



Título del Proyecto



Nombre del
logotipo

Reporte Situacional organizacional

Nombre de la organización:

Dirección de la organización:

Geolocalización de lo evaluado:

Fecha de informe:

Preparado por:

Confidencial, uso exclusivo del cliente, etc.

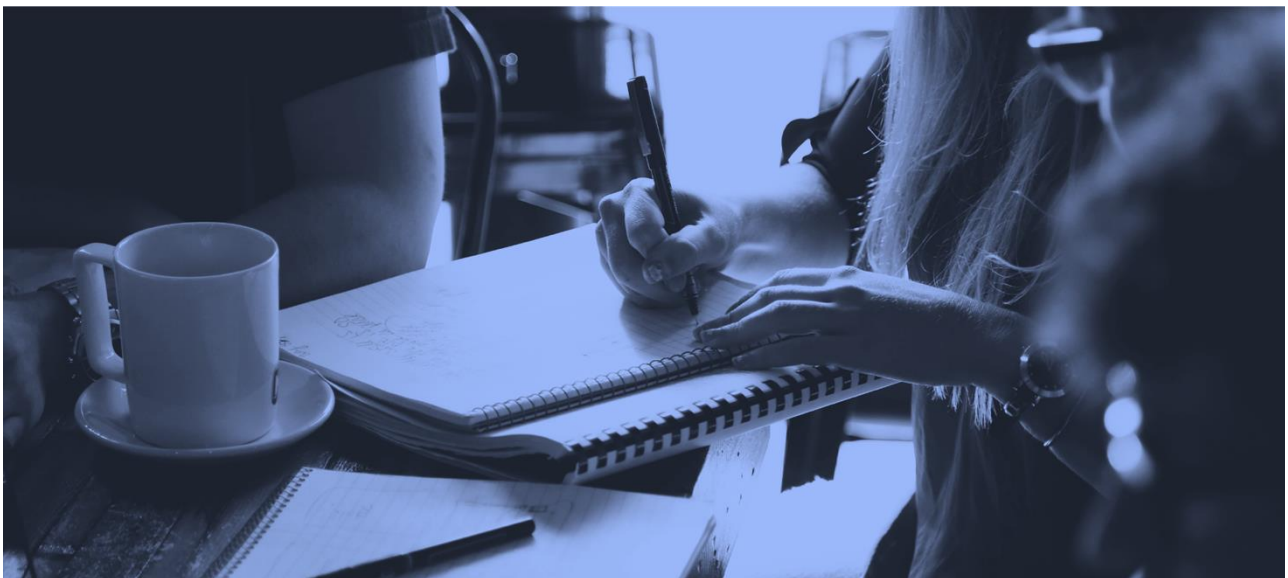
CONTENIDO

Escriba el título de capítulo (nivel 1)	1
Escriba el título de capítulo (nivel 2)	2
Escriba el título de capítulo (nivel 3)	3
Escriba el título de capítulo (nivel 1)	4
Escriba el título de capítulo (nivel 2)	5
Escriba el título de capítulo (nivel 3)	6

Resumen ejecutivo

El resumen ejecutivo debe ofrecer una visión general rápida y efectiva de los hallazgos y recomendaciones clave del reporte. generalmente de 1-2 páginas, diseñada para proporcionar a los lectores una visión rápida de los puntos más importantes del reporte:

- **Descripción General del Entorno de Seguridad:** Resumen de la situación actual en el alcance evaluado.
- **Hallazgos Clave:** Puntos críticos que necesitan atención inmediata, resumen de alto nivel de amenazas y vulnerabilidades identificadas.
- **Acciones Clave Para Implementar:** Un listado de las acciones más urgentes que la organización debe llevar a cabo.
- **Pasos Siguientes:** Recomendaciones sobre las etapas futuras del proceso, incluyendo reevaluaciones o implementación de nuevas medidas.



Metodología

Describe cómo se recopila, analiza y presenta la información para evaluar la probabilidad de riesgo en un país o región. Esta explicación permite a las partes interesadas comprender la base sobre la cual se han realizado las evaluaciones y se han determinado las recomendaciones:

- **Propósito:** Explicar que el objetivo de la metodología es evaluar de manera sistemática y objetiva las vulnerabilidades y amenazas que afectan la seguridad en un país o región durante un periodo específico.
Alcance: Detallar el alcance del análisis, y los mecanismos para evaluar las vulnerabilidades y para identificar y medir las amenazas.
Criterios de Evaluación: Explicar los criterios específicos utilizados para evaluar cada área de vulnerabilidad y amenaza.
- **Limitaciones y Exclusiones:** Aquí se enumeran los supuestos, limitaciones y exclusiones que fueron considerados durante la elaboración del reporte y que pueden afectar el alcance, las interpretaciones y los hallazgos. Es importante que esta sección sea detallada para evitar malentendidos o expectativas irreales por parte del cliente.
- **Referencias:** Cualquier documento, estándar o guía usada como referencia durante la evaluación debe citarse aquí. Esto puede incluir, por ejemplo, el estándar de apreciación de riesgos de seguridad de ASIS o cualquier otro marco normativo relevante.
- **Asignación de Puntuaciones:** Explicar cómo se asignan las puntuaciones a cada criterio evaluado.
- **Promedio de Puntuaciones:** Describir cómo se calculan los promedios de las puntuaciones para cada categoría (vulnerabilidades y amenazas) y cómo estos promedios se utilizan para determinar un puntaje global que representa la probabilidad de riesgo en el país o región.
- **Descriptor de Probabilidad:** Explicar cómo los resultados de la evaluación se interpretan para clasificar el nivel de probabilidad de riesgo. Esta clasificación ayuda a semaforizar y priorizar las áreas más críticas que requieren intervención inmediata o monitoreo continuo.
- **Contextualización:** Detallar cómo se contextualizan los resultados dentro del panorama general del país. Esto incluye cómo las puntuaciones reflejan la situación actual y cómo podrían evolucionar según cambios en el entorno político, económico, o social.

IDENTIFICACIÓN DE RIESGOS

Esta parte del reporte detalla el proceso de categorización de perfiles.

- **Análisis de Vulnerabilidades y Capacidades del EPP:** Identificación de las vulnerabilidades internas y externas, así como las capacidades de la organización para mitigarlas.
- **Narrativa sobre los perfiles identificados:** Descripción de la categorización de los perfiles de ejecutivos
- **Análisis de criticidad:** Evaluación de la severidad potencial de los riesgos a perfiles en la organización.

ANÁLISIS DE RIESGOS

El reporte explica el proceso desde lo particular a lo general, utilizado para analizar y priorizar los perfiles de ejecutivos.

Análisis de Brechas:

- Análisis de oportunidades de mejora en el EPP
- Tolerancia al riesgo de la organización, determinación de los criterios de riesgo, umbral máximo y nivel aceptable de riesgo.
 - a) Identificación de las medidas organizacionales ya implementadas.
- Comparación de mitigaciones existentes y su efectividad frente a los niveles de tolerancia al riesgo.

Riesgo para cada perfil de ejecutivos

- Análisis de probabilidad:
- Vulnerabilidad en el EPP
- Amenaza hacia cada perfil de ejecutivos
- Análisis de criticidad por perfil

Evaluación de perfiles

- a) Priorización de perfiles según su nivel de riesgo

Identificación de los perfiles por encima de la tolerancia:

- Los perfiles que superan los niveles aceptables para la organización y que deben ser registrados para análisis adicionales.

EVALUACIÓN DE RIESGOS

El reporte situacional puede comunicar resultados cualitativos, aunque son los resultados cuantitativos los que generan mayor impacto al tratar con gerentes y directivos.

- **Probabilidad de Riesgo Organizacional:** Evaluación global del riesgo para la organización.
- **Nivel de Riesgo por Perfiles de Ejecutivos:** Análisis específico de los riesgos asociados a diferentes perfiles de ejecutivos dentro de la organización.
- **Mitigaciones Existentes:** Descripción de las estrategias y medidas de protección que ya están en vigor para los perfiles de ejecutivos.
- **Perfiles de ejecutivos que se pueden gestionar con las mitigaciones existentes:** Identificación de los riesgos que ya están adecuadamente gestionados por las estrategias y medidas actuales.
- **Perfiles de ejecutivos que requieren mitigaciones adicionales:** Riesgos que aún superan la tolerancia de la organización y que requieren estrategias y medidas adicionales.

ESTRATEGIAS Y MEDIDAS DE PROTECCIÓN NECESARIAS

Este apartado detalla las opciones para manejar y mitigar los riesgos que no se encuentran en niveles tolerables:

Evitar riesgos: Actividades que se recomienda evitar para eliminar completamente el riesgo identificado.

Transferencia del riesgo: Uso de seguros u otros medios para compartir el riesgo con terceros.

Optimización del riesgo:

- a) Reducción de la probabilidad de ocurrencia través de medidas de preparación y prevención para disminuir la probabilidad de que el riesgo se materialice.
- b) Mitigación de riesgos al perfil reduciendo accesibilidad, exposición, predictibilidad.
- c) Mejora de respuesta en caso de que el riesgo ocurra. incrementa la capacidad y tiempo de respuesta.

Aceptación del Riesgo: Decisión informada de aceptar un riesgo, debido a la imposibilidad de mitigarlos sin incurrir en costos desproporcionados.

Análisis de Costo-Beneficio: Evaluación de las mitigaciones propuestas, considerando sus costos frente a los beneficios en términos de reducción del riesgo. Esto se conecta al presupuesto y reporte de retorno sobre la inversión en protección Ejecutiva (ROEPI)

RESULTADOS Y CONCLUSIONES

En esta sección se consolidan los hallazgos y recomendaciones de la SitRep:

Conclusiones y Recomendaciones de la SitRep: Resumen de las conclusiones alcanzadas y las recomendaciones para mitigar los riesgos identificados.

Alineación con la Tolerancia al Riesgo de la Organización: Explicación de cómo las recomendaciones se alinean con la tolerancia al riesgo establecida por la organización.

Pasos para Ejecutar por la Organización: Recomendaciones específicas sobre las acciones que la organización debe llevar a cabo.

Requisitos Futuros para la Reevaluación: Indicación de cuándo y cómo se deben realizar reevaluaciones para asegurar que los riesgos sigan siendo gestionados de manera efectiva.

APÉNDICES

Los apéndices incluyen información complementaria que respalda el contenido del reporte y puede incluir:

Fotos dibujos o planos: Imágenes relevantes que ilustran puntos clave del reporte.

Datos y estadísticas sobre delincuencia: Información cuantitativa que respalda las conclusiones.

Registro de Amenazas: Caracterización de capacidades e intención además de detalles adicionales sobre las amenazas identificadas.

Copia de seguridad: Información acerca de la custodia de copias de seguridad y nivel de confidencialidad