INSTRUCTIVO

“Reporte de los Avances en la Implementación del EGSI V3.0”

(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 reporte 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 de la Administración Pública Central (APC), que gestionan su planificación institucional bajo la metodología y Sistema Gobierno por Resultados – GPR

4. Reporte del cumplimiento de los hitos del proyecto EGSI V3.0 en GPR

Para el reporte 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 de la Administración Pública Central por parte de los siguientes funcionarios:

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

Las instituciones deben reportar en el sistema GPR dicha ficha, la cual permitirá realizar el control y seguimiento de la implementación del EGSI V3 en las instituciones de la APC.

Las “Fichas de cumplimiento de hitos” que deben reportarse son las que corresponden a los hitos homologados (Anexo 3), es decir ciento ocho (108).

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, desde el mes de enero

- 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
- 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.

- 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. Estas fechas se han planteado con el fin de garantizar el cumplimiento de los plazos establecidos en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003.

El reporte de las fichas de cumplimiento a través del sistema GPR, debería realizarse en las fechas planteadas y de acuerdo a la planificación interna de cada institución.

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 reportar el cumplimiento de los hitos en el sistema GPR

PASO 1:

Utilizar la ficha de cumplimiento para detallar las actividades desarrolladas, en cumplimiento de lo solicitado en cada hito. Esta ficha será el verificable, por tanto, se debe anexar al hito correspondiente en el sistema GPR.

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, 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: no se debe subir otro documento más que la ficha de cumplimiento, las evidencias serán validadas durante el proceso de evaluación que será informada oportunamente.

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, en el cual se describa o registre los motivos del no cumplimiento del hito. Este informe técnico firmado deberá conservarse en cada institución y será el verificable para el registro en las fichas de cumplimiento que correspondan a dichos hitos.

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 (verificables) que se carguen al sistema GPR:

EGSIV3_SiglasEntidad_NroHito_SecArchivo_FechadeCarga

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).
- **FechadeCarga:** Fecha en la que se realiza la carga del verificable al sistema GPR. La fecha deberá estar en el formato “AAAAMMDD” (sin espacios ni guiones).

Nota: Estos archivos (verificables) deberán ser firmados electrónicamente para que tengan validez.

Ejemplo:

a) Reporte de verificables por hito:

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

PASO 5:

Una vez definido los criterios para reportar los verificables, el siguiente paso es ingresar al sistema GPR y subir la ficha de cumplimiento a cada hito.

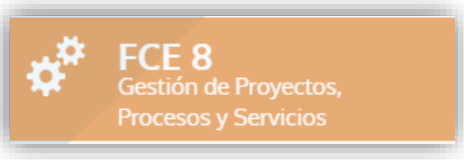
- Ingresar al sistema GPR a través del siguiente enlace: http://gpr.administracionpublica.gob.ec/gpr_ecuador/n4

Seleccionar los datos requeridos de validación de la unidad a la que pertenece:

- **Categoría**: Ministerios, Secretarías, otros
- **Entidad**: Institución respectiva
- **Organización/unidad:** Departamento respectivo
- **Unidad**: Unidad operativa donde labora el Oficial de Seguridad
- **Usuario y clave**: Credenciales del usuario registrado en el sistema GPR

PASO 6:

Escoger la opción “FCE8: Gestión de Proyectos y Procesos”

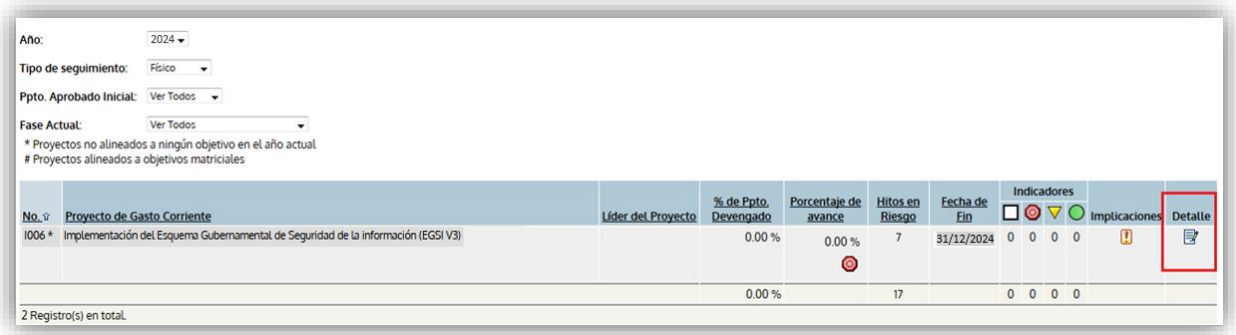


PASO 7:

Escoger la opción “**Proyectos de Gasto Corriente**” del menú que se despliega

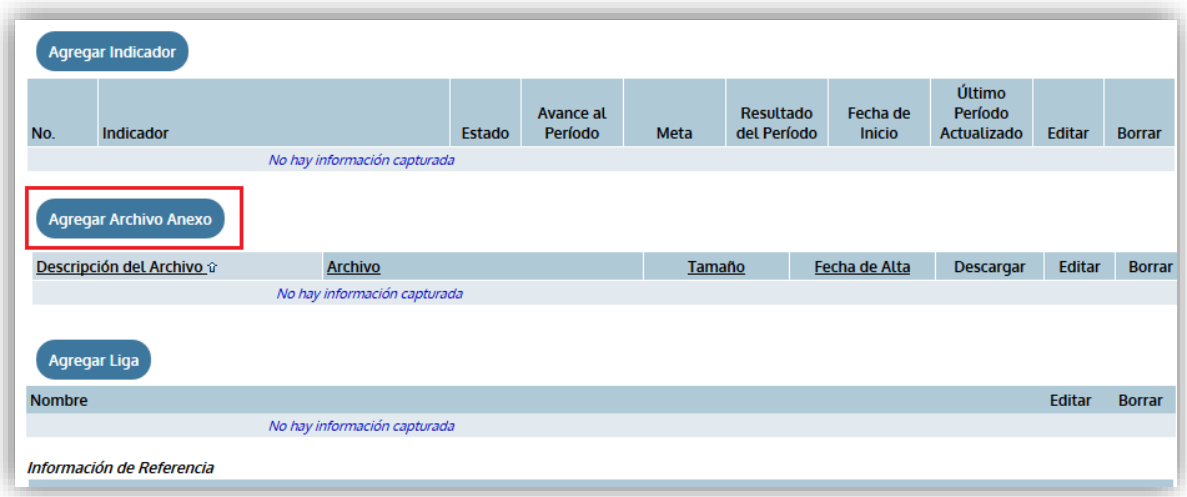
PASO 8:

Escoger el nombre del proyecto **“Implementación del Esquema Gubernamental de Seguridad de la Información (EGSI V3)”** y dar clic en el ícono de la columna “**Detalle**”.



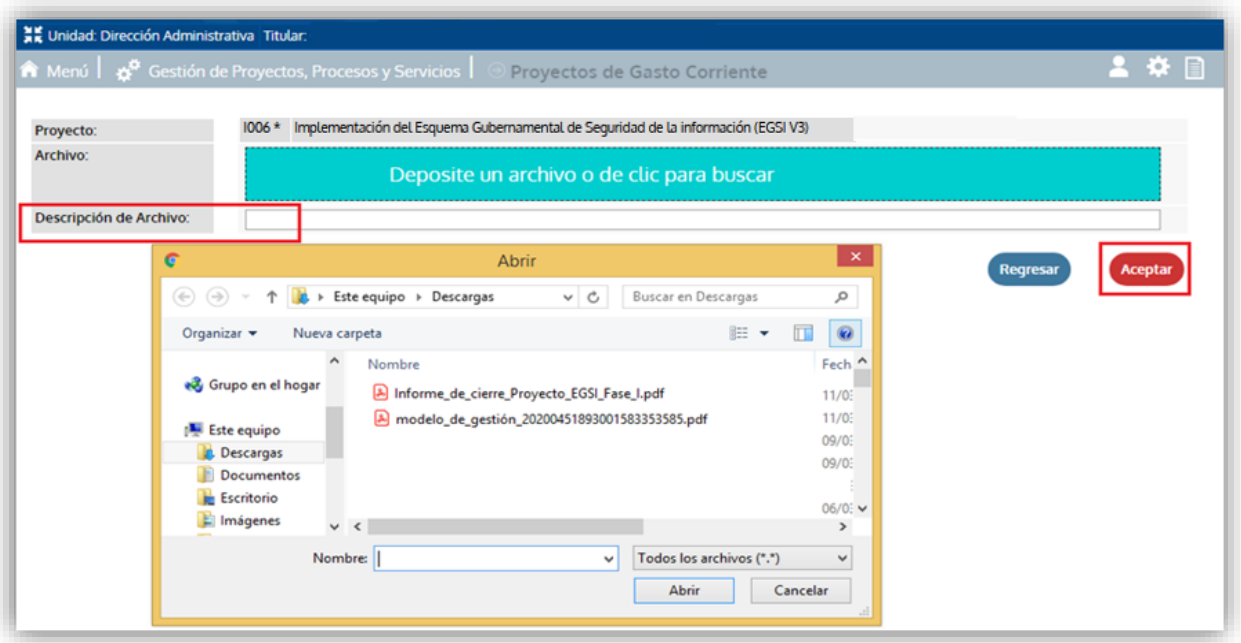
PASO 9:

Ubicarse en la parte inferior de la ficha del proyecto y dar clic en la opción "**Agregar Archivo Anexo**" como lo indica la siguiente figura:



PASO 10:

Hacer clic en "**Examinar"**, seleccionar el archivo PDF a subir, ingresar la "**Descripción del Archivo"** con el mismo nombre del archivo cargado omitiendo la extensión ".pdf" y hacer clic en la opción "**Aceptar"**.



Por ejemplo, si el nombre del archivo es: "EGSI_MINTEL_2.6_01_20240211.pdf"; en el campo "**Descripción de Archivo**" se debe ingresar como: "EGSI_MINTEL_2.6_01_20240211"

PASO 11:

Ubicar la opción "**Editar Hitos**" y hacer clic.

No.	Riesgo	actualización	Responsable	Probabilidad	Impacto	Calificación*	Totales	Editar	Borrar
	No hay información capturada								

Riesgos cerrados: 0, Abiertos: 0 — * probabilidad x impacto: más bajo = 1, más alto = 100.

Editar localidades

No.	Localidad de Impacto
	No hay información capturada

Editar Hitos

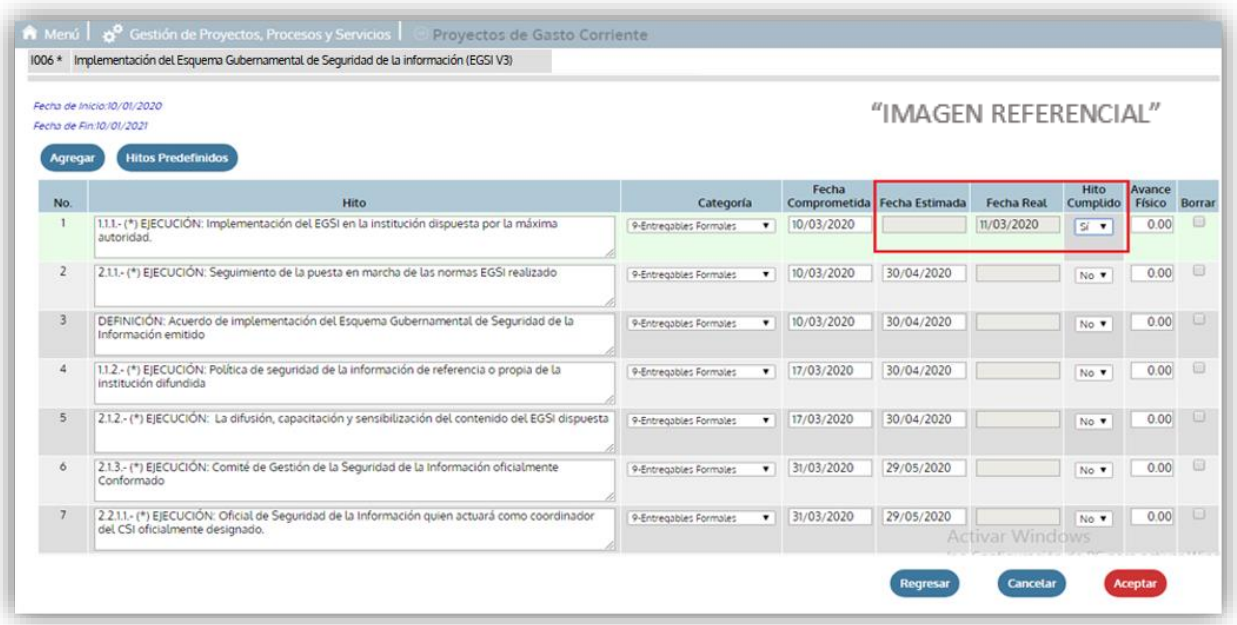
"IMAGEN REFERENCIAL"

No.	Hito	Categoría	Fecha Comprometida	Fecha Estimada	Fecha Real	A tiempo	Hito Cumplido	Avance Físico
1	1.1.1.- (*) EJECUCIÓN: Implementación del EGSI en la institución dispuesta por la máxima autoridad.	9-Entregables Formales	10/03/2020	30/04/2020		▽	No	0.0
2	2.1.1.- (*) EJECUCIÓN: Seguimiento de la puesta en marcha de las normas EGSI realizado	9-Entregables Formales	10/03/2020	30/04/2020		▽	No	0.0
3	DEFINICIÓN: Acuerdo de implementación del Esquema Gubernamental de Seguridad de la Información emitido	9-Entregables Formales	10/03/2020	30/04/2020		▽	No	0.0
4	1.1.2.- (*) EJECUCIÓN: Política de seguridad de la información de referencia o propia de la institución difundida	9-Entregables Formales	17/03/2020	30/04/2020		▽	No	0.0
5	2.1.2.- (*) EJECUCIÓN: La difusión, capacitación y sensibilización del contenido del EGSI dispuesta	9-Entregables Formales	17/03/2020	30/04/2020		▽	No	0.0
6	2.1.3.- (*) EJECUCIÓN: Comité de Gestión de la Seguridad de la Información oficialmente Conformado	9-Entregables Formales	31/03/2020	29/05/2020		▽	No	0.0
7	2.2.1.1.- (*) EJECUCIÓN: Oficial de Seguridad de la Información quien actuará como coordinador del CSI oficialmente designado.	9-Entregables Formales	31/03/2020	29/05/2020		▽	No	0.0
8	2.2.1.2.- (*) EJECUCIÓN: Responsable de seguridad del área de Tecnologías de la Información oficialmente designado.	9-Entregables Formales	31/03/2020	29/05/2020		▽	No	0.0
9	2.5.1.- (*) EJECUCIÓN: Acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las	9-Entregables	31/03/2020	29/05/2020		▽	No	0.0

PASO 12:

Ubicar el hito respectivo al cual se ha dado cumplimiento y modificar la "**Fecha Estimada**" por la fecha en la cual se realizó el cumplimiento.

Ubicar en la columna "**Hito Cumplido**", el hito respectivo y seleccionar "**Si**", tal como lo indica en la siguiente figura:



Menú | Gestión de Proyectos, Procesos y Servicios | Proyectos de Gasto Corriente

I006 * Implementación del Esquema Gubernamental de Seguridad de la información (EGSI V3)

Fecha de Inicio:10/01/2020
Fecha de Fin:10/01/2021

"IMAGEN REFERENCIAL"

Agregar | Hitos Predefinidos

No.	Hito	Categoría	Fecha Comprometida	Fecha Estimada	Fecha Real	Hito Cumplido	Avance Físico	Borrar
1	1.1.1.- (*) EJECUCIÓN: Implementación del EGSI en la institución dispuesta por la máxima autoridad.	9-Entregables Formales	10/03/2020		11/03/2020	Si	0.00	
2	2.1.1.- (*) EJECUCIÓN: Seguimiento de la puesta en marcha de las normas EGSI realizado	9-Entregables Formales	10/03/2020	30/04/2020		No	0.00	
3	DEFINICIÓN: Acuerdo de implementación del Esquema Gubernamental de Seguridad de la Información emitido	9-Entregables Formales	10/03/2020	30/04/2020		No	0.00	
4	1.1.2.- (*) EJECUCIÓN: Política de seguridad de la información de referencia o propia de la institución difundida	9-Entregables Formales	17/03/2020	30/04/2020		No	0.00	
5	2.1.2.- (*) EJECUCIÓN: La difusión, capacitación y sensibilización del contenido del EGSI dispuesta	9-Entregables Formales	17/03/2020	30/04/2020		No	0.00	
6	2.1.3.- (*) EJECUCIÓN: Comité de Gestión de la Seguridad de la Información oficialmente Conformado	9-Entregables Formales	31/03/2020	29/05/2020		No	0.00	
7	2.2.1.1.- (*) EJECUCIÓN: Oficial de Seguridad de la Información quien actuará como coordinador del CSI oficialmente designado.	9-Entregables Formales	31/03/2020	29/05/2020		No	0.00	

Activar Windows

Regresar | Cancelar | Aceptar

La "**Fecha Real**" se actualizará automáticamente con la fecha estimada que modificó anteriormente.

PASO 13:

Finalmente hacer clic en "**Aceptar**"**,** para actualizar la información.

5. Reporte del cumplimiento de los hitos del proyecto EGSI V3.0 a través de correo electrónico.

Para el reporte de los verificables de cumplimiento de cada uno de los hitos homologados, se debe utilizar la Plantilla de 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 de la Administración Pública Central por parte de los siguientes funcionarios:

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

Las instituciones deben reportar a través de correo electrónico dicha ficha, la cual permitirá realizar el control y seguimiento de la implementación del EGSI V3 en las instituciones de la APC.

Las "Fichas de cumplimiento de hitos" que deben reportarse son las que corresponden a los hitos homologados (Anexo 3), es decir ciento ocho (108).

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, desde el mes de enero

- 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
- 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.

- 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. Estas fechas se han planteado con el fin de garantizar el cumplimiento de los plazos establecidos en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003.

El reporte de las fichas de cumplimiento a través de correo electrónico, debería realizarse en las fechas planteadas y de acuerdo a la planificación interna de cada institución.

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.

5.1. Descripción de pasos para reportar el cumplimiento de los hitos a través de correo electrónico

PASO 1:

Utilizar la ficha de cumplimiento para detallar las actividades desarrolladas, en cumplimiento de lo solicitado en cada hito. Esta ficha será el verificable, por tanto, se debe anexar al correo electrónico con el que se reportará los avances del cumplimiento de la implementación del EGSI.

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, 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: no se debe adjuntar al correo electrónico otro documento más que la ficha de cumplimiento, las evidencias serán validadas durante el proceso de evaluación que será informada oportunamente.

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, en el cual se describa o registre

los motivos del no cumplimiento del hito. Este informe técnico firmado, deberá conservarse en cada institución y será el verificable para el registro en las fichas de cumplimiento que correspondan a dichos hitos.

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 (verificables) que se envíen a través de correo electrónico:

EGSIV3_SiglasEntidad_NroHito_SecArchivo_FechadeEnvío

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 enviado. 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).
- **FechadeEnvío:** Fecha en la que se realiza el envío del archivo a través de correo electrónico. La fecha deberá estar en el formato "AAAAMMDD" (sin espacios ni guiones).

Nota: Estos archivos (verificables) deberán ser firmados electrónicamente para que tengan validez.

Ejemplo:

a) Reporte de verificables por hito:

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

PASO 5:

Una vez definido los criterios para reportar los verificables a través de correo electrónico, el siguiente paso es redactar el contenido del correo electrónico, adjuntar la ficha de cumplimiento del hito a reportar e incluir la siguiente descripción de ejemplo como asunto:

- **Asunto:** Reporte de avances EGSIV3_MINTEL_0.0.5_01_20240211

Nota: ingresar como parte del asunto el nombre del archivo, omitiendo la extensión ".pdf", como muestra el ejemplo.

Finalmente enviar el correo electrónico a la dirección:

servicios@gobiernoelectronico.gob.ec

6. Contacto Soporte Técnico

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

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

7. Control de cambios

Versión:	1.1
Fecha de la versión:	27-09-2024
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

8. Historial de cambios

Versión	Fecha	Detalle de la modificación
1.0	05/02/2024	Emisión inicial del documento
1.1	27/06/2024	Actualización del contenido

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
1	**DEFINICIÓN:** 0.1 Perfil de Proyecto EGSI v3, documentado y aprobado	5/2/2024
2	PLANEACIÓN: 0.2 Definición del Alcance, documentado y aprobado	15/2/2024
3	PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado	28/2/2024
4	PLANEACIÓN: 0.4 Plan de evaluación Interna, documentado y aprobado	5/3/2024
5	PLANEACIÓN: 0.5 Política de Seguridad de la información (alto nivel), documentado y aprobado	15/3/2024
6	PLANEACIÓN: 0.6 Metodología de evaluación y tratamiento del riesgo, documentado y aprobado	31/3/2024
7	PLANEACIÓN: 0.7 Informe de la Evaluación de los Riesgos, documentado y aprobado	31/5/2024
8	PLANEACIÓN: 0.8 Declaración de Aplicabilidad (SoA), documentado y aprobado	10/6/2024
9	PLANEACIÓN: 0.9 Plan de Tratamiento de los riesgos, documentado y aprobado	**15/6/2024**
10	EJECUCIÓN:1.1 Políticas de seguridad de la información (específicas), documentado e implementado	**Desde:** 20/06/2024 **Hasta:** 20/10/2024
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	1/11/2024
104	EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado	15/11/2024
105	EJECUCIÓN: 0.12 Informe de los resultados de la revisión de la gestión del EGSI v3, documentado y aprobado	30/11/2024
106	EJECUCIÓN: 0.13 Informe de los resultados de las medidas correctivas aplicadas al EGSI v3, documentado y aprobado	15/12/2024
107	EJECUCIÓN: 0.14 Informe de cumplimiento de la Gestión de Riesgos de seguridad de la información, documentado y aprobado	25/12/2024
108	**CIERRE:** 0.15 Informe de cierre del proyecto EGSI v3, documentado y aprobado	**31/12/2024**