**FORMATO REFERENCIAL PARA LA ELABORACIÓN DEL**

**INFORME TÉCNICO**

**DE LOS CONTROLES DE SEGURIDAD NO SELECCIONADOS (EGSI v3)**

**Tabla de contenido**

[1. Antecedentes 3](#_Toc176775648)

[2. Objetivo del documento 3](#_Toc176775649)

[3. Controles no seleccionados 4](#_Toc176775650)

[3.1. Listado de controles no seleccionados o excluidos 4](#_Toc176775651)

[3.2. Justificación individual de controles excluidos de la implementación 4](#_Toc176775652)

[4. Glosario de términos 6](#_Toc176775653)

[5. Documentos de referencia 6](#_Toc176775654)

[6. Firmas de responsabilidad 6](#_Toc176775655)

[Control de versiones del formato referencial 7](#_Toc176775656)

[Historial de cambios del formato referencial 7](#_Toc176775657)

# Antecedentes

[INCLUIR EN CADA SECCIÓN, LA INFORMACIÓN QUE CORRESPONDE A SU INSTITUCIÓN; el texto del formato es una orientación para la elaboración de su propia documentación, que además requerirá de una investigación complementaria]

En esta sección se debe incluir el contexto necesario para comprender la importancia de documentar la justificación técnica de los controles no seleccionados (no necesarios, no aplicables) en la implementación del EGSI en la institución.

Tener presente que un “informe de no selección de controles” en un Sistema de Gestión de Seguridad de la Información, es un documento concluyente que explica por qué ciertos controles de seguridad recomendados no se han seleccionado para su implementación. Este informe debe ser claro y detallado para justificar la decisión y garantizar que la organización comprenda los riesgos asociados.

*[Ejemplo:*

*Debido a la necesidad de gestionar la seguridad de la información acorde a la evolución normativa y tecnológica, considerando que actualmente los riesgos en seguridad de la información muestran continuos cambios, se desarrollan nuevas amenazas y se revelan vulnerabilidades e incidentes de seguridad que tienen efectos considerables en la sociedad; el Ministerio de Telecomunicaciones y de la Sociedad de la Información a través del Acuerdo Ministerial No. 2024-0003 expidió el Esquema Gubernamental de Seguridad de la Información -EGSI- (versión 3.0), el cual es de implementación obligatoria en las Instituciones del Sector Público.*

*La metodología para la implementación del EGSI v3 socializada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, establece que, en caso de no ser posible la implementación de los controles determinados en el EGSI v3, deberá ser justificado técnicamente a través de un informe; en el que se debe incluir varios elementos clave para garantizar una comprensión clara de las razones detrás de esta decisión y sus implicaciones.*

 *En este contexto la selección de los controles de seguridad de la Información de la institución “X”, provino de un análisis que permitió identificar si cada uno de ellos resulta de aplicación o no en la institución. La aplicabilidad de los controles de seguridad de la información fue considerada según la actividad, la gestión interna y el entorno de la institución.]*

# Objetivo del documento

En esta sección se debe definir el objetivo del Informe de los controles no seleccionados.

*[Ejemplo:*

*Justificar los motivos por los cuales la institución excluyó los controles de seguridad, del grupo de noventa y tres (93) controles establecidos en el Esquema Gubernamental de Seguridad de la Información – EGSI v3 (…)]*

# Controles no seleccionados

## Listado de controles no seleccionados o excluidos

En esta sección se debe listar los controles de seguridad de la información que se han excluido de la implementación.

*[Ejemplo:*

|  |  |  |
| --- | --- | --- |
| ítem | Número de Control(Hito GPR) | Descripción del control |
| 1 | *[4.27]* | *[Arquitectura del sistema seguro y principios de ingeniería]* |
| 2 | *[2.7]* | *[Trabajo remoto]* |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |

*(…) ]*

## Justificación individual de controles excluidos de la implementación

En esta sección se debe justificar de manera individual y detallada los motivos por el cual fueron excluidos los controles de seguridad de la implementación del EGSI v3.

CONSIDERACIONES IMPORTANTES:

* La selección de los controles depende de las decisiones de las instituciones, basadas en los criterios de evaluación y aceptación de riesgos, las cuales deben estar alineadas a la legislación nacional vigente y a las necesidades instituciones.
* La selección de controles define el plan de tratamiento de riesgos que estará enmarcada en la implementación de los 93 controles del EGSI v3. Sin embargo, previo análisis, la institución puede agregar o excluir controles para la protección de la información.
* Aquellos controles no seleccionados, porque se consideran no aplicables (no necesarios, no seleccionados), se debe justificar su exclusión de manera detallada, este documento será el soporte durante la evaluación en sitio que se realice en cada institución y permitirá evidenciar que no se los ha considerado, ignorado o excluido arbitrariamente o de forma involuntaria.

Estos son algunos de los motivos por los que no se podría implementar un control:

* Información no utilizada: Si no gestionamos una determinada información como: los registros de eventos (Control: 4.15), o de gestión de las capacidades (Control: 4.6); no se puede implementar los controles asociados.
* Activos no disponibles: Si no se utilizan dispositivos móviles o portátiles, ya que sólo se dispone de equipos de sobremesa y fijos, no se puede definir Políticas en este sentido (Control: 4.1).
* Actividades no realizadas: Si no hay posibilidad por parte de los empleados de teletrabajar (Control: 2.7), o no se desarrolla software propio (Control: 4.25), o no se tiene área de carga y entrega (Control: 3.2); se puede excluir los controles asociados a estas actividades.
* Información no accesible: Si en la institución sólo se utilizan aplicaciones informáticas comerciales, ésta no es propietaria del código fuente del software que utiliza, ni tiene acceso a él (Control: 4.4). Lo mismo sucede con las claves criptográficas (Control: 4.24).
* No se comparte información: Si no se comparte información sensible con terceros, como pueden ser: clientes, proveedores, socios estratégicos, tampoco sería de aplicación este Control (Control: 1.14).
* No se justifica el esfuerzo de su aplicación: por diferentes decisiones de gestión estratégicas o de coste/efectividad.

*[Ejemplo:*

***Control****: 4.27 – Arquitectura del sistema seguro y principios de ingeniería:*

*El estatuto orgánico de gestión organizacional por procesos de la institución “X”, aprobado con Acuerdo Ministerial “No. XXX”, contempla en su estructura organizacional una Unidad de Gestión Tecnológica, sin embargo, en la institución no se realiza desarrollo de software, razón por la cual en esta unidad no existe personal asignado para dicha actividad. A continuación, se presenta el organigrama del “proceso”:*



*Fig. Estructura organizacional de la institución “X”*

***Control****: 2.7 – Trabajo remoto:*

*(…) ]*

# Glosario de términos

|  |  |
| --- | --- |
| Término | Definición |
| **EGSI** | Esquema Gubernamental de Seguridad de la Información |
|  |  |

# Documentos de referencia

En esta sección incluir las referencias documentales o normativas usadas para la elaborar el plan.

*[Ejemplo:*

* *Acuerdo Ministerial Nro. 2024-0003.*
* *Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)*
* *Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, NTE INEN-ISO/IEC 27002, NTE INEN-ISO/IEC 27005*
* *Agenda y Reglamento Interno del Comité de Seguridad de la Información.*
* *(…)*

*]*

# Firmas de responsabilidad

|  |  |  |
| --- | --- | --- |
|  | Nombre/Cargo | Firma |
| **Elaborado por:** | Quién elaboró el documento |  |
| **Revisado por:** | Quién revisó el documento |  |
| **Aprobado por:** | Quién aprobó el documento |  |

# Control de versiones del formato referencial

|  |  |
| --- | --- |
| **Versión**: | 1.0 |
| **Fecha de la versión**: | 09-09-2024 |
| **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 |

# Historial de cambios del formato referencial

|  |  |  |
| --- | --- | --- |
| **Versión** | **Fecha** | **Detalle del cambio** |
| 1.0 | 09/09/2024 | Emisión inicial del documento |