*[Logo de la institución]*

*[Nombre de la institución]*

**INFORME DE CUMPLIMIENTO DE LA GESTIÓN DE RIESGOS**

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





*[versión 1.0]*

**Tabla de contenido**

[1. Descripción de la institución 3](#_Toc165474415)

[2. Estándar y/o Metodología de Gestión de Riesgos 3](#_Toc165474416)

[3. Definición del Contexto 3](#_Toc165474417)

[4. Valoración del Riesgo 4](#_Toc165474418)

[4.1. Identificación de Activos de Información 4](#_Toc165474419)

[4.2. Identificación de Amenazas y Vulnerabilidades 5](#_Toc165474420)

[4.3. Identificación de controles existentes 5](#_Toc165474421)

[4.4. Evaluación del Riesgo 6](#_Toc165474422)

[5. Tratamiento del Riesgo 7](#_Toc165474423)

[5.1. Selección de controles 7](#_Toc165474424)

[6. Niveles de Riesgo una vez implementados los controles 7](#_Toc165474425)

[7. Aceptación del Riesgo 8](#_Toc165474426)

[8. Plan de acción 9](#_Toc165474427)

[9. Conclusiones y Recomendaciones 9](#_Toc165474428)

[10. Revisión y actualización 9](#_Toc165474429)

[11. Documentos de referencia 10](#_Toc165474430)

[12. Firmas de Responsabilidad 10](#_Toc165474431)

[Anexo 1 12](#_Toc165474432)

[Controles de seguridad - Esquema Gubernamental de Seguridad de la Información 12](#_Toc165474433)

# Descripción de la institución

[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:

* Misión
* Visión
* Objetivos estratégicos institucionales, y;
* Organigrama.

Adicionalmente incluir los Objetivos de la Seguridad de la Información, estos objetivos deben estar alineados a los objetivos estratégico institucionales.

# Estándar y/o Metodología de Gestión de Riesgos

En esta sección se debe describir de manera breve que estándar y/o metodología se seleccionó para el proceso de gestión de los riesgos de la seguridad de la información en la institución.

La máxima autoridad a través del Comité de Seguridad de la Información, el nivel directivo y todo el personal de la institución serán responsables de efectuar el proceso de la Gestión los riesgos de la Seguridad de la Información, que implica la selección del estándar/metodología, estrategias, técnicas y procedimientos, a través de los cuales les permitan a las unidades administrativas, identificar, analizar y tratar los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos institucionales.

# Definición del Contexto

En esta sección ingresar de manera resumida el alcance definido para la Gestión de los riesgos de seguridad de la información de acuerdo a lo establecido en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003 y su Anexo (EGSI V3).

Para que la institución pueda conocer los riesgos a los que está expuesta debe conocer el entorno interno y externo en el cual busca definir y lograr sus objetivos.

Se debe establecer el contexto para la gestión del riesgo de la seguridad de la información, lo cual implica establecer los criterios básicos que son necesarios para la gestión del riesgo de la seguridad de la información: definir el alcance y los límites, establecer una organización adecuada que opere la gestión del riesgo de la seguridad de la información.

# Valoración del Riesgo

La valoración del riesgo le ayuda a la institución a tomar decisiones de cómo: tratar los riesgos, mantener los controles existentes, revaluar los objetivos, entre otros. Las decisiones se deberían tomar de acuerdo con los requisitos legales, reglamentarios y requisitos de otro tipo

Los riesgos se deberían identificar, describir cuantitativamente o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la institución.

En este proceso se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. La valoración del riesgo consta de las siguientes actividades:

## Identificación de Activos de Información

En esta sección se debe listar de manera general los activos de información que fueron valorados dentro del proceso de Gestión de Riesgos.

Adicionalmente se debe describir los criterios seleccionados para la valoración de los activos de información, en el ejemplo que se muestra a continuación, se define en función de los principios de la seguridad de la información.



*[Ejemplo referencial, Criterio para valorar el impacto]*

La identificación de los activos es un punto clave para: la identificación de las amenazas, vulnerabilidades, determinar el nivel de riesgo o exposición de los activos y la selección de controles, para mitigarlos.

De este proceso se genera una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia.

## Identificación de Amenazas y Vulnerabilidades

En esta sección se debe identificar las amenazas y sus orígenes. Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, a las organizaciones. Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo los activos que se vean afectados.

Se debe identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la institución. La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla

Finalmente, se debe describir los criterios seleccionados para la valoración de la probabilidad de ocurrencia de amenazas y la probabilidad de ocurrencia de vulnerabilidades.



*[Ejemplo referencial, Criterio para valorar la probabilidad]*

## Identificación de controles existentes

En esta sección se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de los controles. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente, una referencia a los reportes de auditoría del SGSI ya existente debería limitar el tiempo que tarda esta labor. Si el control no funciona como se espera, puede causar vulnerabilidades.

Resumir el número de controles existentes que la institución ha identificado (previo a la identificación del riesgo inherente) en relación a los 93 controles que son parte del Anexo del EGSI V3.

|  |  |  |
| --- | --- | --- |
| **ÍTEM** | **GRUPO DE CONTROLES** | **Controles existentes** |
| 1 | Controles de PERSONAS |   |
| 2 | Controles FISICOS |   |
| 3 | Controles ORGANIZACIONALES |   |
| 4 | Controles TECNOLÓGICOS |   |
|  | **TOTAL** |  |

## Evaluación del Riesgo

En esta sección se debe describir los criterios seleccionados para el cálculo de la Evaluación de los riesgos y su semaforización; así como un mapa de calor que muestre los riesgos identificados por nivel. Ejemplo:

El producto de: la probabilidad de ocurrencia de una amenaza, la probabilidad de ocurrencia de vulnerabilidades y el valor del impacto del activo de la información (CID), tenemos como resultado el nivel de riesgo de cada activo, es decir:

*𝑵𝒊𝒗𝒆𝒍 𝒅𝒆 𝒓𝒊𝒆𝒔𝒈𝒐= 𝐕𝐀(𝐂𝐈𝐃)∗ 𝐍𝐢𝐯𝐞𝐥 𝐝𝐞 𝐚𝐦𝐞𝐧𝐚𝐳𝐚 ∗𝐍𝐢𝐯𝐞𝐥 𝐝𝐞 𝐯𝐮𝐥𝐧𝐞𝐫𝐚𝐛𝐢𝐥𝐢𝐝𝐚𝐝*



*[Ejemplo referencial, Nivel de los riesgos]*



*[Ejemplo referencial, Mapa de Calor de los niveles de riesgos]*

|  |
| --- |
| **RESUMEN DE LOS RIESGOS IDENTIFICADOS x NIVEL** |
| **Bajos** | **Medios** | **Altos** | **TOTAL** |
|   |   |   |   |

Recordar que la evaluación del riesgo es el proceso global de la identificación, análisis y valoración del riesgo.

# Tratamiento del Riesgo

En esta sección se debe describir de manera resumida, que tipos de riesgos (alto, medio, bajo) han sido parte del tratamiento de riesgos, los llamados riesgos NO ACEPTABLES.

Indicar cuáles de las 4 opciones de tratamiento fueron seleccionadas:

* Aplicar controles de seguridad obtenidos del Anexo (Guía para la implementación de controles de seguridad de la información) para modificar/reducir el riesgo.
* Compartir el riesgo con terceros, por ejemplo, comprando un seguro con una compañía aseguradora.
* Evitar riegos al detener la ejecución de la actividad que genera un elevado riesgo, o al hacerla de forma diferente.
* Aceptar el riesgo, por ejemplo, si el costo de atenuación es mayor que el daño en sí mismo.

El tratamiento del riesgo implica la selección y la implementación de una o varias opciones para modificar los riesgos, permite tomar decisiones frente a los diferentes riesgos existentes de acuerdo a la estrategia de la institución. Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo, el tratamiento de riesgo supone un proceso cíclico como:

* Formular y seleccionar opciones para el tratamiento del riesgo.
* Planificar e implementar el tratamiento del riesgo.
* Evaluar la eficacia del tratamiento del riesgo.
* Decidir si los niveles de riesgo residual son tolerables.
* Si no son tolerables, efectuar un tratamiento del riesgo adicional

## Selección de controles

En esta sección se debe especificar que controles de los 93 que son parte del Anexo del Esquema Gubernamental de Seguridad de la Información, son necesarios (aplicables) y se implementaron. Tomar como referencia el Anexo 1 de este documento para la selección de controles.

# Niveles de Riesgo una vez implementados los controles

En esta sección se debe representar gráficamente la cantidad de riesgos identificados en cada nivel, por ejemplo, bajo, medio, alto; una vez implementados los controles.

Los niveles de riesgo pueden ser representados gráficamente a través de un Mapa de Calor del Riesgo. Un mapa de calor de riesgo consiste en una matriz con dos ejes, donde el eje x representa la probabilidad de frecuencia del riesgo y el eje y representa el impacto que puede tener el mismo.

El mapa se representa gráficamente ubicando los riesgos en un cuadrante, dependiendo de la probabilidad de que determinado riesgo pueda ocurrir y el impacto cuantitativo o cualitativo que se produce en caso de que se materialice el riesgo.



*[Ejemplo referencial, Mapa de Calor de los niveles de riesgos]*

|  |
| --- |
| **RESUMEN DE LOS RIESGOS IDENTIFICADOS x NIVEL** |
| **Bajos** | **Medios** | **Altos** | **TOTAL** |
|   |   |   |   |

# Aceptación del Riesgo

En esta sección se debe describir las escalas o criterios definidas en cada institución, para los niveles de aceptación del riesgo. Se deberían considerar varios aspectos, entre los que podemos citar:

* Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.
* Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado.
* Los diferentes criterios de aceptación del riesgo se pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes, podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos, si esto se especifica como un requisito contractual.
* Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.



*[Ejemplo referencial, Niveles Aceptables y No Aceptables de los riesgos]*

Se deber tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarla de manera formal. Esta opción se toma cuando los costos de implementación de un control de seguridad sobrepasan el valor del activo de información que se desea proteger o cuando el nivel del riesgo es muy bajo, en ambos casos la organización asume los daños provocados por la materialización del riesgo.

# Plan de acción

En esta sección se debe describir de forma resumida el plan de acción a implementar, para la reducción de la probabilidad o del impacto en los riesgos que son parte del grupo NO ACEPTABLE, fundamentalmente con el análisis coste-beneficio.

# Conclusiones y Recomendaciones

En esta sección se debe incluir el resumen final obtenido con el desarrollo de esta gestión, además de las recomendaciones para el ciclo de mejora continua.

#  Revisión y actualización

Este documento debe ser revisado continuamente y estará sujeto a una actualización periódica que tendrá lugar anualmente y antes del año, cuando se realice un cambio significativo en los procesos/tecnologías o cuando lo considere oportuno el Comité de Seguridad de la información - CSI.

|  |  |
| --- | --- |
| **Revisión y actualización** | Oficial de Seguridad de la Información |
| **Aprobación** | Comité de Seguridad de la información |
| **Adopción** | Funcionarios que son parte de la implementación en la institución. |

# Documentos de referencia

En esta sección listar los documentos que se utilizó para la elaboración del presente informe.

Ejemplo:

* Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003
* Esquema Gubernamental de Seguridad de la Información (EGSI V3)
* Normas Técnicas ISO/IEC 27001, NTE INEN-ISO/IEC 27002, ISO/IEC 27005
* Agenda y Reglamento Interno del Comité de Seguridad de la Información.
* Y demás documentación generada durante el proceso de implementación y que se requiera para la elaboración del presente Informe.

# Firmas de Responsabilidad

|  |  |  |
| --- | --- | --- |
|  | **NOMBRE/CARGO** | **FIRMA** |
| **ELABORADO POR:** |  |  |
| **REVISADO POR:** |  |  |
| **APROBADO POR:** |  |  |

**Historial de modificaciones del formato elaborado por el MINTEL**

|  |  |  |
| --- | --- | --- |
| **Versión** | **Fecha** | **Detalle de la modificación** |
| 1.0 | 30/04/2024 | Emisión inicial del documento |

# Anexo 1

## Controles de seguridad - Esquema Gubernamental de Seguridad de la Información

**(EGSI V3)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nro.** | **Control** | **Implementado(SI/NO)** | **Observaciones** |
| 1.1 | Políticas de seguridad de la información (específicas) |   |   |
| 1.2 | Roles y Responsabilidades de Seguridad de la Información  |   |   |
| 1.3 | Separación de Funciones  |   |   |
| 1.4 | Responsabilidades de la dirección  |   |   |
| 1.5 | Contacto con las autoridades  |   |   |
| 1.6 | Contacto con grupos de interés especial  |   |   |
| 1.7 | Inteligencia de amenazas  |   |   |
| 1.8 | Seguridad de la información en la Gestión de proyectos  |   |   |
| 1.9 | Inventario de información y otros activos asociados  |   |   |
| 1.10 | Uso aceptable de la información y otros activos asociados  |   |   |
| 1.11 | Devolución de activos  |   |   |
| 1.12 | Clasificación de la información  |   |   |
| 1.13 | Etiquetado de la información  |   |   |
| 1.14 | Transferencia de información  |   |   |
| 1.15 | Control de Acceso  |   |   |
| 1.16 | Gestión de Identidad  |   |   |
| 1.17 | Información de autenticación  |   |   |
| 1.18 | Derechos de acceso  |   |   |
| 1.19 | Seguridad de la información en las relaciones con proveedores  |   |   |
| 1.20 | Seguridad de la información en los acuerdos con proveedores  |   |   |
| 1.21 | Gestión de la seguridad de la información en la cadena de suministro de las TIC |   |   |
| 1.22 | Monitoreo, revisión y gestión de cambios de servicios de proveedores  |   |   |
| 1.23 | Seguridad de la información para el uso de servicios en la nube  |   |   |
| 1.24 | Planificación y preparación de la gestión de incidentes de seguridad de la información  |   |   |
| 1.25 | Evaluación y decisión sobre eventos de seguridad de la información  |   |   |
| 1.26 | Respuesta a incidentes de seguridad de la información  |   |   |
| 1.27 | Aprendiendo de los incidentes de seguridad de la información  |   |   |
| 1.28 | Recopilación de evidencias  |   |   |
| 1.29 | Seguridad de la Información durante la interrupción  |   |   |
| 1.30 | Preparación de las TIC para la continuidad del Negocio  |   |   |
| 1.31 | Requisitos legales, estatutarios, reglamentarios y contractuales  |   |   |
| 1.32 | Derechos de propiedad intelectual  |   |   |
| 1.33 | Protección de los registros  |   |   |
| 1.34 | Privacidad y protección de PII  |   |   |
| 1.35 | Revisión independiente de seguridad de la información  |   |   |
| 1.36 | Cumplimiento de políticas, reglas y normas de seguridad de la información  |   |   |
| 1.37 | Procedimientos operativos  |   |   |
| 2.1 | Selección de personas  |   |   |
| 2.2 | Términos y condiciones de empleo  |   |   |
| 2.3 | Concienciación, educación y formación en seguridad de la información  |   |   |
| 2.4 | Proceso disciplinario  |   |   |
| 2.5 | Responsabilidades después de la terminación o cambio de empleo  |   |   |
| 2.6 | Acuerdo de confidencialidad o no divulgación  |   |   |
| 2.7 | Trabajo remoto  |   |   |
| 2.8 | Reporte de eventos de seguridad de la información  |   |   |
| 3.1 | Perímetros de seguridad física  |   |   |
| 3.2 | Entrada física  |   |   |
| 3.3 | Seguridad de oficinas, despachos e instalaciones  |   |   |
| 3.4 | Monitoreo de seguridad física  |   |   |
| 3.5 | Protección contra las amenazas externas y ambientales  |   |   |
| 3.6 | Trabajo en áreas seguras  |   |   |
| 3.7 | Puesto de trabajo despejado y pantalla limpia  |   |   |
| 3.8 | Ubicación y protección de equipos  |   |   |
| 3.9 | Seguridad de los activos fuera de las instalaciones  |   |   |
| 3.10 | Medios de almacenamiento  |   |   |
| 3.11 | Servicios de Soporte  |   |   |
| 3.12 | Seguridad del cableado  |   |   |
| 3.13 | Mantenimiento de equipo  |   |   |
| 3.14 | Eliminación segura o reutilización de equipos  |   |   |
| 4.1 | Dispositivos de usuario final  |   |   |
| 4.2 | Derechos de acceso privilegiado  |   |   |
| 4.3 | Restricción de acceso a la información  |   |   |
| 4.4 | Acceso al código fuente  |   |   |
| 4.5 | Autenticación Segura  |   |   |
| 4.6 | Gestión de la capacidad  |   |   |
| 4.7 | Protección contra malware  |   |   |
| 4.8 | Gestión de vulnerabilidades técnicas  |   |   |
| 4.9 | Gestión de la Configuración  |   |   |
| 4.10 | Eliminación de información  |   |   |
| 4.11 | Enmascaramiento de datos  |   |   |
| 4.12 | Prevención de fuga de datos  |   |   |
| 4.13 | Copia de seguridad de la información  |   |   |
| 4.14 | Redundancia de las instalaciones de tratamiento de información  |   |   |
| 4.15 | Registros de eventos  |   |   |
| 4.16 | Actividades de monitoreo  |   |   |
| 4.17 | Sincronización de reloj  |   |   |
| 4.18 | Uso de programas de utilidad privilegiados  |   |   |
| 4.19 | Instalación de software en sistemas operativos  |   |   |
| 4.20 | Seguridad de redes  |   |   |
| 4.21 | Seguridad de los servicios de red  |   |   |
| 4.22 | Separación en las redes  |   |   |
| 4.23 | Filtrado web  |   |   |
| 4.24 | Uso de criptografía  |   |   |
| 4.25 | Ciclo de vida de desarrollo seguro  |   |   |
| 4.26 | Requisitos de seguridad de la aplicación  |   |   |
| 4.27 | Arquitectura del sistema seguro y principios de ingeniería  |   |   |
| 4.28 | Codificación Segura  |   |   |
| 4.29 | Pruebas de seguridad en el desarrollo y la aceptación  |   |   |
| 4.30 | Desarrollo subcontratado  |   |   |
| 4.31 | Separación de los entornos de desarrollo, prueba y producción  |   |   |
| 4.32 | Gestión de cambios  |   |   |
| 4.33 | Información de pruebas  |   |   |
| 4.34 | Protección de los sistemas de información durante las pruebas de auditoría |   |   |