# METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

<table>
<thead>
<tr>
<th>Código:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Versión:</td>
</tr>
<tr>
<td>Fecha de la versión:</td>
</tr>
<tr>
<td>Creado por:</td>
</tr>
<tr>
<td>Aprobado por:</td>
</tr>
<tr>
<td>Nivel de confidencialidad:</td>
</tr>
</tbody>
</table>

Historial de modificaciones

<table>
<thead>
<tr>
<th>Fecha</th>
<th>Versión</th>
<th>Creado por</th>
<th>Descripción de la modificación</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/01/2013</td>
<td>0.1</td>
<td>Dejan Kosutic</td>
<td>Descripción básica del documento</td>
</tr>
</tbody>
</table>

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS .......................................................................................... 3
2. DOCUMENTOS DE REFERENCIA .............................................................................................. 3
3. METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS ........................................... 3
   3.1. EVALUACIÓN DE RIESGOS .............................................................................................. 3
       3.1.1. El proceso ........................................................................................................... 3
       3.1.2. Activos, vulnerabilidades y amenazas ................................................................. 3
       3.1.3. Identificación de los propietarios de riesgos ...................................................... 4
       3.1.4. Consecuencias y probabilidad ............................................................................ 4
   3.2. CRITERIOS PARA LA ACEPTACIÓN DE RIESGOS .......................................................... 4
   3.3. TRATAMIENTO DEL RIESGO .......................................................................................... 4
   3.4. REVISIONES PERIÓDICAS DE LA EVALUACIÓN Y EL TRATAMIENTO DE RIESGOS .......... 5
   3.5. DECLARACIÓN DE APLICABILIDAD Y PLAN DE TRATAMIENTO DEL RIESGO ............... 5
   3.6. INFORMES .................................................................................................................. 5
4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO .................................. 6
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS .............................................................................. 7
6. APÉNDICES ......................................................................................................................... 7
1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en [nombre de la organización] y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La evaluación y tratamiento de riesgos se aplican a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

Los usuarios de este documento son todos los empleados de [nombre de la organización] que participan en la evaluación y tratamiento de riesgos.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos 6.1.2, 6.1.3, 8.2, y 8.3
- Política de Seguridad de la Información
- Lista de requisitos legales, normativos y contractuales y demás requisitos
- Política de seguridad para proveedores
- Declaración de aplicabilidad

3. Metodología de evaluación y tratamiento de riesgos

3.1. Evaluación de riesgos

3.1.1. El proceso

La evaluación de riesgos se implementa a través del Cuadro de evaluación de riesgos. El proceso de realizar los propietarios de los activos, y la evaluación de riesgos es compartida por todos. La evaluación de riesgos es realizada por los propietarios de los riesgos.

3.1.2. Activos, vulnerabilidades y amenazas

El primer paso en la evaluación de riesgos es la identificación de todos los activos dentro del alcance del proceso. Los activos pueden ser productos, servicios, informes, bases de datos, software, aplicaciones, plantas, etc. Los activos deben ser identificados y categorizados en función de su importancia y vulnerabilidad.

El siguiente paso es identificar todas las amenazas y vulnerabilidades relacionadas con cada activo. Las amenazas pueden ser internas o externas, y pueden estar vinculadas a varias vulnerabilidades.
3.1.3. **Identificación de los propietarios de riesgos**

Para cada riesgo es necesario identificar a propietario, la persona o entidad que tenga responsabilidad de cada riesgo. *Esta persona puede o no ser la misma que el propietario del activo.*

3.1.4. **Consecuencias y probabilidad**

Una vez que se han identificado los riesgos, es necesario evaluar las consecuencias para cada combinación de costos y riesgos asociados de un activo específico, en caso que ello se pueda producir:

<table>
<thead>
<tr>
<th>Consecuencia</th>
<th>Consecuencia</th>
<th>Consecuencia</th>
</tr>
</thead>
<tbody>
<tr>
<td>La pérdida de confidencialidad, disponibilidad o integridad de la organización.</td>
<td>La pérdida de confidencialidad, disponibilidad o integridad causa daños materiales o económicos.</td>
<td>La pérdida de confidencialidad, disponibilidad o integridad tiene consecuencias legales o contractuales o sobre el prestigio de la organización.</td>
</tr>
</tbody>
</table>

Luego de la evaluación de consecuencias es necesario evaluar la probabilidad de que un materializado el riesgo. En este caso, la probabilidad de que una amenaza de seguridad de la vulnerabilidad del activo en cuestión.

<table>
<thead>
<tr>
<th>Probabilidad</th>
<th>Probabilidad</th>
<th>Probabilidad</th>
</tr>
</thead>
<tbody>
<tr>
<td>En el futuro no se pueden implementar nuevos.</td>
<td>Las consecuencias legales son menores.</td>
<td>Las consecuencias legales son mayores.</td>
</tr>
</tbody>
</table>

Ingresando los valores de consecuencia y probabilidad en el Cuadro de evaluación de riesgos, el nivel de riesgo se calculará automáticamente con uno de los siguientes métodos. Los criterios de seguridad son menores en la última columna del Cuadro de evaluación de riesgos.

3.2. **Criterios para la aceptación de riesgos**

Los valores 0, 1 y 2 son riesgos aceptables, mientras que los valores 3 y 4 son riesgos no aceptables. Los riesgos no aceptables deben ser tratados.

3.3. **Tratamiento del riesgo**
El tratamiento de riesgos se implementa mediante el Cuadro de tratamiento de riesgos, copiando como no aceptables. El por el [cargo].

Para los riesgos aplicarán en el caso de ser necesario una o más opciones de tratamiento.

1. Eliminación de control o control de seguridad del Anexo A de la norma ISO/IEC 27001 u
   ejemplo, restringiendo una pala de seguridad
   o un proveedores o socios.
2. Transferencia de los riesgos a terceros;
   ejemplo, contratación de una empresa de servicios
   que actualmente no se realizara dicha acción.
3. Evitar los riesgos discontinuando
4. Aceptación del riesgo: esta opción está permitida solamente si la selección de otras
   opciones de tratamiento es costosa, ineficaz o ineficiente

La elección de opciones se implementa a través del Cuadro de tratamiento de riesgos. Generalmente,
se selecciona la opción que involucre en menos riesgos, en la que se realiza en menos tiempo, etc.

En el caso de la opción 1 (elección de controles de seguridad), es necesario evaluar el nuevo valor de
los controles planificados.

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

Los propietarios de riesgos deben revisar los riesgos vigentes y deben actualizar el Cuadro de
tratamiento de riesgos. Los propietarios de riesgos deben revisar, actualizar y revisar de manera
periodica el Cuadro de Tratamiento de Riesgos. Los propietarios de riesgos, en el entorno empresarial, etc.

3.5. Declaración de aplicabilidad y Plan de tratamiento del riesgo

El [cargo] debe documentar los siguiente en la Declaración de aplicabilidad: qué controles de
aplicabilidad se consideran; pueden aplicables y no; la justificación de esa
decisión y si están implementados o no.

En nombre de los propietarios de riesgos, la alta dirección aceptará todos los riesgos residuales si
a través de la Declaración de aplicabilidad.

El [cargo] preparará el Plan de tratamiento de riesgos en el que se planificará la implementación de
Plan de tratamiento de riesgos.

3.6. Informes
El [cargo] documentará los resultados de la evaluación y del tratamiento de riesgos, y de todos los informes de evaluación y tratamiento de riesgos.

El [cargo] supervisará el progreso de la Plan de tratamiento de riesgos e informará los resultados [cargo] mensualmente.

4. Gestión de registros guardados en base a este documento

<table>
<thead>
<tr>
<th>Nombre del registro</th>
<th>Ubicación de archivo</th>
<th>Persona responsable del archivo</th>
<th>Controles para la protección del registro</th>
<th>Tiempo de retención</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cuadro de evaluación de riesgos (formulario electrónico, documento en Excel)</td>
<td>Ordenador del [cargo]</td>
<td>[cargo del propietario del Cuadro de evaluación de riesgos]</td>
<td>Solamente el [cargo] tiene derecho a crear entradas y a realizar modificaciones en el Cuadro de evaluación de riesgos</td>
<td>Los datos son archivados de forma permanente</td>
</tr>
<tr>
<td>Cuadro de tratamiento de riesgos (formulario electrónico, documento en Excel)</td>
<td>Ordenador del [cargo]</td>
<td>[cargo del propietario del Cuadro de tratamiento de riesgos]</td>
<td>Solamente el [cargo] tiene derecho a crear entradas y a realizar modificaciones en el Cuadro de tratamiento de riesgos</td>
<td>Los datos son archivados de forma permanente</td>
</tr>
<tr>
<td>Informe sobre evaluación y tratamiento de riesgos (formulario electrónico, en formato PDF)</td>
<td>Ordenador del [cargo]</td>
<td>[cargo del propietario del Informe]</td>
<td>El Informe se prepara en formato PDF de sólo lectura</td>
<td>El informe es almacenado por el plazo de 3 años.</td>
</tr>
<tr>
<td>Declaración de aplicabilidad (formulario electrónico, en formato PDF)</td>
<td>Ordenador del [cargo]</td>
<td>[cargo del propietario del Informe]</td>
<td>Solamente el [cargo] tiene derecho a crear entradas y a realizar modificaciones en la Declaración de aplicabilidad</td>
<td>Las versiones no vigentes de la DdA son almacenadas por un plazo de 3 años.</td>
</tr>
<tr>
<td>Plan de tratamiento de riesgos (formulario electrónico, documento de</td>
<td>Ordenador del [cargo]</td>
<td>[cargo de la persona responsable del Plan de tratamiento de</td>
<td>Solamente el [cargo] tiene derecho a crear entradas y a realizar modificaciones en el Plan de tratamiento de riesgos</td>
<td>Las versiones no vigentes del Plan de tratamiento de riesgos</td>
</tr>
</tbody>
</table>

Comment [DK11]: Esto es sólo una recomendación; ajustar la frecuencia según sea necesario.

Comment [DK12]: En esta columna ingrese datos que reflejen sus necesidades reales.
Solamente el [cargo] puede permitir [otro espacio de texto, acces cuenta con [nombre] de [organización] mencionados]

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargo], que debe verificar y, si es necesario, actualizar el documento por lo menos [una vez al año], en función del proceso periódico 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 riesgos que se identificaron pero que no fueron incluidos en la evaluación de riesgos.
- La cantidad de riesgos que no fueron tratados adecuadamente.
- La cantidad de riesgos en el proceso de evaluación y tratamiento de riesgos debido a [otro espacio de texto, acces cuenta con [nombre] de [organización] definiciones poco claras de funciones y responsabilidades].

6. Apéndices

- Apéndice 1: Formulario - Cuadro de evaluación de riesgos
- Apéndice 2: Formulario - Cuadro de tratamiento de riesgos
- Apéndice 3: Formulario - Informe sobre evaluación y tratamiento de riesgos

[cargo]
[nombre]

[firma]