|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
| Documento de Identificación, Evaluación y Resultados del Análisis de Riesgos |  | **MAAGTICSI** |

|  |  |
| --- | --- |
| Documento en el cual se realizará un registro, evaluación, así como la presentación de resultados del Análisis de Riesgos. | **Proyecto:**  **ID:** |

**CONTENIDO**

[1. Objetivo del Documento 2](#_Toc394417113)

[2. Abreviaturas y definiciones 3](#_Toc394417114)

[3. Referencias 3](#_Toc394417115)

[4. Objetivo de la evaluación 4](#_Toc394417116)

[5. Alcance de la evaluación 4](#_Toc394417117)

[Tabla 1. Probabilidad de ocurrencia 4](#_Toc394417118)

[Tabla 2. Nivel de impacto 4](#_Toc394417119)

[Tabla 3. Existencia del agente amenaza para el cálculo de P. 5](#_Toc394417120)

[Tabla 4. Niveles de Interés del agente amenaza para el cálculo de P. 6](#_Toc394417121)

[Tabla 5. Capacidad del agente amenaza para el cálculo de P. 6](#_Toc394417122)

[Tabla 6 Vulnerabilidad del Activo de información para el cálculo de P. 6](#_Toc394417123)

[Tabla 7. Nivel de impacto para el cálculo de R. 7](#_Toc394417124)

[6. Tabla de Análisis y Determinación de Riesgos 9](#_Toc394417125)

[Tabla 8. Matriz de riesgos. 10](#_Toc394417126)

[7. ESTRATEGIAS: 11](#_Toc394417127)

[8. Tabla de Evaluación de Riesgos 13](#_Toc394417128)

[9. Riesgos Residuales 13](#_Toc394417129)

[10. Riesgos aceptados 14](#_Toc394417130)

[11. Bitácora de Control de Cambios 14](#_Toc394417131)

# Objetivo del Documento

*[Esta fase tiene el propósito de proporcionar una relación de todas aquellas amenazas posibles, las que en caso de materializarse, tendrían efectos negativos sobre la seguridad en uno o varios de los activos de información identificados en factores críticos anteriores.]*

# Abreviaturas y definiciones

|  |  |
| --- | --- |
| **Abreviación o definición** | **Descripción** |
|  |  |
|  |  |
|  |  |

# Referencias

|  |  |
| --- | --- |
| **Nombre del documento** | **Descripción del documento** |
| *[Nombre del o los documentos a los que se hace referencia a lo largo del llenado de este formato].* | *[Escriba una breve descripción del documento, así como su ubicación física o lógica].* |
|  |  |
|  |  |

# Objetivo de la evaluación

*[Efectuar los cálculos necesarios que permiten establecer el valor relativo del riesgo para cada escenario planteado, de acuerdo a la secuencia que se define en el presente formato.]*

# Alcance de la evaluación

*[Los Departamento de la STIC del INR:*

* *Enlistar Deptos.]*

Para determinar el valor de “P” e “I”, se deben utilizar tres valores en cada una de las siguientes tablas:

## Tabla 1. Probabilidad de ocurrencia

|  |  |  |
| --- | --- | --- |
| **Valor** | **Probabilidad de ocurrencia de la amenaza** | **Homologación al Manual de Control Interno** |
| 0.9 | Alta | 6-10 |
| 0.5 | Media | 2-5 |
| 0.1 | Baja | 1 |

## Tabla 2. Nivel de impacto

|  |  |
| --- | --- |
| **Valor** | **Impacto** |
| 100 | Alto |
| 50 | Medio |
| 10 | Bajo |

Utilizando la fórmula y las tablas antes mostradas, se está en posibilidad de determinar el valor del riesgo de una forma sencilla, pueden aplicarse dos estrategias para obtener mayor precisión en los valores de riesgo que se calculen:

* Incluir factores adicionales que ejercen influencia en la probabilidad de ocurrencia, e
* Incrementar la cantidad de valores a considerar para las ponderaciones en las tablas.

Con base en lo anterior, la fórmula que se establece como: P=(e+i+c+v)/4

Donde:

“P”.- Probabilidad de ocurrencia.

“e”.- Existencia de un agente amenaza desde la perspectiva de un activo de información particular (existir).

“i”.- Interés del agente amenaza para atacar al activo de información (querer).

“c”.- Capacidad del agente amenaza para atacar al activo de información (poder).

“v”.- Vulnerabilidad del activo de información.

Nota: Cada variable e, i, c y v influye **en igual proporción**.

Considerando la Nota anterior, este modelo permite realizar estimaciones básicas de los escenarios, utilizando inicialmente un criterio conservador. A medida que éste se utilice, puede ajustar el modelo, con base en los resultados que se obtengan de su aplicación y constante evaluación.

Para la ponderación de los valores requeridos en esta fórmula, se propone el uso de las tablas siguientes:

## Tabla 3. Existencia del agente amenaza para el cálculo de P.

|  |  |
| --- | --- |
| **Valor** | **Probabilidad de existencia del agente amenaza** |
| 0.9 | Es casi seguro que existe |
| 0.7 | Es muy posible que exista |
| 0.5 | Es probable que exista |
| 0.3 | Es poco probable que exista |
| 0.1 | Es casi imposible que exista |

## Tabla 4. Niveles de Interés del agente amenaza para el cálculo de P.

|  |  |
| --- | --- |
| **Valor** | **Nivel de interés del agente amenaza** |
| 0.9 | El interés es incontrolable |
| 0.7 | Se genera mucho interés |
| 0.5 | Se genera regular interés |
| 0.3 | Se genera poco interés |
| 0.1 | Casi no se genera interés |

## Tabla 5. Capacidad del agente amenaza para el cálculo de P.

|  |  |
| --- | --- |
| **Valor** | **Nivel de capacidad del agente amenaza** |
| 0.9 | Los recursos son superiores |
| 0.7 | Cuenta con muchos recursos |
| 0.5 | Los recursos son regulares |
| 0.3 | Cuenta con muy pocos recursos |
| 0.1 | Los recursos son casi nulos |

## Tabla 6 Vulnerabilidad del Activo de información para el cálculo de P.

|  |  |
| --- | --- |
| **Valor** | **Vulnerabilidad del activo de información** |
| 0.9 | Sin ningún tipo de protección |
| 0.7 | Muy poca protección |
| 0.5 | Medianamente protegido |
| 0.3 | Protección normal |
| 0.1 | Protección reforzada |

Una vez que se ha visto como obtener el valor de “P”, debe obtenerse el valor del impacto (I), refiriéndose a la Tabla 7 (los valores de esta tabla pueden ser modificados de acuerdo a las necesidades de cada Institución).

## Tabla 7. Nivel de impacto para el cálculo de R.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Impacto** | **Humano** | **Material** | **Financiero** | **Operativo** | **Imagen** |
| 10 | Desastroso | Muertes | Pérdidas graves no recuperables | Más de $1,000,000.00 | Afectación de procesos críticos que no pueden restablecerse en menos de dos días | Difusión a nivel internacional |
| 8 | Gran impacto | Heridos | Pérdidas graves recuperables a largo plazo | Entre $100,000.00 y $1,000,000.00 | Afectación de procesos críticos, que pueden restablecerse en menos de dos días | Difusión a nivel nacional |
| 6 | Regular impacto | Lesiones que producen una incapacidad | Pérdidas leves no recuperables | Entre $50,000.00 y $100,000.00 | Afectación de varios procesos no críticos | Difusión a nivel local |
| 4 | Mínimo impacto | Lesiones leves | Pérdidas leves recuperables | Entre $10,000.00 y $50,000.00 | Afectación de un proceso no crítico | Difusión dentro de la dependencia o entidad |
| 2 | Insignificante | Sin lesiones | Sin pérdidas materiales | Menor de $10,000.00 | Sin afectación de procesos | Difusión dentro de la unidad |

Una vez evaluado cada uno de los cincos tipos de impacto, únicamente se utilizará el valor más alto que se haya obtenido, a fin de sustituirlo en la fórmula principal R= PI.

De esta manera, se tiene la certeza de que se han considerado los posibles impactos desde diferentes perspectivas y no únicamente con base en las primeras impresiones (fenómeno que tiende a presentarse cuando se realizan tareas mentales repetitivas, como lo es en este caso, la ponderación del impacto para una gran cantidad de amenazas).

Es importante resaltar que el cálculo de P con base en los cuatro factores (e, i, c y v), solo se aplica para aquellos casos en que participe el elemento humano como agente perpetrador. En otros casos no se considera el interés (i). Así, al tratarse de amenazas naturales (medio ambiente), o materiales (incendio), la fórmula a emplearse se reduce a la siguiente: P= (e+c+v)/3

El análisis y determinación de riesgos, se resume como la realización de dos actividades primordiales: el establecimiento de los escenarios de riesgo (cada uno de los activos de información se relaciona con cada amenaza y su respectivo agente), mediante la “Tabla de Análisis y Determinación de Riesgos” mostrada a continuación; y el consenso de valores asignados a cada factor, se sugiere el empleo del método "Delphi". Todo ello para poder finalmente calcular el valor relativo del riesgo.

# Tabla de Análisis y Determinación de Riesgos

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Código**  *[Codificar cada escenario de riesgo (R-1, R-2, Etc.)]* | **Amenaza**  *[Anotar el número de referencia de la primera amenaza]* | **Activo**  *[Anotar el número de referencia del primer activo afectado por la amenaza]* | **e**  *[Anotar el valor resultante de la ponderación de la Tabla 3]* | **i**  *[Anotar el valor resultante de la ponderación de la Tabla 4]* | **c**  *[Anotar el valor resultante de la ponderación de la Tabla 5]* | **v**  *[Anotar el valor resultante de la ponderación de la Tabla 6]* | **P**  *[Anotar el valor resultante de la media aritmética de los valores "e", "i", "c" y "v"]* | **ih**  *[Anotar el valor resultante de la ponderación de la tercera columna de la Tabla 7]* | **im**  *[Anotar el valor resultante de la ponderación de la cuarta columna de la Tabla 7]* | **if**  *[Anotar el valor resultante de la ponderación de la quinta columna de la Tabla 7]* | **io**  *[Anotar el valor resultante de la ponderación de la sexta columna de la Tabla 7]* | **ii**  *[Anotar el valor resultante de la ponderación de la séptima columna de la Tabla 7]* | **I**  *[Anotar el valor mas alto que se haya obtenido de las columnas "ih", "im", "if, "io" e "ii"]* | **R**  *[Anotar el valor resultante delproduto de "P" por "I"]* |
| R-1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| R-2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| R-3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| R-4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| R-5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| R-6 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| : |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| R-n |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

*e: existencia de agente amenaza im: impacto material*

*i: interés del agente amenaza if: impacto financiero*

*c: capacidad del agente amenaza io: impacto operativo Deberá:*

*v: vulnerabilidades del activo de información ii: impacto de imagen 1. En la columna P anotar el resultado de (e+i+c+v)/4.*

*P: probabilidad de ocurrencia I: impacto 2. En la columna I anotar el valor MAS ALTO de entre las columnas ih, im, if, io, ii.*

*ih: impacto humano R: riesgo 3. En la columna R anotar el valor de PI.*

Una vez que se cuenta con los valores de cada uno de los riesgos correspondientes a los diversos escenarios planteados, se debe proporcionar la siguiente información, que será requerida para soportar la posterior toma de decisiones:

* La relación de riesgos que no requieren ser atendidos.
* La relación de riesgos que si tienen que ser atendidos.
* El orden de prioridad para los riesgos que serán atendidos.
* La estrategia de seguridad a seguir.
* La relación de controles propuestos.

El criterio de aceptación para diferenciar los riesgos que requieren ser atendidos, de aquellos que pueden ser aceptados, se basa en el valor máximo que puede tener un riesgo cuyo impacto se ha ponderado como insignificante; esto es, la dependencia está dispuesta a asumir todos aquellos riesgos cuyo impacto ha sido evaluado con el mínimo valor, durante el análisis y determinación de riesgos.

Al representar mediante una matriz los diversos valores de riesgo posibles (Tabla 8), es posible observar que el máximo valor de un riesgo que ha sido ponderado como insignificante, es **1.8**. Este valor delimita entonces el rango de riesgos aceptables, por lo que todos aquellos riesgos cuyo valor sea igual o menor a **1.8**, no requieren de llevar a cabo acción alguna por parte de la dependencia o entidad.

## Tabla 8. Matriz de riesgos.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Probabilidad de Ocurrencia** | | | | | | |
| 0.9 | **Casi Seguro** | 1.8 | 3.6 | 6.4 | 7.2 | 9 |
| 0.7 | **Alta** | 1.4 | 2.8 | 4.2 | 5.6 | 7 |
| 0.5 | **Mediana** | 1 | 2 | 3 | 4 | 5 |
| 0.3 | **Baja** | 0.6 | 1.2 | 1.8 | 2.4 | 3 |
| 0.1 | **Casi imposible** | 0.2 | 0.4 | 0.6 | 0.8 | 1 |
|  |  | **Insignificante** | **Significativo** | **Grave** | **Crítico** | **Desastroso** |
|  |  | 2 | 4 | 6 | 8 | 10 |
|  | **IMPACTO** | | | | | |

Por otra parte, aquellos riesgos cuyo valor sea mayor a **1.8, si** tienen que ser atendidos, siendo necesario entonces establecer un nivel de prioridad para su atención.

El nivel de prioridad de cada riesgo está basado en su valor relativo, esto es, al escenario de riesgo cuyo valor relativo es el más alto, le corresponde la prioridad de 1, al riesgo con el segundo valor más alto, le corresponde la prioridad 2 y así sucesivamente hasta completar todos los escenarios.

Una vez establecidas las prioridades, el siguiente paso es determinar la estrategia de seguridad a seguir para enfrentar el riesgo. Para ello, se consideran 5 distintas alternativas: evitar, prevenir, mitigar, financiar o asumir. Estas estrategias de seguridad deben evaluarse en el orden en que se han mencionado, ya que como se entenderá durante la descripción de cada una de ellas, los beneficios que representan son mayores para la primera alternativa, disminuyendo hasta ser casi nulos en la última de las estrategias.

# ESTRATEGIAS:

* **Evitar:** Se trata de implementar lo necesario para que la amenaza no se materialice. Esto sólo será posible si de los componentes del escenario de riesgo (causa - evento - consecuencia), es eliminado el único factor no probabilístico sobre el que se tiene control, esto es, el activo de información. De manera que, en este caso, la única manera de evitar que un riesgo ocurra es eliminando la actividad o proceso que, en un particular escenario de riesgo, represente el objeto o blanco de la amenaza. Por ejemplo, consideremos el siguiente escenario:

Amenaza: Modificación

Agente amenaza: Un hacker en la red

Activo de información: Sitio Web de la dependencia o entidad.

En este caso, el riesgo de que una página Web de la organización sea modificada por un hacker, se puede evitar eliminando al agente amenaza, pero esa es una situación fuera de nuestro alcance, por lo que la única forma factible de evitar este riesgo, sería no exponer el activo de información, es decir, no contar con un sitio Web.

Definitivamente, la estrategia de "evitar', representa el extremo en el compromiso entre seguridad y funcionalidad, sin embargo, debe ser considerada al principio de la evaluación con el fin de asegurar que en primera instancia se intentó desaparecer por completo al riesgo. La pregunta a contestar para decidir el empleo de esta alternativa sería: ¿La dependencia o entidad se ve más afectada si se enfrenta a este riesgo, que si se enfrenta a las consecuencias de desactivar este activo de información?

* **Prevenir:** Estrategia que se enfoca en reducir el valor de "**P**” en la ecuación del riesgo. Esto se logra mediante la implementación de controles que ayuden a disminuir la probabilidad de ocurrencia (acciones preventivas), enfocándose para ello en afectar de manera negativa, y sea el interés o capacidad del agente amenaza, o vulnerabilidades de nuestro activo de información. Una forma de facilitar la toma de decisiones respecto a la conveniencia de esta estrategia, es con ayuda de la matriz mostrada en la tabla 8, mediante la cual se puede apreciar en qué magnitud se debe reducir “**P**”, para ubicar al riesgo en una zona de aceptabilidad.
* **Mitigar:** Se trata de una estrategia enfocada en acciones correctivas, ya que los controles a implementarse intentarán reducir el valor de “**I**”' en la ecuación del riesgo. Esta alternativa asume que la amenaza se ha materializado y que los esfuerzos deben encaminarse a una rápida respuesta, para que el impacto sea reducido al mínimo valor posible. Al igual que en la estrategia anterior, la matriz de la tabla 8 permite determinar la magnitud en que “**I**” debe reducirse para que el riesgo sea aceptable. La elección de la estrategia depende entonces, del resultado de la comparación entre las magnitudes en que se requeriría modificar a “**P**” e “**I**”, para que el valor del riesgo sea igual o menor a **1.8**.
* **Aceptar:** Última de las alternativas como estrategia de seguridad, en la cual no se emplea ningún tipo de control cuando se prefiere conservar el riesgo con su valor actual. Esto puede ser ocasionado por las limitantes que sufre la dependencia o entidad ante restricciones económicas, materiales o de personal, siempre y cuando ninguna de las alternativas anteriores satisfaga los mínimos requerimientos de seguridad, o como resultado del análisis costo-beneficio en el que se refleje que es más costoso implementar el control, que soportar el impacto por la materialización de la amenaza.

# Tabla de Evaluación de Riesgos

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Código Escenario** | **P**  *[Anotar los valores de "P", de acuerdo al código de cada escenario (un escenario por fila)]* | **I**  *[Anotar los valores de "I", de acuerdo al código de cada escenario (un escenario por fila)]* | **R**  *[Anotar los valores de "R", de acuerdo al código de cada escenario (un escenario por fila)]* | **Criterio Aceptación**  *[Comparar el valor de "R" con el criterio de aceptación propuesto por esta metodología (1.8)]* | **¿Requiere control?**  *[Anotar que* ***SI*** *se requiere control, cuando el valor de "R" es mayor a 1.8. en caso contrario anotar* ***NO****]* | **Prioridad**  *[Asignar prioridades, únicamente a todos los escenarios que* ***SI*** *requieren control, tomando como referencia el valor de "R" de mayor a menor]* | **Estrategia**  *[Determinar su tipo en términos de “Evitar”, “Prevenir” o “Mitigar”]* | **Controles**  **Propuestos**  *[Mediante técnica de “Tormenta de ideas”, proponer controles y consensuar los mismos en el Grupo para la asignación de valores de efectividad: alto, medio o bajo]* | **Inversión requerida**  *[Indicar de acuerdo a los estudios costo beneficio, cual es la inversión requerida y cuál es la pérdida que se pretende evitar (l$)]* |
| R-1 |  |  |  | 1.8 |  |  |  |  |  |
| R-2 |  |  |  | 1.8 |  |  |  |  |  |
| R-3 |  |  |  | 1.8 |  |  |  |  |  |
| .  .  . |  |  |  | 1.8 |  |  |  |  |  |
| R-6 |  |  |  | 1.8 |  |  |  |  |  |
|  |  |  |  |  |  |  |  | Total | $ |

P: probabilidad de ocurrencia I: impacto R: riesgo

# Riesgos Residuales

|  |  |
| --- | --- |
| **Riesgos residuales**  *[Por cada activo protegido, resumir cual es el riesgo residual que será asumido, explicando la justificación para ello]* | **Requerimientos especiales**  *[Indicar los requerimientos especiales para cada control recomendado]* |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Riesgos aceptados

*[Indicar cuáles son los riesgos aceptados y su justificación.]*

*[Indicar comentarios respecto a apoyos o limitantes ocurridos durante el desarrollo del estudio.]*

*[Indicar comentarios relativos a la metodología que se aplica en los presentes formatos.]*

# Bitácora de Control de Cambios

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Descripción del Cambio** | **Impacto** | **Fecha de evaluación** | **Aprobador** | **Aceptado /Rechazado** | **Fecha de aplicación** |
| Actualización de la imagen institucional | Bajo | JUN 15 | Mtra. Lourdes Zaldívar Martínez | Aceptado | JUN 15 |
| Revisión de contenidos y actualización de encabezados | Bajo | JUN 18 | M. en I. María Isabel Garrido Galindo | Aceptado | JUN 18 |
| Revisión de contenidos y actualización de encabezados | Bajo | DIC 20 | M. en I. María Isabel Garrido Galindo | Aceptado | DIC 20 |