CONSEJO NACIONAL PARA LA IGUALDAD DE GÉNERO

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI versión 2.0)

Responsable: Rocío Balarezo B

2020

1. Objetivo

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en la institución y definir el nivel aceptable de riesgos según lo establecido en el Esquema Gubernamental de Seguridad de la información

2. Alcance

La evaluación y tratamiento de riesgos se aplican a todo 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.

3. Usuarios/as

Los/as usuarios/as de este documento son las y los servidores funcionarios/as del Consejo Nacional para la Igualdad de Género que participan en la evaluación y tratamiento de riesgos.

4. Metodología de evaluación y tratamiento de riesgos

4.1.El proceso

La evaluación de riesgos se implementa a través de la Matriz de evaluación de riesgos definida, el proceso de evaluación de riesgos es coordinado por la Oficial de Seguridad de la Información al interior de cada dirección, la identificación de amenazas y vulnerabilidades la realizan los/as propietarios/as de los activos, y la evaluación de consecuencias y probabilidad es realizada por los/as propietarios/as de los riesgos.

Propietario/a de los activos: puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El/la propietario/a del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución.

Propietario/a de los riesgos: Persona o entidad propietaria del riesgo con responsabilidad y autoridad para gestionar un riesgo

Para simplificar el proceso, se podría definir que el/a propietario/a del activo para cada riesgo también será el propietario/a del riesgo.

4.2.Activos, vulnerabilidades y amenazas

El primer paso en la evaluación de riesgos es la identificación de todos los activos dentro del alcance del EGSI; es decir, todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en la organización.

Los activos pueden ser:

- Personas
- Instalaciones
- Tecnología: hardware, software
- Información: impresa o electrónica
- Proveedores
- Suministros

Al identificar los activos también es necesario identificar a sus propietarios/as: la persona o unidad organizativa responsable de cada activo.

El siguiente paso es identificar todas las amenazas y vulnerabilidades relacionadas con cada activo. Las amenazas y vulnerabilidades se identifican utilizando los catálogos incluidos en la Norma Técnica NTE INEN-ISO/IEC 27005. Cada activo puede estar relacionado a varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

4.3.Identificación de los/as propietarios/as de riesgos

Para cada riesgo es necesario identificar un/a propietario/a.
Propietario del riesgo: es la persona o unidad organizativa responsable de cada riesgo. Esta persona puede o no ser la misma que el/a propietario/a del activo.
Para simplificar el proceso, se puede definir que el/a propietario/a del activo para cada riesgo también será el/a propietario/a del riesgo.

4.4.Impacto y probabilidad

Una vez que se han identificado las amenazas y vulnerabilidades, es necesario evaluar el impacto (consecuencias) para cada combinación de amenazas y vulnerabilidades de un activo específico en caso que ello se pueda producir:
Para evaluar el impacto se considera 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 o contractuales o el prestigio de la institución.

Valoración del impacto	en términos de la perdida de la **confidencialidad** (Criterio)	en términos de la perdida de la **integridad** (Criterio)	en términos de la perdida de la **disponibilidad** (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	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

	información pública)		

Ingresando los valores de confidencialidad, integridad y disponibilidad en la matriz de evaluación de riesgos, el valor del activo (VA) se calcula automáticamente sumando los tres valores y dividiendo para tres.
Luego de la evaluación del impacto es necesario 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 debe analizar si los controles de seguridad existentes son seguros y hasta el momento han suministrado un adecuado nivel de protección.

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

Ingresando los valores del impacto y probabilidad en la matriz de evaluación de riesgos, el **NIVEL DE RIESGO** se calcula automáticamente multiplicando los tres valores. Los controles de seguridad existentes tienen que ser ingresados en la columna **controles implementados existentes** de la matriz de evaluación de riesgos.

4.5.Criterios para la aceptación de riesgos

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

Los valores 1, 2 y 3 son riesgos aceptables, mientras que los valores desde 4 a 27 son riesgos no aceptables. Los riesgos no aceptables deben ser tratados.

4.6.Tratamiento del riesgo

El tratamiento de riesgos se implementa mediante el cuadro de tratamiento de riesgos de la matriz de evaluación de riesgos, seleccionando todos los riesgos identificados como no aceptables.

Para los riesgos calificados desde 4 a 27 se deben seleccionar una o más opciones de tratamiento: Reducción, Transferencia, Evitar o Aceptación del riesgo.

1. **Reducción del riesgo**, elección de control o controles de seguridad del Anexo del Acuerdo Ministerial No. 025-2019.
2. **Transferencia de los riesgos** a terceros; por ejemplo, suscribiendo una póliza de seguros o un contrato con proveedores o socios.
3. **Evitar los riesgos** discontinuando una actividad comercial que ocasiona ese riesgo.
4. **Aceptación del riesgo**: esta opción está permitida solamente si la selección de otras opciones de tratamiento del riesgo costaría más que el potencial impacto en el caso de que se materializara dicho riesgo.

La elección de opciones se implementa a través del cuadro de tratamiento de riesgos, columna **Método de tratamiento de Riesgos**, generalmente se escoge la opción 1: **Reducción del riesgo**.

Cuando se escogen varios controles de seguridad para un riesgo, se insertan filas adicionales en la tabla, inmediatamente debajo de la fila en que se especifica el riesgo.

El tratamiento de riesgos relacionados con procesos externalizados debe ser atendido por medio de contratos con los terceros responsables.

En el caso de la opción 1, es necesario evaluar el nuevo valor del impacto y probabilidad en el Cuadro de tratamiento de riesgos, para evaluar la efectividad de los controles planificados.

4.7.Revisiones periódicas de la evaluación y el tratamiento de riesgos

Los/as propietarios/as de riesgos deben revisar los riesgos vigentes y deben actualizar la Matriz de evaluación de riesgos y el Cuadro de tratamiento de riesgos de acuerdo con los nuevos riesgos identificados. La revisión se realiza al menos una vez por año, o con mayor frecuencia en caso de cambios organizacionales significativos, cambios importantes en tecnología, en los objetivos de negocios, en el entorno empresarial, otros.

4.8.Declaración de aplicabilidad y Plan de tratamiento del riesgo

La Oficial de Seguridad de la Información debe documentar en la Declaración de aplicabilidad: qué controles de seguridad del Anexo del Acuerdo Ministerial No. 025-2019 son aplicables y cuáles no, la justificación de esa decisión y si están implementados o no.

En nombre de los/as propietarios/as de riesgos, la máxima autoridad aceptará todos los riesgos residuales a través del Informe de cumplimiento de la Gestión de Riesgos.

La Oficial de Seguridad de la Información preparará el Plan de tratamiento de riesgos en el que se planificará la implementación de los controles. En nombre de los propietarios de riesgos, la máxima autoridad o el Comité de Seguridad de la Información en su representación, aprobará el Plan de tratamiento de riesgos.

4.9.Informes

La Oficial de Seguridad de la Información documentará los resultados de la evaluación y del tratamiento de riesgos, y de todas las revisiones subsiguientes, en el Informe de cumplimiento de la Gestión de Riesgos.

La Oficial de Seguridad de la Información supervisará el progreso de la implementación del Plan de tratamiento de riesgos e informará los resultados al Comité de Seguridad de la Información anualmente.

5. Validez y gestión de documentos

Este documento es válido hasta julio de 2021.
La propietaria de este documento es la Oficial de Seguridad de la Información, que debe verificar y actualizar el documento por lo menos una vez al año, antes de la revisión periódica sobre la evaluación de riesgos vigente.
Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- La cantidad de incidentes que se produjeron pero que no fueron incluidos en la evaluación de riesgos.
- La cantidad de riesgos que no fueron tratados adecuadamente.
- La cantidad de errores en el proceso de evaluación y tratamiento de riesgos debido a definiciones poco claras de funciones y responsabilidades.

6. Notas aclaratorias

La metodología de evaluación y tratamiento de riesgos, descrita en el presente documento está basada en la **GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** que es parte del Acuerdo Ministerial No. 025-2019 y en el Formato **Referencial Matriz de Riesgos de Seguridad de la Información (EGSI)**, que fue socializado meses atrás.

Las instituciones de la Administración Pública Central, elaborarán el contenido de este documento basados en la Metodología seleccionada internamente en su institución para el cumplimiento de la implementación del Esquema Gubernamental de Seguridad de la Información.

Historial de modificaciones

Versión	Fecha	Detalle de la modificación
1.1	1/12/2020	Descripción básica del documento

Dirección: Av. 12 de Octubre N24-41 y Foch
Código postal: 170523 / Quito-Ecuador
Teléfono: 593-2 255 6518 | 593-2 254 9342
www.igualdadgenero.gob.ec

Anexo 1

Matriz de evaluación de riesgos

Análisis de Riesgos						Evaluación de Riesgos					
						Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Proceso Macro	Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
		A1				0,00				0,00	
						0,00				0,00	
						0,00				0,00	

Cuadro de tratamiento de riesgos

Tratamiento de Riesgos							
Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	CID	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado
			0,00				
			0,00				
			0,00				
			0,00				

Dirección: Av. 12 de Octubre N24-41 y Foch
Código postal: 170523 / Quito-Ecuador
Teléfono: 593-2 255 6518 | 593-2 254 9342
www.igualdadgenero.gob.ec