UAE Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales -ITRC

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

SIG

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA AGENCIA ITRC

GENERALIDADES

La gestión de riesgos de seguridad de la información propende por la protección de la información de la Agencia ITRC, con el propósito principal de apoyar el logro de los objetivos misionales y de mantener la continuidad de la operación de la entidad. En este contexto se debe llevar a cabo el análisis de las amenazas y las vulnerabilidades que afecten a los activos de información que apoyen los procesos de la Agencia ITRC establecidos como alcance del análisis, evaluación y tratamiento de riesgos.

El objeto del análisis es proporcionar información que sirva para la evaluación y el posterior tratamiento de riesgos de seguridad de la información. El análisis de riesgos toma en consideración los factores que afectan, las consecuencias (impacto por la pérdida de Confidencialidad, Integridad y Disponibilidad) y la probabilidad (ocurrencia en el tiempo de que una amenaza explote una vulnerabilidad). El riesgo se debe analizar mediante la combinación de cálculos de impactos y probabilidades en el contexto de las medidas de control existentes.

Este análisis de riesgos se debe llevar a cabo para los activos de información valorados de más alto impacto considerando los siguientes aspectos:

- Definición de las amenazas
- Definición de las vulnerabilidades asociadas a cada amenaza
- Análisis de la probabilidad que la amenaza penetre la vulnerabilidad
- Evaluación de riesgos, partiendo de la valoración de cada activo de información (Impacto) y la calificación de probabilidad de materialización del riesgo

- Análisis de los controles del anexo A de la norma ISO 27001 aplicables y calificación de la gestión de dichos controles.
- Ejecución de la evaluación de riesgos, considerando la efectividad de la gestión de los controles existentes
- Establecimiento de Niveles para la Aceptación del Riesgo

Posteriormente se deben identificar las amenazas, que son factores externos y no controlables por la Agencia ITRC, las cuales se constituyen en fuentes de riesgo para los activos de información. Las amenazas pueden ser intencionales o accidentales. Se deben identificar las amenazas para cada activo de información que hace parte del análisis y evaluación de riesgos.

Las vulnerabilidades son las debilidades, brechas de seguridad o situaciones inherentes a los activos de información que pueden ser explotadas por las amenazas. Por cada amenaza identificada, se debe identificar aquellas vulnerabilidades que pueden ser explotadas por ésta.

1. OBJETIVO GENERAL

Programar la Gestión de Riesgos de Seguridad de la Información en el cual se identifiquen las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta desde la perspectiva del entorno cibernético, respecto a los criterios de *Confidencialidad*, *Integridad, y Disponibilidad*, con el fin de implementar un ambiente de control, intensificar la confianza en los usuarios internos y externos.

2. OBJETIVOS ESPECÍFICOS

a. Establecer una metodología para el tratamiento de riesgos de seguridad y privacidad de la información.
b. Orientar y generar cultura dentro de la Agencia ITRC en el tratamiento de riesgos de seguridad digital.
c. Gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad como son Confidencialidad, Integridad, Disponibilidad.
d. Aplicar los lineamientos soportados en los estándares de seguridad de la información fijados por el Ministerio de Tecnologías de la Información y las Comunicaciones.
e. Convertir a la OATI en un facilitador de apropiación de cultura en seguridad de la Información dentro de la entidad.
f. Orientar a la Agencia en la toma de decisiones sobre aspectos relacionados con la seguridad de la información

3. LINEAMIENTOS MARCO

Conscientes de que la *Seguridad Digital* es fundamental para el desarrollo del país, el Gobierno Nacional, se ha puesto a la vanguardia de la lucha contra las amenazas en el ámbito digital definiendo estrategias tales como la creación de lineamientos como la Política para Ciberseguridad y Ciberdefensa (CONPES 3701 y 3854), un modelo de seguridad y privacidad de la información (MSPI) y misiones de asistencia técnica internacional.

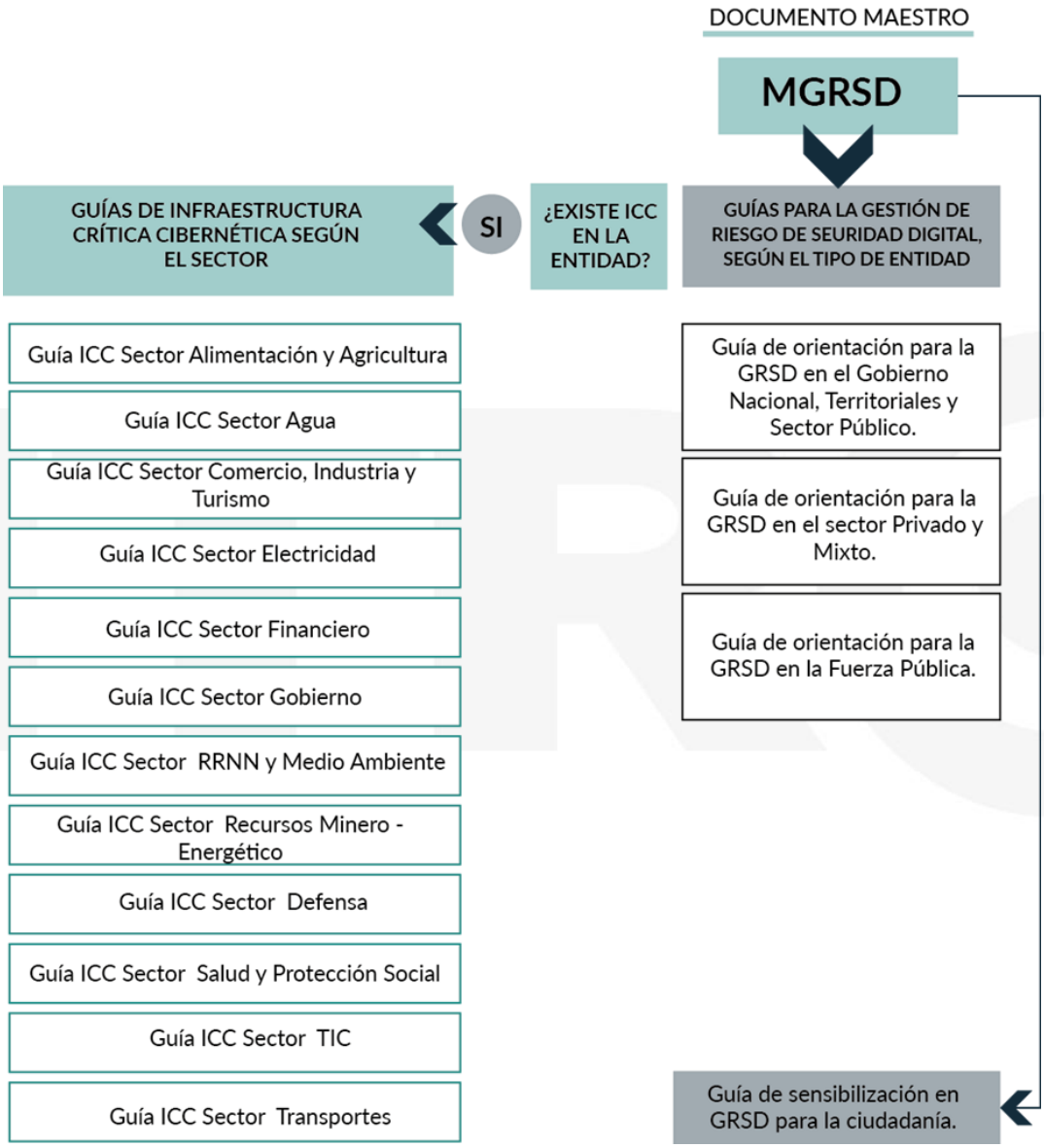
De otra parte, se han creado grupos de trabajo de apoyo transversal de diferentes organizaciones para la prevención y gestión de incidentes, como el MinTIC, Grupo de Respuestas a Emergencias Cibernéticas de Colombia-ColCERT, Equipo de respuesta a incidentes de seguridad informática CSIRT, -Centro Cibernético Policial de la Policía Nacional, entre otros. Como también, mecanismos de investigación (a través de la Fiscalía General de la Nación, Centro Cibernético Policial y de judicialización, Rama Judicial, con las cuales se busca aumentar la capacidad de defensa ante las amenazas presentes en el medio digital.

Así mismo, el Gobierno colombiano ha creado Políticas como el CONPES 3854 de 2016 para la protección del entorno digital y cibernético; en él se involucran a todos los ciudadanos y sectores económicos para fortalecer la prosperidad económica, social y ambiental del país. [1]

Por lo anteriormente mencionado, dentro del Modelo de Seguridad y Privacidad de la información (en adelante MSPI), un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones, y por ello, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión, es importante aprovechar el trabajo adelantado en la identificación de Riesgos de la Agencia ITRC para ser complementados con los Riesgos de Seguridad de la información.

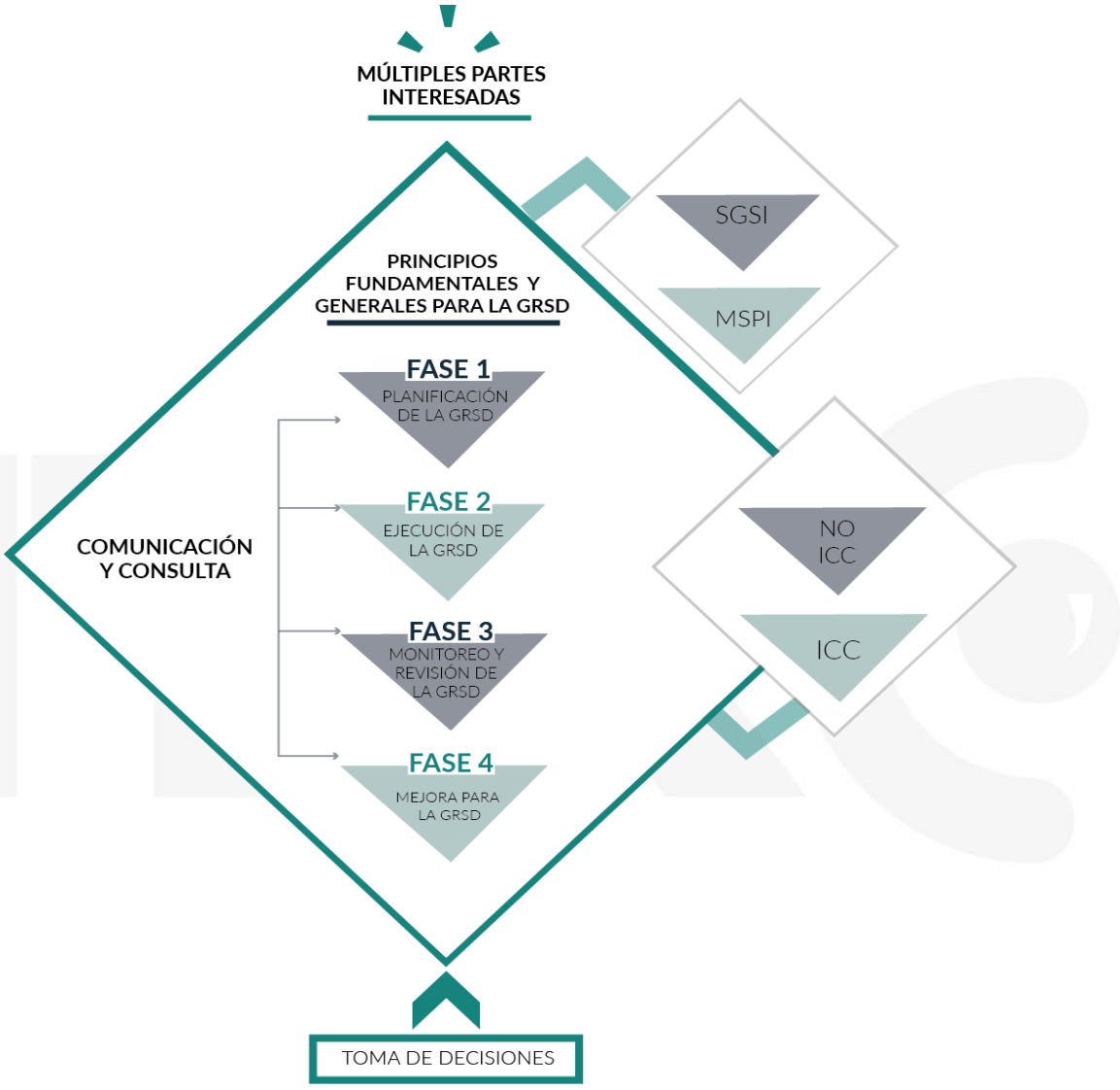
[1] Modelo Nacional de Gestión de Riesgos de Seguridad Digital - MINTIC

No obstante, es importante tomar como referencia el l Modelo Nacional de Gestión de Riesgos de Seguridad Digital el cual se encuentra estructurado de la siguiente forma:



Fuente: Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MINTIC- . Interacción del modelo de gestión del riesgo digital: guías de orientación para la GRSD y guías para el sector ICC.

Bajo este contexto, el Modelo Nacional de Gestión de riesgos de Seguridad Digital establece el siguiente esquema, en donde las entidades del sector público deben acoplarse con base a los lineamientos allí definidos.



Fuente: Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MINTIC- . . Marco conceptual del MGRSD

4. MODELO DE TRATAMIENTO DE RIESGOS DE SEGURIDAD EN LA AGENCIA ITRC

- **ESTRATEGIAS DE TRATAMIENTO DE RIESGOS DE RIESGOS.**

La Oficina de Tecnologías de la Información – OATI de la Agencia ITRC, ha definido dos estrategias principales dentro del modelo de tratamiento de riesgos:

•***Estrategias de Evitación***: consiste en minimizar la probabilidad de que el riesgo se presente. Para ello Se pueden definir cuatro (4) modalidades: transferencia, reducción, elusión y diversificación.

•***Estrategias de Minimización***: consiste en reducir el impacto del riesgo en los activos de información. Estas estrategias son una alternativa cuando las de evitación no son lo suficientemente efectivas, y por tanto, el riesgo pasa a ser un hecho. Para estos casos, es necesario definir un plan de contingencia, que intentará atenuar los efectos negativos del riesgo, una vez éste se ha presentado.

Para las estrategias de ***Evitación*** se dispone de 4 modalidades que se detallan a continuación:

"• ***Transferencia***: representa el conjunto de procedimientos cuyo objetivo es eliminar el riesgo transfiriéndolo de un lugar a otro. Consiste, por ejemplo, en vender un activo dudoso, asegurar una actividad con importantes riesgos, etc.

• ***Reducción***: esta estrategia busca, bien reducir la probabilidad de ocurrencia de un riesgo, bien reducir sus consecuencias, o bien lograr ambos objetivos a la vez. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, arreglos organizacionales, y procedimientos encaminados a reducir la frecuencia o la oportunidad de que ocurra un error. Las consecuencias pueden reducirse asegurando o garantizando que todos los controles se encuentren en el lugar apropiado para minimizar cualquier consecuencia adversa.

• ***Elusión***: existen dos opciones para intentar eludir un riesgo: no proceder con el proyecto o la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad, que logren el mismo resultado y no incorporen el riesgo detectado. El problema de eludir riesgos es que podemos perder oportunidades de negocio, y además, otros riesgos no identificados anualmente, pueden volverse más significativos.

• ***Diversificación***: consiste en intentar extender el riesgo de un área en concreto, a diferentes secciones, con el fin de impedir la pérdida de todo el negocio. Son ejemplos de diversificación orientarse a nuevos mercados y proveedores, diversificar la lista de productos y servicios, etc."[2]

Para las Estrategias de ***Minimización*** "Se aplican cuando los riesgos ya han producido sus efectos, y son, por tanto, una realidad. En este momento, lo único que cabe es tomar medidas correctoras con el fin de minimizar las consecuencias. Estas situaciones producen retrasos en los proyectos, gabinetes de crisis, etc, por lo que no son aconsejables, y sólo deben ser utilizadas como medida de emergencia.

La principal medida que se puede adoptar en estas situaciones, con el fin de paliar los efectos derivados de la realización del riesgo, son los Planes de Contingencia.

Un Plan de Contingencia define los procedimientos y procesos alternativos que se han de acometer en una organización cuando un riesgo deja de serlo para convertirse en realidad, así como las personas implicadas en dichos procedimientos. Se asume, por tanto, que han fallado las estrategias de evitación y monitorización de los riesgos, y sus efectos ya son inevitables.

En tal caso se realiza una activación del Plan de Contingencia que debe cubrir tres actividades principales: coordinar el manejo de la crisis, asegurar la utilización de procesos alternativos que permitan la continuidad del negocio, y resolver el incidente para restituir la normalidad en los procesos y operaciones.

[2] MM La suma de todos. Gestión de Riesgos/Tratamiento. Análisis de Riesgos
http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/5TratamientodelRiesgo(AR)_es.pdf

No hay que olvidar que tan complejo como el paso a contingencia es la vuelta a la normalidad, ya que durante el período transitorio se habrán realizado operaciones que implican que la vuelta a la normalidad no deba realizarse restituyendo las condiciones al punto en que se pasó a contingencia, sino que deberá actualizarse para reflejar los resultados de los procesos alternativos ejecutados durante la crisis. [3]

- **VALORACION DE LA PROBABILIDAD DE OCURRENCIA**

La valoración de la probabilidad de ocurrencia de que una vulnerabilidad se explotada por una amenaza se debe medir en una escala de cinco (5) valores como se muestra en el cuadro a continuación:

PROBABILIDAD	VALOR
Raro	1
Poco probable	2
Probable	3
Muy probable	4
Casi cierto	5

En la Matriz de Riesgos de seguridad se generarán filas Activo-Amenaza- Vulnerabilidad, donde para cada activo de información analizado se deben considerar todas las combinaciones posibles de Amenazas y Vulnerabilidades.

- **CALCULO DEL RIESGO BRUTO**

Para la valoración de impacto de los activos de información y la valoración de que las amenazas exploten las vulnerabilidades se cuenta con escalas de medición de cinco (5) valores, de tal manera que el rango de los niveles de riesgo se encontrará en valores comprendidos entre 1 y 25.

[3] MM La suma de todos. Gestión de Riesgos/Tratamiento. Análisis de Riesgos http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/5TratamientodelRiesgo(AR)_es.pdf

La valoración del Riesgo Bruto se calculará partiendo de la valoración de impacto de cada activo de información, es decir el impacto por la pérdida de Confidencialidad, Integridad y Disponibilidad y, de la valoración de la probabilidad de que una amenaza explote una vulnerabilidad como se muestra a continuación:

RIESGO BRUTO = IMPACTO ACTIVO X PROBABILIDAD DE OCURRENCIA

Los valores de Riesgo Bruto deben ser calculados sin tener en cuenta los controles que hayan sido implantados por la entidad ni la efectividad de dichos controles.

- **IDENTIFICACION Y EVALUACIÓN DE LA GESTIÓN DE CONTROLES APLICABLES DEL ANEXO A DE LA NORMA ISO 27001**

Una vez identificados todos aquellos controles del Anexo A de la norma ISO/IEC 27001 que resultan aplicables por cada Vulnerabilidad asociada a un activo de información, se debe realizar la calificación de la gestión de dichos controles, para lo cual se requiere valorar su efectividad en una escala de cinco (5) valores los cuales se mencionan a continuación:

ESTADO	CRITERIO	VALOR
No implantado	No existen controles; es posible que se haya identificado su carencia, pero no se han implantado.	1
Inicial	Los controles están implantados, pero no han sido estandarizados. No están documentados y no dejan evidencia.	2
Repetible	Los controles están implantados de manera estandarizada y dejan evidencia, pero no están documentados.	3
Definido	Los controles están implantados de manera estandarizada, se encuentran documentados, se han difundido y dejan evidencia. No se encuentran en un proceso de mejora continua.	4
Administrado	Es posible monitorear y medir el cumplimiento de los controles y tomar medidas cuando no estén trabajando de forma efectiva. Los controles se encuentran en un proceso de mejora continua proporcionan buenas prácticas y, pueden hacer parte de un Sistema de Gestión.	5

Posteriormente, se debe obtener un promedio de calificación para dichos controles aplicables a cada Vulnerabilidad asociada a un activo de información, con el objetivo de obtener un único valor de calificación de la gestión de los controles implantados.

CALIFICACIÓN DE CONTROLES = (CONTROL 1 + CONTROL 2 + ... + CONTROL N) / N (NUMERO DE CONTROLES)

- **CALCULO DEL RIESGO RESIDUAL**

El Riesgo Residual corresponde a la necesidad real de implantación de controles, teniendo en cuenta la valoración de los riesgos identificados previamente y la efectividad de la gestión de los controles existentes.

Para hallar el valor del Riesgo Residual se debe tomar el valor del riesgo bruto y se debe restar el valor obtenido como calificación de la gestión de los controles aplicables.

RIESGO RESIDUAL = RIESGO BRUTO - CALIFICACION DE CONTROLES

- **DEFINICION DE LOS NIVELES DE ACEPTACIÓN DEL RIESGO**

La aceptación del riesgo está determinada por el nivel que la U.A.E Agencia ITRC esté dispuesta a asumir y que no genere ningún efecto adverso en su operación. Dicho criterio se fundamenta en la aplicación de controles a los riesgos brutos con los cuales se generan los riesgos residuales. La escala de los Niveles de Aceptación del Riesgo está determinada por Zonas de Riesgo que la U.A.E Agencia ITRC establezca. A continuación, se presentan dos ejemplos de Niveles de Aceptación del Riesgo:

PROBABILIDAD	NIVEL DE IMPACTO				
	1. Mínimo	2. Bajo	3. Moderado	4. Alto	5. Critico
1. Raro	B	B	B	M	M
2. Improbable	B	M	M	M	A
3. Probable	B	M	A	A	E
4. Muy probable	M	M	A	E	E
5. Casi cierto	M	A	E	E	E

Ejemplo 1: Matriz de 4 Zonas de Riesgo

Zonas de Riesgo:

Ejemplo 2: Matriz de 3 Zonas de Riesgo

PROBABILIDAD	NIVEL DE IMPACTO				
	1. Mínimo	2. Bajo	3. Moderado	4. Alto	5. Crítico
1. Raro	A	A	A	A	T
2. Poco probable	A	A	T	T	T
3. Probable	A	T	T	T	T
4. Muy probable	A	T	T	I	I
5. Casi cierto	T	T	T	I	I

VERDE	Zona de riesgo **B**ajo (1 <= VR <= 3)
AMARILLO	Zona de riesgo **M**edio (4 <= VR <= 8)
NARANJA	Zona de riesgo **A**lto (9 <= VR <= 12)
ROJO	Zona de riesgo **E**xtremo (13 <= VRB <= 25)

VERDE	Zona de riesgo **A**ceptable (1<= VR <= 4)
AMARILLO	Zona de riesgo **T**olerable (5<= VR <= 15)
ROJO	Zona de riesgo **I**ntolerable (16<= VR <= 25)

Zonas de Riesgo:

La evaluación de riesgos se realizará usando los niveles de aceptación de riesgo del ejemplo número 2 del presente documento, debido a que fueron los niveles de aceptación de riesgo seleccionados para el desarrollo del análisis de riesgos; considerando las zonas de riesgo definidas, la evaluación de riesgos pretende separar los riesgos Aceptables de los Tolerables e Intolerables, de tal forma que se obtenga una lista priorizada de riesgos para tomar acciones posteriores. Al final de esta fase se debe generar un mapa de riesgos que contemple los activos de información, sus amenazas, vulnerabilidades, impactos, probabilidades, riesgos brutos, controles y su calificación de gestión, riesgos residuales y niveles de aceptación del riesgo.

A partir de lo anterior se formula el plan de tratamiento de riesgos que busca mitigar efectivamente los riesgos, considerando los activos de información, las vulnerabilidades y los niveles de riesgo obtenidos para los activos de información de la U.A.E. Agencia ITRC en el análisis de riesgos de seguridad de la información. En el tratamiento del riesgo se deben considerar las siguientes etapas:

- Identificar las opciones de tratamiento
- Evaluar las opciones de tratamiento.
- Seleccionar las opciones de tratamiento.
- Preparar planes de tratamiento de riesgos de seguridad.

El plan de tratamiento de riesgos de seguridad de la información se debe plantear en términos de los controles de la norma ISO 27001 y del manual de buenas prácticas de la norma ISO 27002.

1. **Identificación de las opciones de tratamiento del riesgo**

El plan de tratamiento de riesgos de seguridad de la información debe considerar las posibilidades de aceptar, evitar, transferir, compartir o reducir (eliminando o minimizando vulnerabilidades asociadas a los activos de información) el riesgo identificado, teniendo en cuenta la selección de controles específicos para llevar dicho riesgo a un nivel aceptable. Las siguientes son las descripciones de las opciones de tratamiento del riesgo:

- Aceptar: Describe la convivencia con el riesgo si éste llegara a materializarse. Esta situación se presenta cuando el riesgo, a pesar de existir, se encuentra controlado o no genera impacto alguno para el activo de información.
- Evitar: Describe las acciones encaminadas a prevenir la materialización del riesgo.
- Compartir o Transferir: Describe la reducción del riesgo a través del traslado de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.
- Reducir: Esta acción va encaminada a reducir la probabilidad de ocurrencia del riesgo, eliminando o minimizando las vulnerabilidades asociadas a los activos de información.

2. **Generación del plan de tratamiento del riesgo**

Para cada control seleccionado durante el análisis y evaluación de riesgos, teniendo en cuenta todos los Niveles de Aceptación de Riesgo en los cuales es aplicable el control, se debe definir la opción de tratamiento de riesgo para el Nivel de Aceptación de Riesgo de mayor criticidad y una guía de tratamiento para el mismo, la cual comprende las acciones y recomendaciones a llevar a cabo para la implantación o mejora de la efectividad del control.

En este plan se deberán definir las acciones para reducir los riesgos e implantar los controles requeridos para proteger los activos de información.

Ejemplo:

CONTROL	
A.10.10.2 Monitoreo del uso del sistema	
NIVELES DE RIESGO RESIDUAL	**ACCION DE TRATAMIENTO**
	REDUCIR
INTOLERABLE	
GUIA	
Realizar un monitoreo periódico sobre los registros (logs) de auditoria, con el objetivo de identificar alarmas o eventos anómalos que se estén presentando en los componentes de la plataforma tecnológica y generar un procedimiento o guia para este fin.	

Para la elaboración del plan de tratamiento de riesgos, se deben tener en cuenta las vulnerabilidades con mayor nivel de riesgo residual que se mencionarán a continuación:

- Ausencia de control de cambios
- Ausencia de controles de acceso lógico
- Ausencia de controles de auditoria y monitoreo
- Ausencia de UPS y/o planta eléctrica
- Condiciones ambientales inadecuadas
- Configuraciones estándar
- Mantenimiento insuficiente
- Planes de contingencia inexistentes
- Susceptibilidad a las variaciones de voltaje