

**METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS
ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA
INFORMACIÓN (EGSI versión 3.0)**

OCTUBRE 2025

Contenido

1. OBJETIVO	3
2. ALCANCE	3
3. USUARIOS	3
4. METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS.....	3
4.1. EL PROCESO	3
4.2. ACTIVOS, VULNERABILIDADES Y AMENAZAS	4
4.3. IDENTIFICACIÓN DE LOS PROPIETARIOS DE RIESGOS	4
4.4. IMPACTO Y PROBABILIDAD	5
4.5. CRITERIOS PARA LA ACEPTACIÓN DE RIESGOS.....	6
4.6. TRATAMIENTO DEL RIESGO	6
4.7. REVISIONES PERIÓDICAS DE LA EVALUACIÓN Y EL TRATAMIENTO DE RIESGOS.....	6
4.8. DECLARACIÓN DE APLICABILIDAD Y PLAN DE TRATAMIENTO DEL RIESGO	7
4.9. INFORMES	7
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS	7
6. NOTAS ACLARATORIAS	7
7. FIRMAS DE RESPONSABILIDAD	9
CONTROL DE VERSIONES.....	10
HISTORIAL DE MODIFICACIONES	10

1. Objetivo

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en la Empresa Pública de Comunicación del Ecuador EP y definir el nivel aceptable de riesgo según lo establecido en el Esquema Gubernamental de Seguridad de la información.

2. Alcance

La presente metodología tendrá como alcance, la definición de lineamientos básicos para el levantamiento de los activos de información, tasación de la criticidad, identificación, análisis y tratamiento de los riesgos de seguridad de la información; así como la evaluación de la eficiencia y/o eficacia de la aplicación de la presente metodología a base del resultado de los indicadores de procesos.

Adicionalmente el alcance de la presente será de forma transversal a todos los procesos institucionales, en los que se identifique procesos o servicios críticos, para el cumplimiento de la misión, en cuyo caso el Comité de Seguridad de la Información determinará como parte de sus atribuciones los roles y responsabilidades, adicionales a los que dispone la Política de Seguridad de la Información de la Empresa Pública de Comunicación del Ecuador EP.

3. Usuarios

Los usuarios de este documento son todos los empleados de la Empresa Pública de Comunicación del Ecuador EP que participan en la evaluación y tratamiento de riesgos.

4. Metodología de evaluación y tratamiento de riesgos

4.1. El proceso

La Metodología de Evaluación y Tratamiento de Riesgos, se establece en base de los lineamientos dispuestos por la Política de Seguridad de la Información establecida por la Empresa Pública de Comunicación del Ecuador EP, la norma ISO 27005 [1] y la metodología MAGERIT [2] con el uso del cuadro de la matriz de evaluación de riesgos que se ha definido (ANEXO 1).

El proceso de evaluación de riesgos es coordinado por el Oficial de Seguridad de la Información al interior de cada institución, la identificación de amenazas y vulnerabilidades la realizan los propietarios de los activos, y la evaluación de consecuencias y probabilidad es realizada por los propietarios de los riesgos.

Propietario 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 propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución.

Propietario de los riesgos: persona o entidad propietaria del riesgo con responsabilidad y autoridad para gestionar un 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 [3]; es decir, todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en la institución.

Tipo de activos identificados:

Categoría	Tipo de activo
Información	Información electrónica
	Información escrita
	información hablada
	Otro tipo de información
Software	Software comercial o herramientas, utilitarios
	Software desarrollado por terceros
	Software desarrollado internamente
	Software de administración de base de datos
	Otro software
Físicos (hardware, comunicaciones e infraestructura)	Equipo de procesamiento
	Equipo de comunicación
	Medio de almacenamiento
	Mobiliario y equipamiento
	Otros equipos
Servicios	Procesamiento y comunicación
	Servicios generales
	Otros servicios
Personal	Clientes (usuarios)
	Empleados
	Personal externo
Instalaciones	Control de acceso físico a las edificaciones y los recintos
Organización	Procedimientos y procesos
	Auditorías
Imagen y reputación	Imagen y reputación

Tabla 1: Categorías y tipos de activos.

Al identificar los activos también es necesario identificar a sus propietarios: 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 [4].

Cada activo puede estar relacionado a varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

4.3. Identificación de los propietarios de riesgos

Para cada riesgo es necesario identificar un propietario.

Propietario del riesgo: es la persona o unidad organizativa responsable de cada riesgo. Esta persona puede o no ser la misma que el propietario del activo.

Para simplificar el proceso, se puede definir que el propietario del activo para cada riesgo también será el propietario 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 de 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 pérdida de la <u>confidencialidad</u> (Criterio)	en términos de la pérdida de la <u>integridad</u> (Criterio)	en términos de la pérdida de la <u>disponibilidad</u> (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

Tabla 2: Escala de valor de los activos.

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 <u>amenaza</u> (criterio)	Ejemplo de amenaza (TI)	Estimación de la <u>vulnerabilidad</u> (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

Tabla 3: Nivel de amenaza y vulnerabilidad.

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

Tabla 4: Nivel de aceptación de riesgos.

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. El tratamiento de riesgos es realizado por el Oficial de Seguridad de la Información.

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 Nro. MINTEL-MINTEL-2024-0003.
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 propietarios 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 institucional, otros.

4.8. Declaración de aplicabilidad y Plan de tratamiento del riesgo

El Oficial de Seguridad de la Información debe documentar en la Declaración de aplicabilidad: qué controles de seguridad del Anexo del Acuerdo Nro. MINTEL-MINTEL-2024-0003 son aplicables y cuáles no, la justificación de esa decisión y si están implementados o no.

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

El 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

- El 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.
- El 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 trimestralmente.

5. Validez y gestión de documentos

El propietario de este documento es el 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

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.

Referencia:	[1] ISO 27002, Gestión de riesgos de la Seguridad la Información. [2] MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [3] EGSI, Esquema Gubernamental de Seguridad de la Información. [4] NTE INEN-ISO/IEC 27000, NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27000.
-------------	---

7. Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	Mgs. Angel Franco Calixto Oficial de Seguridad de la Información	
Revisado y aprobado por:	Eco. Mónica Salas Herrera Presidente del Comité de Seguridad de la Información	
Aprobado por:	Lcda. Ana Lizbeth Brito Figueroa Integrante del Comité de Seguridad de la Información	
Aprobado por:	Mgs. Grace Cordero Loor Integrante del Comité de Seguridad de la Información	
Aprobado por:	Espc. José Estrella Lopez Integrante del Comité de Seguridad de la Información	
Aprobado por:	Mgs. Omar Barrera Romero Integrante del Comité de Seguridad de la Información	

Control de versiones

Versión:	1.0
Fecha de la versión:	20-10-2025
Creado por:	Oficial de Seguridad de la Información de la Empresa Pública de Comunicación del Ecuador EP
Revisado por:	Comité de Seguridad de la Información de la Empresa Pública de Comunicación del Ecuador
Aprobado por:	Empresa Pública de Comunicación del Ecuador EP
Nivel de confidencialidad:	Bajo

Historial de modificaciones

Versión	Fecha	Detalle del cambio
1.0	20/10/2025	Emisión inicial del documento

ANEXO 1

Matriz de evaluación de riesgos

Análisis de Riesgos				Evaluación de Riesgos					
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
				VA (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							Riesgo residual
Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	