



## **PROCEDIMIENTO DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS**

Código:	GSI-PR-01
Versión:	0.1
Fecha de la versión:	12.08.2020
Creado por:	Oficial de Seguridad
Revisado por:	Comité de Seguridad de la Información
Aprobado por:	Comité de Seguridad de la Información
Nivel de confidencialidad:	Uso Interno

### Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
11.08.2020	0.1	Oficial de Seguridad	Creación del documento

## Tabla de contenido

<b>1. OBJETIVO .....</b>	<b>4</b>
<b>2. ALCANCE .....</b>	<b>4</b>
<b>3. VIGENCIA .....</b>	<b>4</b>
<b>4. DISTRIBUCIÓN .....</b>	<b>4</b>
<b>5. GLOSARIO DE TÉRMINOS Y/O DEFINICIONES .....</b>	<b>4</b>
<b>6. DOCUMENTOS DE REFERENCIA.....</b>	<b>5</b>
<b>7. CRITERIOS BÁSICOS .....</b>	<b>5</b>
7.1. CRITERIOS DE VALORACIÓN DE IMPACTO DE LOS ACTIVOS DE INFORMACIÓN .....	5
7.2. CRITERIOS DE PROBABILIDAD DE OCURRENCIA DE AMENAZAS Y PROBABILIDAD DE OCURRENCIA DE VULNERABILIDADES ....	6
7.3. CRITERIOS PARA LA EVALUACIÓN DEL RIESGO .....	7
7.4. CRITERIOS PARA LA ACEPTACIÓN DE RIESGOS .....	7
<b>8. METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS .....</b>	<b>7</b>
8.1. ANÁLISIS DE RIESGOS .....	7
8.1.1. <i>El proceso.....</i>	7
8.1.2. <i>Identificación y valoración de activos.....</i>	8
8.1.3. <i>Identificación de amenazas y vulnerabilidades.....</i>	8
8.2. EVALUACIÓN DEL RIESGO .....	8
8.3. TRATAMIENTO DEL RIESGO .....	8
8.4. REVISIONES PERIÓDICAS DE LA EVALUACIÓN Y EL TRATAMIENTO DE RIESGOS.....	9
8.5. DECLARACIÓN DE APLICABILIDAD Y PLAN DE TRATAMIENTO DEL RIESGO .....	9
8.6. INFORMES .....	9
<b>9. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO.....</b>	<b>9</b>
<b>10. VALIDEZ Y GESTIÓN DE DOCUMENTOS .....</b>	<b>11</b>
<b>11. ANEXOS .....</b>	<b>11</b>
11.1. ANEXO 1: IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS .....	12
11.2. ANEXO 2: CUADRO DE ANÁLISIS DE RIESGOS .....	12
11.3. ANEXO 3: CUADRO DE EVALUACIÓN DE RIESGOS .....	13
11.4. ANEXO 4: CUADRO DE TRATAMIENTO DE RIESGOS.....	13

## 1. OBJETIVO

Definir la metodología para evaluar y tratar los riesgos de la seguridad de la información de los activos de la información identificados en el INSTITUTO NACIONAL DE ESTADISTICA Y CENSOS y su nivel aceptable de riesgo.

## 2. ALCANCE

La evaluación y tratamiento de riesgos es aplicable a todos los activos de información de todos los procesos de institucionales actuales y futuros del Instituto Nacional de Estadística y Censos.

## 3. VIGENCIA

El presente documento tendrá vigencia a partir de la fecha de su aprobación.

## 4. DISTRIBUCIÓN

Los usuarios de este documento son todos los empleados de INSTITUTO NACIONAL DE ESTADISTICA Y CENSOS que participan en la evaluación y tratamiento de riesgos.

## 5. GLOSARIO DE TÉRMINOS Y/O DEFINICIONES

**Información:** conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado. La información, también es considerada uno de los activos que como otros activos importantes del INEC, tiene valor para la entidad y por lo tanto, se requiere proteger su confidencialidad, integridad y disponibilidad de las amenazas propias de su naturaleza y características, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

**Activo de Información:** Cualquier elemento o recurso que genera, procesa, transporta y/o resguarda información necesaria para la operación y el cumplimiento de los objetivos Institucionales y que tenga valor para la institución; por ejemplo un listado de personal (información) puede estar incluido en una hoja Excel (activo intangible), que se encuentra en un ordenador de sobremesa (activo material), situado en la oficina principal (activo material) del INEC.

**Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

**Vulnerabilidad:** Debilidad de un activo que puede ser explotada por una o más amenazas.

**Riesgo:** Es la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

**Riesgo Inherente:** Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

**Riesgo Residual:** Nivel resultante del riesgo después de aplicar los controles.

**Control:** Mecanismo que permite atenuar el riesgo inherente, con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que dicho riesgo se materialice.

**Confidencialidad:** Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.

**Integridad:** Propiedad de proteger la precisión y completitud de los activos.

**Disponibilidad:** Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada.

**EGSI:** Esquema Gubernamental de Seguridad de la Información.

**Procesos de negocio:** Conjunto de tareas destinadas a ofrecer un servicio o un producto a un cliente interno o externo.

## 6. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2013, capítulos 6.1.2, 6.1.3, 8.2, y 8.3
- Norma Técnica NTE INEN- ISO/IEC27005:2012 Gestión del Riesgo en la Seguridad de la Información
- Metodología de análisis y gestión de riesgos de los Sistemas de Información MAGERIT
- Acuerdo Ministerial No. 025-2019 del Ministerio de Telecomunicaciones de la Sociedad de la Información (EGSI v2.0).
- Política de Seguridad de la Información

## 7. CRITERIOS BÁSICOS

### 7.1. Criterios de valoración de impacto de los activos de información

Para determinar la criticidad de los distintos activos, en la presente metodología se evaluará en términos de “alto, medio o bajo”, donde se asigna un valor cuantitativo a cada valor cualitativo de impacto asociado a la pérdida de Confidencialidad, Integridad y Disponibilidad para cada activo, siendo los propietarios de la misma quienes lo califiquen, teniendo como criterios la siguientes tablas:

Valoración del impacto en términos de la pérdida de la **confidencialidad**

CONFIDENCIALIDAD	CRITERIO
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.

Valoración del impacto en términos de la pérdida de la **integridad**

INTEGRIDAD	CRITERIO
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución

Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución
----------	--

Valoración del impacto en términos de la pérdida de la **disponibilidad**

DISPONIBILIDAD	CRITERIO
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Basados en este criterio se podrá obtener el valor del impacto del activo de la Información (VA)

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

## 7.2. Criterios de probabilidad de ocurrencia de amenazas y probabilidad de ocurrencia de vulnerabilidades

A continuación se detalla los criterios cualitativos y cuantitativos para calcular la posibilidad de la ocurrencia de amenazas y que podrían explotar alguna vulnerabilidad existente.

### Estimación de amenazas

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es probable (probabilidad =50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Falla de hardware
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	En rara ocasión	El atacante no se beneficia del ataque	desastres naturales

### Estimación de vulnerabilidades

Nivel de	Criterio	Ejemplo
----------	----------	---------

vulnerabilidad		
Alto (3)	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)	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 medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

### 7.3. Criterios para la evaluación del riesgo

El nivel de riesgo se calcula multiplicando los factores de probabilidad e impacto:

Nivel de Riesgo = probabilidad \* impacto

Impacto= Valor del impacto del activo de la Información (VA)

Probabilidad: Nivel de amenaza \* Nivel de vulnerabilidad

Aplicando estos criterios se puede obtener la siguiente clasificación de los niveles de riesgo:

Tabla de evaluación del activo										
Nivel de Amenaza		Bajo (1)			Medio (2)			Alto (3)		
Nivel de Vulnerabilidades		Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)	Bajo (1)	Medio (2)	Alto (3)
Valor del impacto en términos de la pérdida de (CID) en los activos	Bajo (1)	1	2	3	2	4	6	3	6	9
	Medio (2)	2	4	6	4	8	12	6	12	18
	Alto (3)	3	6	9	6	12	18	9	18	27

Nivel de Riesgo	
1 - 3	El riesgo del activo es <b>BAJO</b>
4 - 8	El riesgo del activo es <b>MEDIO</b>
9 - 27	El riesgo del activo es <b>ALTO</b>

### 7.4. Criterios para la aceptación de riesgos

Nivel de Riesgo		Aceptabilidad	
1 - 3	El riesgo del activo es <b>BAJO</b>	RIESGO ACEPTABLE	No se deben aplicar opciones de tratamiento del riesgo
4 - 8	El riesgo del activo es <b>MEDIO</b>	RIESGO NO ACEPTABLE	Se deben aplicar opciones de tratamiento del riesgo
9 - 27	El riesgo del activo es <b>ALTO</b>		

Es posible que en el caso de que la Institución no encuentre controles para mitigar el riesgo, o que la implantación de controles pueda tener un costo mayor que las consecuencias del mismo se podrá tomar la decisión de aceptar el riesgo, siendo la Institución quien asume los daños provocados por la materialización del mismo.

## 8. METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

### 8.1. Análisis de riesgos

#### 8.1.1. El proceso

La evaluación de riesgos se implementa a través del Cuadro de evaluación de riesgos. El proceso de evaluación de riesgos es coordinado por el Oficial de Seguridad de la Información, la identificación de amenazas y vulnerabilidades la realizan los propietarios de los activos.

### **8.1.2. Identificación y valoración de activos**

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

Los activos pueden ser documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI, infraestructura y servicios externos o procesos externalizados. Al identificar los activos también es necesario identificar a sus propietarios: la persona o unidad organizativa responsable de cada activo Ver (**Anexo 1**).

### **8.1.3. Identificación de amenazas y vulnerabilidades**

El siguiente paso es identificar todas las amenazas y vulnerabilidades relacionadas con cada activo. Cada activo puede estar relacionado a varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades Ver (**Anexo 2**).

## **8.2. Evaluación del riesgo**

Una vez identificados los activos y su valoración, al igual que ya están identificadas las amenazas y vulnerabilidades, se procede a realizar la evaluación del riesgo, para lo cual se aplicará el criterio descrito el ítem 7.3 del presente documento, haciendo uso del cuadro de evaluación de riesgos Ver (**Anexo 3**).

## **8.3. Tratamiento del riesgo**

El tratamiento de riesgos se implementa mediante el Cuadro de tratamiento de riesgos Ver (**Anexo 4**).

Para los riesgos calificados en 4 y 27 se deben seleccionar una o más opciones de tratamiento.

1. **Mitigar los riesgos** utilizando los controles del Anexo A de la norma ISO/IEC 27001 u otros controles de seguridad, para reducir el riesgo a un nivel aceptable para la institución.
2. **Evitar el riesgo** cuando se busca eliminar actividad, fuente del riesgo o vulnerabilidad.
3. **Transferencia / Compartir el riesgo a terceros** con una entidad interna o externa, mediante el traspaso de la gestión del activo y/o del riesgo, por ejemplo suscribiendo una póliza de seguros o un contrato con proveedores o socios.
4. **Aceptación del riesgo** esta opción está permitida solamente si las selecciones de otras opciones de tratamiento del riesgo costarían 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. Generalmente, se escoge la opción 1: Mitigar los riesgos mediante la elección de uno o más controles de seguridad.

El tratamiento de riesgos relacionados con procesos externalizados debe ser atendido por medio de contratos con los terceros responsables, como se especifica en la Política de seguridad para proveedores.

En el caso de la opción 1 (Mitigar el riesgo), es necesario evaluar el nuevo valor de consecuencia y probabilidad en el Cuadro de tratamiento de riesgos, para evaluar la efectividad de los controles planificados.

En el caso de que el nivel de riesgo residual no satisfaga los criterios de aceptación del riesgo debido a que los criterios que se aplican no toman en consideración las circunstancias prevalentes; por ejemplo cuando el costo de la reducción del riesgo es demasiado alto, se tomará la decisión de aceptar el riesgo, para lo cual se deberá contar con la aprobación formal del Director Ejecutivo de la entidad, el Director del área propietario del activo y el oficial de Seguridad de la Información, previo proceso de evaluación por parte del Comité de Seguridad de la Información. Este tipo de riesgos serán ratificados en caso de que los mismos no hayan sido cerrados anualmente.

#### 8.4. Revisiones periódicas de la evaluación y el tratamiento de riesgos

Los propietarios de riesgos que a su vez son los propietarios de los activos deben revisar los riesgos vigentes y deben actualizar el Cuadro 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 institucionales, etc.

#### 8.5. Declaración de aplicabilidad y Plan de tratamiento del riesgo

El Responsable de Gestión de Seguridad de la Información debe documentar los siguiente en la Declaración de aplicabilidad: qué controles de seguridad del Anexo A de la norma ISO/IEC 27001 son aplicables y cuáles no, la justificación de esa decisión y si están implementados o no.

El Propietario del riesgo preparará el Plan de tratamiento de riesgos en el que se planificará la implementación de los controles y aprobará el mismo, esta información se reflejará mediante la columna "Aprobación del Plan de tratamiento" en el Cuadro de tratamiento de riesgos, en el que se identifique a la persona que aprueba y la fecha como constancia de aprobación.

#### 8.6. Informes

El Propietario del activo documentará los resultados de la evaluación y del tratamiento de riesgos, y de todas las revisiones subsiguientes, en el Informe de evaluación y tratamiento de riesgos.

El Responsable de Gestión 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 trimestral y por parte del semestral previa revision con el comite.

### 9. GESTIÓN DE REGISTROS GUARDADOS CON BASE A ESTE DOCUMENTO

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Cuadro de Identificación y valoración de activos (formulario)	Ordenador del Oficial de Seguridad de la	Oficial de Seguridad de la Información	Solamente el Oficial de Seguridad de la Información tiene derecho a crear entradas	Los datos son archivados de forma

electrónico, documento en Excel)	Información		y a realizar modificaciones en el Cuadro de evaluación de riesgos	permanente
Cuadro de análisis de riesgos (formulario electrónico, documento en Excel)	Ordenador del Oficial de Seguridad de la Información	Oficial de Seguridad de la Información	Solamente el Oficial de Seguridad de la Información tiene derecho a crear entradas y a realizar modificaciones en el Cuadro de evaluación de riesgos	Los datos son archivados de forma permanente
Cuadro de evaluación de riesgos (formulario electrónico, documento en Excel)	Ordenador del Oficial de Seguridad de la Información	Oficial de Seguridad de la Información	Solamente el Oficial de Seguridad de la Información tiene derecho a crear entradas y a realizar modificaciones en el Cuadro de evaluación de riesgos	Los datos son archivados de forma permanente
Cuadro de tratamiento de riesgos (formulario electrónico, documento en Excel)	Ordenador del Oficial de Seguridad de la Información	Oficial de Seguridad de la Información	Solamente el Oficial de Seguridad de la Información tiene derecho a crear entradas y a realizar modificaciones en el Cuadro de tratamiento de riesgos	Los datos son archivados de forma permanente
Informe sobre evaluación y tratamiento de riesgos (formulario electrónico, en formato PDF)	Ordenador del Oficial de Seguridad de la Información	Oficial de Seguridad de la Información	El Informe se prepara en formato PDF de sólo lectura	El informe es almacenado por el plazo de 3 años.
Declaración de aplicabilidad (formulario electrónico, en formato PDF)	Ordenador del Oficial de Seguridad de la Información	Oficial de Seguridad de la Información	Solamente el Oficial de Seguridad de la Información tiene derecho a crear entradas y a realizar modificaciones en la Declaración de	Las versiones no vigentes de la pdf son almacenadas por un plazo de 3 años.

			aplicabilidad	
--	--	--	---------------	--

Solamente el Oficial de Seguridad de la Información puede permitir a otros empleados el acceso a los documentos mencionados precedentemente.

## 10.VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido hasta nueva actualización.

El propietario de este documento es el Oficial de Seguridad de la Información, que debe verificar y, si es necesario, 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.

## 11.ANEXOS

- Anexo 1: Identificación y valoración de activos
- Anexo 2: Cuadro de análisis de riesgos
- Anexo 3: Cuadro de evaluación de riesgos
- Anexo 4: Cuadro de tratamiento de riesgos

## 11.1. ANEXO 1: Identificación y valoración de activos

### IDENTIFICACION Y VALORACION DE ACTIVOS

NOTA: Diligencie solo las celdas que se encuentran sombreadas en color gris claro

Nro. Activo	Proceso Macro	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Intención del Uso	Tipo de soporte	Ubicación	Valoración de Impacto (pérdida)			
									C: Confidencialidad I: Integridad D: Disponibilidad			
									C	I	D	VA
A1												0.00
A2												0.00
A3												0.00
A4												0.00
A5												0.00
A6												0.00
A7												0.00
A8												0.00

## 11.2. ANEXO 2: Cuadro de análisis de riesgos

Análisis de Riesgos					
Proceso Macro	Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad
0	0	A1	0		
0	0	A2	0		
0	0	A3	0		

### 11.3. ANEXO 3: Cuadro de evaluación de riesgos

Evaluación de Riesgos					
Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
CID	Nivel de amenaza	Nivel de vulnerabilidad			
0.00					
0.00					
0.00					
0.00					
0.00					
0.00					
0.00					
0.00					
0.00					

### 11.4. ANEXO 4: 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	Nivel de Riesgo con el control Implementado	