**INFORME DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS**

**ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI versión 2.0)**

# Objetivo

En esta sección se debe incluir el objetivo del documento.

*[Ejemplo:*

*El objetivo del presente documento es mostrar el resultado de la evaluación de riesgos y el tratamiento que se dará a los riesgos de seguridad de la información identificados ...]*

# Descripción de la institución

En esta sección se debe incluir la misión, visión, objetivos estratégicos y organigrama de la institución. Adicionalmente incluir los objetivos de la seguridad de la información, estos objetivos deben estar alineados a los objetivos estratégicos de la institución.

*[Ejemplo:*

*MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN*

***Misión****: ser el órgano rector del desarrollo de las tecnologías de la información y comunicación en el Ecuador, que incluyen las telecomunicaciones y el espectro radioeléctrico, que emite políticas, planes generales y realiza el seguimiento y evaluación de su implementación, coordinando acciones con los actores de los sectores estratégicos para garantizar el acceso igualitario a los servicios y promover su uso efectivo, eficiente y eficaz, que asegure el avance hacia la sociedad de la información para el buen vivir de la población ecuatoriana…**]*

# Contexto de la evaluación de riesgos

En esta sección se debe incluir de manera resumida el contexto definido para realizar la evaluación de riesgos, lo cual implica el establecimiento de los criterios básicos que son necesarios para la evaluación del riesgo de la seguridad de la información: definir el alcance y los límites.

*[Ejemplo:*

*La evaluación de riesgos se aplicó al proceso “X” definido en el alcance del Esquema Gubernamental de seguridad de la información (EGSI); es decir, a todos los activos que se utilizan dentro de la institución o que pueden tener un impacto sobre la seguridad de la información en el ámbito del EGSI…]*

# Metodología de evaluación y tratamiento de riesgos

## La metodología

En esta sección se debe incluir de manera resumida la metodología y/o estándar seleccionados para el desarrollo de la de evaluación de riesgos que se siguió al interior de la institución.

*[Ejemplo:*

*La evaluación de riesgos se realizó basados en el estándar “ISO 27005” y la metodología “Magerit” con el uso del cuadro de la matriz de evaluación de riesgos definido en el “Anexo del Acuerdo Ministerial No. 025-2019”. El proceso de evaluación de riesgos lo coordinó el Oficial de Seguridad de la Información al interior de la institución conjuntamente con el Comité de Seguridad de la Información…]*

## Identificación y valoración de los activos (impacto)

En esta sección se debe incluir de manera resumida un cuadro resumen de los tipos de activos de información identificados y los criterios que se usaron para la valoración de los activos de información.

*[Ejemplo*

*Tipo de activos de información identificados:*

|  |
| --- |
| ***Activos de Información Identificados*** |
| ***Tipo*** | ***Descripción*** |
| *Información física* | *Corresponde a todos los documentos físicos, como actas, acuerdos, circulares, informes, manuales, planes, entre otros.* |
| *Información digital* | *Corresponde a este tipo los archivos de datos digitales, archivados electrónicamente: Correos electrónicos, Copias de seguridad, Base de datos, entre otros.* |
| *Software* | *Corresponde al Software de aplicación, software del sistema, herramientas de desarrollo y utilidades, entre otros.* |
| *Servicios* | *Corresponde a los servicios tecnológicos que ayudan a la administración o flujo de información generada por los procesos de la institución, tales como el correo electrónico, office 365, telefonía IP, entre otros.* |

*Criterios seleccionados:*

*Para la evaluación del impacto se consideró los principios de la seguridad de la información en la que se analiza la pérdida de confidencialidad, disponibilidad o integridad; en qué medida afecta las finanzas, las obligaciones legales y contractuales o el prestigio de la institución. Para lo cual se estableció los siguientes criterios:*

|  |  |  |  |
| --- | --- | --- | --- |
| *Valoración del impacto* | *en términos de la perdida de la* ***confidencialidad*** *-* ***C****(Criterio)* | *en términos de la perdida de la* ***integridad*** *-* ***I****(Criterio)* | *en términos de la perdida de la* ***disponibilidad*** *-* ***D****(Criterio)* |
| *Alto (3)* | *La divulgación no autorizada de la información tiene un efecto crítico para la institución. (Ej. Divulgación de información confidencial o sensible)* | *La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución* | *El no acceso para aquellos que estén autorizados a la información o los sistemas tienen un efecto severo para la institución* |
| *Medio (2)* | *La divulgación no autorizada de la información tiene un efecto limitado para la institución. (Ej. Divulgación de información de uso interno)* | *La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución* | *El no acceso para aquellos que estén autorizados a la información o los sistemas tienen un efecto considerable para la institución* |
| *Bajo (1)* | *La divulgación de la información no tiene ningún efecto para la institución. (Ej. Divulgación de información pública)* | *La destrucción o modificación de la información tiene un efecto leve para la institución* | *El no acceso para aquellos que estén autorizados a la información o los sistemas tienen un efecto mínimo para la institución* |

 *La valoración del impacto de un activo (VA), resultó del promedio de los valores de las tres dimensiones de la Gestión de la Seguridad de la Información asociado a cada activo de información identificado:*

$$VA=\frac{C+I+D}{3}$$

*...]*

## Identificación de amenazas y vulnerabilidades (probabilidad)

En esta sección se debe describir los criterios seleccionados para la valoración de la probabilidad de ocurrencia de las amenazas y la probabilidad de ocurrencia de las vulnerabilidades.

*[Ejemplo:*

*Luego de la evaluación del impacto se procedió a evaluar la probabilidad de que se materialice ese riesgo; es decir, la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo en cuestión.*

*Se analizó si los controles de seguridad existentes son seguros y si hasta el momento han suministrado un adecuado nivel de protección. Para lo cual se estableció los siguientes criterios:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Valoración de la probabilidad* | *Estimación de la* ***amenaza****(criterio)* | *Ejemplo de amenaza (TI)* | *Estimación de la* ***vulnerabilidad****(criterio)* | *Ejemplo de vulnerabilidad (TI)* |
| *Alto (3)* | *La ocurrencia es muy probable (probabilidad > 50%)* | *Código malicioso* | *No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza* | *No se utilizan contraseñas para que los usuarios ingresen a los sistemas* |
| *Medio (2)* | *La ocurrencia es probable (probabilidad =50%)* | *Falla de hardware* | *Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable* | *Existen normas para la utilización de contraseñas, pero no se implementa* |
| *Bajo (1)* | *La ocurrencia es menos probable (probabilidad >0 y <50%)* | *desastres naturales* | *La medida de seguridad es adecuada* | *Existen normas para la utilización de contraseñas y es aplicada* |

## Identificación de controles existentes

En esta sección se debe describir en un cuadro resumen la cantidad o el porcentaje de controles existentes, es decir, controles ya implementados que la institución ha identificado en relación a los 115 controles que son parte del Anexo del EGSI versión 2.0.

*[Ejemplo:*

|  |
| --- |
| *Resumen de controles implementados por cada Dominio* |
| ***ítem*** | ***Dominio*** | ***ControlesEGSI V2*** | ***Controles implementados*** | ***Cumplimiento(%)*** |
| *1* | *Políticas de seguridad de la información* | *2* | *[1]* | *[100%]* |
| *2* | *Organización de la seguridad de la información*  | *8* |  |  |
| *3* | *Seguridad de los recursos humanos* | *6* |  |  |
| *4* | *Gestión de activos* | *10* |  |  |
| *5* | *Control de acceso* | *14* |  |  |
| *6* | *Criptografía* | *2* |  |  |
| *7* | *Seguridad física y del entorno* | *15* |  |  |
| *8* | *Seguridad de las operaciones* | *14* |  |  |
| *9* | *Seguridad en las comunicaciones* | *7* |  |  |
| *10* | *Adquisición, desarrollo y mantenimiento de los sistemas* | *13* |  |  |
| *11* | *Relaciones con proveedores* | *5* |  |  |
| *12* | *Gestión de incidentes de seguridad de la información* | *7* |  |  |
| *13* | *Aspectos de seguridad de la información para la gestión de la continuidad del negocio* | *4* |  |  |
| *14* | *Cumplimiento* | *8* |  |  |
|  | ***TOTAL*** | ***115*** |  |  |

***\**** *Ejem: de los 2 controles que tiene el Dominio, ítem 1, la institución tiene implementado 1 control al 100%*

*].*

## Evaluación del riesgo

En esta sección se debe describir los criterios seleccionados para el cálculo de la evaluación de los riesgos y su semaforización.

*[Ejemplo:*

*El nivel del riesgo se identificó como el resultado del producto de la probabilidad de ocurrencia de la amenaza, la probabilidad de ocurrencia de la vulnerabilidad y el valor del impacto del activo de la información (CID), es decir:*

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

*Con este resultado se estableció una semaforización que nos permitirá seleccionar una opción de tratamiento de los riesgos:*

|  |  |
| --- | --- |
| *El Riesgo es:* | *NIVEL DE RIESGO(nivel de amenaza \* nivel de vulnerabilidad \* VA)* |
| *ALTO* | *de 9 a 27* |
| *MEDIO* | *de 4 a 8* |
| *BAJO* | *de 1 a 3* |

*Los riesgos identificados en un nivel MEDIO y ALTO, es decir, cuyo resultado es desde 4 a 27, son riesgos NO aceptables y serán tratados. Mientras que los riesgos de nivel BAJO, es decir, cuyo resultado es desde 1 a 3 son riesgos aceptables y serán asumidos por la institución.*

## Tratamiento del riesgo

En esta sección se debe incluir las opciones de tratamiento que se considerará para la ejecución del Plan de Tratamiento de los riesgos.

*[Ejemplo:*

*El tratamiento de los riesgos se aplicará a todos los riesgos identificados como NO aceptables, para este proceso se ha definido cuatro opciones de tratamiento de riesgos:*

1. *Aplicar controles de seguridad obtenidos del Anexo (Guía para la implementación de controles de seguridad de la información) para disminuir/****reducir*** *el riesgo.*
2. ***Transferir*** *el riesgo a otras empresas/personas, por ejemplo, comprando un seguro con una compañía aseguradora.*
3. ***Evitar*** *riegos al detener la ejecución de la actividad que genera un elevado riesgo, o al hacerla de forma diferente.*
4. ***Aceptar*** *el riesgo, por ejemplo, si el costo de atenuación es mayor que el daño en sí mismo...]*

# Niveles de riesgo

En esta sección se debe exponer los niveles de riesgo, representados gráficamente a través de un mapa de calor del riesgo.

*[Ejemplo:*

*Una vez realizado el proceso de análisis y evaluación de los riesgos a continuación se presenta gráficamente a través de un mapa de calor los niveles de riesgo identificados, donde el eje “x” representa la probabilidad de frecuencia del riesgo y el eje “y” representa el impacto que puede tener el mismo.*



# Nota aclaratoria

Las instituciones de la Administración Pública Central, elaborarán el contenido de este documento basados en la metodología y/o estándar seleccionado internamente en su institución para el cumplimiento de la evaluación de los riesgos que es parte de la primera etapa de la implementación del Esquema Gubernamental de Seguridad de la Información.

**Historial de modificaciones**

|  |  |  |
| --- | --- | --- |
| **Versión** | **Fecha** | **Detalle de la modificación** |
| 1.0 | 23/09/2020 | Descripción básica del documento |
| 1.1 | 29/09/2020 | Modificación del contenido, documento final |