interesado en el que manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para el ejercicio de una actividad, que dispone de la documentación que así lo acredita y que se compromete a mantener su cumplimiento durante el periodo de tiempo inherente a dicho ejercicio (…)".

Anexo 3

Plantilla de los hitos homologados

Ítem	HITOS HOMOLOGADOS	Fecha Comprometida
0	**(*) INICIO** DEL PROYECTO	1/3/2024
1	**DEFINICIÓN:** 0.1 Perfil de Proyecto EGSI v3, documentado y aprobado	5/4/2024
2	PLANEACIÓN: 0.2 Definición del Alcance, documentado y aprobado	15/4/2024
3	PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado	28/4/2024
4	PLANEACIÓN: 0.4 Plan de evaluación Interna, documentado y aprobado	5/5/2024
5	PLANEACIÓN: 0.5 Política de Seguridad de la información (alto nivel), documentado y aprobado	15/5/2024
6	PLANEACIÓN: 0.6 Metodología de evaluación y tratamiento del riesgo, documentado y aprobado	31/5/2024
7	PLANEACIÓN: 0.7 Informe de la Evaluación de los Riesgos, documentado y aprobado	31/7/2024
8	PLANEACIÓN: 0.8 Declaración de Aplicabilidad (SoA), documentado y aprobado	10/8/2024
9	**(*)** PLANEACIÓN: 0.9 Plan de Tratamiento de los riesgos, documentado y aprobado	**15/8/2024**
10	EJECUCIÓN:1.1 Políticas de seguridad de la información (específicas), documentado e implementado	**Desde:** 20/8/2024 **Hasta:** 20/12/2024
11	EJECUCIÓN:1.2 Roles y Responsabilidades de Seguridad de la Información, documentado e implementado	
12	EJECUCIÓN:1.3 Separación de Funciones, documentado e implementado	
13	EJECUCIÓN:1.4 Responsabilidades de la dirección, documentado e implementado	
14	EJECUCIÓN:1.5 Contacto con las autoridades, documentado e implementado	
15	EJECUCIÓN:1.6 Contacto con grupos de interés especial, documentado e implementado	
16	EJECUCIÓN:1.7 Inteligencia de amenazas, documentado e implementado	
17	EJECUCIÓN:1.8 Seguridad de la información en la Gestión de proyectos, documentado e implementado	
18	EJECUCIÓN:1.9 Inventario de información y otros activos asociados, documentado e implementado	
19	EJECUCIÓN:1.10 Uso aceptable de la información y otros activos asociados, documentado e implementado	
20	EJECUCIÓN:1.11 Devolución de activos, documentado e implementado	
21	EJECUCIÓN:1.12 Clasificación de la información, documentado e implementado	
22	EJECUCIÓN:1.13 Etiquetado de la información, documentado e implementado	
23	EJECUCIÓN:1.14 Transferencia de información, documentado e implementado	
24	EJECUCIÓN:1.15 Control de Acceso, documentado e implementado	
25	EJECUCIÓN:1.16 Gestión de Identidad, documentado e implementado	
26	EJECUCIÓN:1.17 Información de autenticación, documentado e implementado	
27	EJECUCIÓN:1.18 Derechos de acceso, documentado e implementado	
28	EJECUCIÓN:1.19 Seguridad de la información en las relaciones con proveedores, documentado e implementado	
29	EJECUCIÓN:1.20 Seguridad de la información en los acuerdos con proveedores, documentado e implementado	
30	EJECUCIÓN:1.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC, documentado e implementado	
31	EJECUCIÓN:1.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores, documentado e implementado	
32	EJECUCIÓN:1.23 Seguridad de la información para el uso de servicios en la nube, documentado e implementado	
33	EJECUCIÓN:1.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, documentado e implementado	
34	EJECUCIÓN:1.25 Evaluación y decisión sobre eventos de seguridad de la información, documentado e implementado	
35	EJECUCIÓN:1.26 Respuesta a incidentes de seguridad de la información, documentado e implementado	
36	EJECUCIÓN:1.27 Aprendiendo de los incidentes de seguridad de la información, documentado e implementado	

37	EJECUCIÓN:1.28 Recopilación de evidencias, documentado e implementado	
38	EJECUCIÓN:1.29 Seguridad de la Información durante la interrupción, documentado e implementado	
39	EJECUCIÓN:1.30 Preparación de las TIC para la continuidad del Negocio, documentado e implementado	
40	EJECUCIÓN:1.31 Requisitos legales, estatutarios, reglamentarios y contractuales, documentado e implementado	
41	EJECUCIÓN:1.32 Derechos de propiedad intelectual, documentado e implementado	
42	EJECUCIÓN:1.33 Protección de los registros, documentado e implementado	
43	EJECUCIÓN:1.34 Privacidad y protección de PII, documentado e implementado	
44	EJECUCIÓN:1.35 Revisión independiente de seguridad de la información, documentado e implementado	
45	EJECUCIÓN:1.36 Cumplimiento de políticas, reglas y normas de seguridad de la información, documentado e implementado	
46	EJECUCIÓN:1.37 Procedimientos operativos, documentado e implementado	
47	EJECUCIÓN:2.1 Selección de personas, documentado e implementado	
48	EJECUCIÓN:2.2 Términos y condiciones de empleo, documentado e implementado	
49	EJECUCIÓN:2.3 Concienciación, educación y formación en seguridad de la información, documentado e implementado	
50	EJECUCIÓN:2.4 Proceso disciplinario, documentado e implementado	
51	EJECUCIÓN:2.5 Responsabilidades después de la terminación o cambio de empleo, documentado e implementado	
52	EJECUCIÓN:2.6 Acuerdo de confidencialidad o no divulgación, documentado e implementado	
53	EJECUCIÓN:2.7 Trabajo remoto, documentado e implementado	
54	EJECUCIÓN:2.8 Reporte de eventos de seguridad de la información, documentado e implementado	
55	EJECUCIÓN:3.1 Perímetros de seguridad física, documentado e implementado	
56	EJECUCIÓN:3.2 Entrada física, documentado e implementado	
57	EJECUCIÓN:3.3 Seguridad de oficinas, despachos e instalaciones, documentado e implementado	
58	EJECUCIÓN:3.4 Monitoreo de seguridad física, documentado e implementado	
59	EJECUCIÓN:3.5 Protección contra las amenazas externas y ambientales, documentado e implementado	
60	EJECUCIÓN:3.6 Trabajo en áreas seguras, documentado e implementado	
61	EJECUCIÓN:3.7 Puesto de trabajo despejado y pantalla limpia, documentado e implementado	
62	EJECUCIÓN:3.8 Ubicación y protección de equipos, documentado e implementado	
63	EJECUCIÓN:3.9 Seguridad de los activos fuera de las instalaciones, documentado e implementado	
64	EJECUCIÓN:3.10 Medios de almacenamiento, documentado e implementado	
65	EJECUCIÓN:3.11 Servicios de Soporte, documentado e implementado	
66	EJECUCIÓN:3.12 Seguridad del cableado, documentado e implementado	
67	EJECUCIÓN:3.13 Mantenimiento de equipo, documentado e implementado	
68	EJECUCIÓN:3.14 Eliminación segura o reutilización de equipos, documentado e implementado	
69	EJECUCIÓN:4.1 Dispositivos de usuario final, documentado e implementado	
70	EJECUCIÓN:4.2 Derechos de acceso privilegiado, documentado e implementado	
71	EJECUCIÓN:4.3 Restricción de acceso a la información, documentado e implementado	
72	EJECUCIÓN:4.4 Acceso al código fuente, documentado e implementado	
73	EJECUCIÓN:4.5 Autenticación Segura, documentado e implementado	
74	EJECUCIÓN:4.6 Gestión de la capacidad, documentado e implementado	
75	EJECUCIÓN:4.7 Protección contra malware, documentado e implementado	
76	EJECUCIÓN:4.8 Gestión de vulnerabilidades técnicas, documentado e implementado	
77	EJECUCIÓN:4.9 Gestión de la Configuración, documentado e implementado	
78	EJECUCIÓN:4.10 Eliminación de información, documentado e implementado	
79	EJECUCIÓN:4.11 Enmascaramiento de datos, documentado e implementado	
80	EJECUCIÓN:4.12 Prevención de fuga de datos, documentado e implementado	
81	EJECUCIÓN:4.13 Copia de seguridad de la información, documentado e implementado	
82	EJECUCIÓN:4.14 Redundancia de las instalaciones de tratamiento de información	
83	EJECUCIÓN:4.15 Registros de eventos, documentado e implementado	

84	EJECUCIÓN:4.16 Actividades de monitoreo, documentado e implementado	
85	EJECUCIÓN:4.17 Sincronización de reloj, documentado e implementado	
86	EJECUCIÓN:4.18 Uso de programas de utilidad privilegiados, documentado e implementado	
87	EJECUCIÓN:4.19 Instalación de software en sistemas operativos, documentado e implementado	
88	EJECUCIÓN:4.20 Seguridad de redes, documentado e implementado	
89	EJECUCIÓN:4.21 Seguridad de los servicios de red, documentado e implementado	
90	EJECUCIÓN:4.22 Separación en las redes, documentado e implementado	
91	EJECUCIÓN:4.23 Filtrado web, documentado e implementado	
92	EJECUCIÓN:4.24 Uso de criptografía, documentado e implementado	
93	EJECUCIÓN:4.25 Ciclo de vida de desarrollo seguro, documentado e implementado	
94	EJECUCIÓN:4.26 Requisitos de seguridad de la aplicación, documentado e implementado	
95	EJECUCIÓN:4.27 Arquitectura del sistema seguro y principios de ingeniería, documentado e implementado	
96	EJECUCIÓN:4.28 Codificación Segura, documentado e implementado	
97	EJECUCIÓN:4.29 Pruebas de seguridad en el desarrollo y la aceptación, documentado e implementado	
98	EJECUCIÓN:4.30 Desarrollo subcontratado, documentado e implementado	
99	EJECUCIÓN:4.31 Separación de los entornos de desarrollo, prueba y producción, documentado e implementado	
100	EJECUCIÓN:4.32 Gestión de cambios, documentado e implementado	
101	EJECUCIÓN:4.33 Información de pruebas, documentado e implementado	
102	EJECUCIÓN:4.34 Protección de los sistemas de información durante las pruebas de auditoría, documentado e implementado	
103	EJECUCIÓN: 0.10 Informe del monitoreo del desempeño y los indicadores de la gestión del EGSI v3, documentado y aprobado	2/01/2025
104	EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado	15/01/2025
105	EJECUCIÓN: 0.12 Informe de los resultados de la revisión de la gestión del EGSI v3, documentado y aprobado	30/01/2025
106	EJECUCIÓN: 0.13 Informe de los resultados de las medidas correctivas aplicadas al EGSI v3, documentado y aprobado	15/02/2025
107	EJECUCIÓN: 0.14 Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información, documentado y aprobado	25/02/2025
108	**(*) CIERRE:** 0.15 Informe de cierre del proyecto EGSI v3, documentado y aprobado	**28/02/2025**

Nota: Para cumplir con el plazo establecido para la implementación del EGSI V3 (doce meses), las fechas de los hitos marcados con **(*)** no podrán ser cambiadas, mientras que las fechas intermedias podrán ser reprogramadas de acuerdo a la necesidad y planificación de cada institución.

Anexo 4

Listado de los hitos homologados con porcentaje de avance

ítem	HITOS HOMOLOGADOS – PROYECTO DE IMPLEMENTACIÓN EGSI V3	Porcentaje (%)
1	**DEFINICIÓN:** 0.1 Perfil de Proyecto EGSI v3, documentado y aprobado	2
2	**PLANEACIÓN**: 0.2 Definición del Alcance, documentado y aprobado	6
3	PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado	4
4	PLANEACIÓN: 0.4 Plan de evaluación Interna, documentado y aprobado	4
5	PLANEACIÓN: 0.5 Política de Seguridad de la información (alto nivel), documentado y aprobado	7
6	PLANEACIÓN: 0.6 Metodología de evaluación y tratamiento del riesgo, documentado y aprobado	10
7	PLANEACIÓN: 0.7 Informe de la Evaluación de los Riesgos, documentado y aprobado	12
8	PLANEACIÓN: 0.8 Declaración de Aplicabilidad (SoA), documentado y aprobado	2
9	PLANEACIÓN: 0.9 Plan de Tratamiento de los riesgos, documentado y aprobado	3
10	**EJECUCIÓN**:1.1 Políticas de seguridad de la información (específicas), documentado e implementado	0,43
11	EJECUCIÓN:1.2 Roles y Responsabilidades de Seguridad de la Información, documentado e implementado	0,43
12	EJECUCIÓN:1.3 Separación de Funciones, documentado e implementado	0,43
13	EJECUCIÓN:1.4 Responsabilidades de la dirección, documentado e implementado	0,43
14	EJECUCIÓN:1.5 Contacto con las autoridades, documentado e implementado	0,43
15	EJECUCIÓN:1.6 Contacto con grupos de interés especial, documentado e implementado	0,43
16	EJECUCIÓN:1.7 Inteligencia de amenazas, documentado e implementado	0,43
17	EJECUCIÓN:1.8 Seguridad de la información en la Gestión de proyectos, documentado e implementado	0,43
18	EJECUCIÓN:1.9 Inventario de información y otros activos asociados, documentado e implementado	0,43
19	EJECUCIÓN:1.10 Uso aceptable de la información y otros activos asociados, documentado e implementado	0,43
20	EJECUCIÓN:1.11 Devolución de activos, documentado e implementado	0,43
21	EJECUCIÓN:1.12 Clasificación de la información, documentado e implementado	0,43
22	EJECUCIÓN:1.13 Etiquetado de la información, documentado e implementado	0,43
23	EJECUCIÓN:1.14 Transferencia de información, documentado e implementado	0,43
24	EJECUCIÓN:1.15 Control de Acceso, documentado e implementado	0,43
25	EJECUCIÓN:1.16 Gestión de Identidad, documentado e implementado	0,43
26	EJECUCIÓN:1.17 Información de autenticación, documentado e implementado	0,43
27	EJECUCIÓN:1.18 Derechos de acceso, documentado e implementado	0,43
28	EJECUCIÓN:1.19 Seguridad de la información en las relaciones con proveedores, documentado e implementado	0,43
29	EJECUCIÓN:1.20 Seguridad de la información en los acuerdos con proveedores, documentado e implementado	0,43
30	EJECUCIÓN:1.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC, documentado e implementado	0,43
31	EJECUCIÓN:1.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores, documentado e implementado	0,43
32	EJECUCIÓN:1.23 Seguridad de la información para el uso de servicios en la nube, documentado e implementado	0,43
33	EJECUCIÓN:1.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, documentado e implementado	0,43
34	EJECUCIÓN:1.25 Evaluación y decisión sobre eventos de seguridad de la información, documentado e implementado	0,43
35	EJECUCIÓN:1.26 Respuesta a incidentes de seguridad de la información, documentado e implementado	0,43
36	EJECUCIÓN:1.27 Aprendiendo de los incidentes de seguridad de la información, documentado e implementado	0,43
37	EJECUCIÓN:1.28 Recopilación de evidencias, documentado e implementado	0,43

38	EJECUCIÓN:1.29 Seguridad de la Información durante la interrupción, documentado e implementado	0,43
39	EJECUCIÓN:1.30 Preparación de las TIC para la continuidad del Negocio, documentado e implementado	0,43
40	EJECUCIÓN:1.31 Requisitos legales, estatutarios, reglamentarios y contractuales, documentado e implementado	0,43
41	EJECUCIÓN:1.32 Derechos de propiedad intelectual, documentado e implementado	0,43
42	EJECUCIÓN:1.33 Protección de los registros, documentado e implementado	0,43
43	EJECUCIÓN:1.34 Privacidad y protección de PII, documentado e implementado	0,43
44	EJECUCIÓN:1.35 Revisión independiente de seguridad de la información, documentado e implementado	0,43
45	EJECUCIÓN:1.36 Cumplimiento de políticas, reglas y normas de seguridad de la información, documentado e implementado	0,43
46	EJECUCIÓN:1.37 Procedimientos operativos, documentado e implementado	0,43
47	EJECUCIÓN:2.1 Selección de personas, documentado e implementado	0,43
48	EJECUCIÓN:2.2 Términos y condiciones de empleo, documentado e implementado	0,43
49	EJECUCIÓN:2.3 Concienciación, educación y formación en seguridad de la información, documentado e implementado	0,43
50	EJECUCIÓN:2.4 Proceso disciplinario, documentado e implementado	0,43
51	EJECUCIÓN:2.5 Responsabilidades después de la terminación o cambio de empleo, documentado e implementado	0,43
52	EJECUCIÓN:2.6 Acuerdo de confidencialidad o no divulgación, documentado e implementado	0,43
53	EJECUCIÓN:2.7 Trabajo remoto, documentado e implementado	0,43
54	EJECUCIÓN:2.8 Reporte de eventos de seguridad de la información, documentado e implementado	0,43
55	EJECUCIÓN:3.1 Perímetros de seguridad física, documentado e implementado	0,43
56	EJECUCIÓN:3.2 Entrada física, documentado e implementado	0,43
57	EJECUCIÓN:3.3 Seguridad de oficinas, despachos e instalaciones, documentado e implementado	0,43
58	EJECUCIÓN:3.4 Monitoreo de seguridad física, documentado e implementado	0,43
59	EJECUCIÓN:3.5 Protección contra las amenazas externas y ambientales, documentado e implementado	0,43
60	EJECUCIÓN:3.6 Trabajo en áreas seguras, documentado e implementado	0,43
61	EJECUCIÓN:3.7 Puesto de trabajo despejado y pantalla limpia, documentado e implementado	0,43
62	EJECUCIÓN:3.8 Ubicación y protección de equipos, documentado e implementado	0,43
63	EJECUCIÓN:3.9 Seguridad de los activos fuera de las instalaciones, documentado e implementado	0,43
64	EJECUCIÓN:3.10 Medios de almacenamiento, documentado e implementado	0,43
65	EJECUCIÓN:3.11 Servicios de Soporte, documentado e implementado	0,43
66	EJECUCIÓN:3.12 Seguridad del cableado, documentado e implementado	0,43
67	EJECUCIÓN:3.13 Mantenimiento de equipo, documentado e implementado	0,43
68	EJECUCIÓN:3.14 Eliminación segura o reutilización de equipos, documentado e implementado	0,43
69	EJECUCIÓN:4.1 Dispositivos de usuario final, documentado e implementado	0,43
70	EJECUCIÓN:4.2 Derechos de acceso privilegiado, documentado e implementado	0,43
71	EJECUCIÓN:4.3 Restricción de acceso a la información, documentado e implementado	0,43
72	EJECUCIÓN:4.4 Acceso al código fuente, documentado e implementado	0,43
73	EJECUCIÓN:4.5 Autenticación Segura, documentado e implementado	0,43
74	EJECUCIÓN:4.6 Gestión de la capacidad, documentado e implementado	0,43
75	EJECUCIÓN:4.7 Protección contra malware, documentado e implementado	0,43
76	EJECUCIÓN:4.8 Gestión de vulnerabilidades técnicas, documentado e implementado	0,43
77	EJECUCIÓN:4.9 Gestión de la Configuración, documentado e implementado	0,43
78	EJECUCIÓN:4.10 Eliminación de información, documentado e implementado	0,43
79	EJECUCIÓN:4.11 Enmascaramiento de datos, documentado e implementado	0,43
80	EJECUCIÓN:4.12 Prevención de fuga de datos, documentado e implementado	0,43
81	EJECUCIÓN:4.13 Copia de seguridad de la información, documentado e implementado	0,43

82	EJECUCIÓN:4.14 Redundancia de las instalaciones de tratamiento de información	0,43
83	EJECUCIÓN:4.15 Registros de eventos, documentado e implementado	0,43
84	EJECUCIÓN:4.16 Actividades de monitoreo, documentado e implementado	0,43
85	EJECUCIÓN:4.17 Sincronización de reloj, documentado e implementado	0,43
86	EJECUCIÓN:4.18 Uso de programas de utilidad privilegiados, documentado e implementado	0,43
87	EJECUCIÓN:4.19 Instalación de software en sistemas operativos, documentado e implementado	0,43
88	EJECUCIÓN:4.20 Seguridad de redes, documentado e implementado	0,43
89	EJECUCIÓN:4.21 Seguridad de los servicios de red, documentado e implementado	0,43
90	EJECUCIÓN:4.22 Separación en las redes, documentado e implementado	0,43
91	EJECUCIÓN:4.23 Filtrado web, documentado e implementado	0,43
92	EJECUCIÓN:4.24 Uso de criptografía, documentado e implementado	0,43
93	EJECUCIÓN:4.25 Ciclo de vida de desarrollo seguro, documentado e implementado	0,43
94	EJECUCIÓN:4.26 Requisitos de seguridad de la aplicación, documentado e implementado	0,43
95	EJECUCIÓN:4.27 Arquitectura del sistema seguro y principios de ingeniería, documentado e implementado	0,43
96	EJECUCIÓN:4.28 Codificación Segura, documentado e implementado	0,43
97	EJECUCIÓN:4.29 Pruebas de seguridad en el desarrollo y la aceptación, documentado e implementado	0,43
98	EJECUCIÓN:4.30 Desarrollo subcontratado, documentado e implementado	0,43
99	EJECUCIÓN:4.31 Separación de los entornos de desarrollo, prueba y producción, documentado e implementado	0,43
100	EJECUCIÓN:4.32 Gestión de cambios, documentado e implementado	0,43
101	EJECUCIÓN:4.33 Información de pruebas, documentado e implementado	0,43
102	EJECUCIÓN:4.34 Protección de los sistemas de información durante las pruebas de auditoría, documentado e implementado	0,43
103	EJECUCIÓN: 0.10 Informe del monitoreo del desempeño y los indicadores de la gestión del EGSI v3, documentado y aprobado	1
104	EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado	2
105	EJECUCIÓN: 0.12 Informe de los resultados de la revisión de la gestión del EGSI v3, documentado y aprobado	2
106	EJECUCIÓN: 0.13 Informe de los resultados de las medidas correctivas aplicadas al EGSI v3, documentado y aprobado	2
107	EJECUCIÓN: 0.14 Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información, documentado y aprobado	2
108	**CIERRE:** 0.15 Informe de cierre del proyecto EGSI v3, documentado y aprobado	1
	TOTAL	**100**