Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE CONTINUIDAD DEL NEGOCIO ISO 22301

CICLO REGULAR

MÓDULO II

CLASE 01

RIESGO Y AMENAZA DE LA CONTINUIDAD DEL NEGOCIO

Ing. Johnattan Sifuentes Rojas

MODULO II – Riesgo Y AMENZAS DE LA CONTINUIDAD DEL NEGOCIO

CONTENIDO MODULO II

1. Definiciones, Conceptos e Identificación de Riesgo y Amenaza.
2. Planificación y Operación del Riesgo en la Continuidad de Negocio
3. Análisis y evaluación del Riesgo de Continuidad del Negocio
4. Determinación de criterios del riesgo
5. Tratamiento del riesgo
6. Aceptación del riesgo
7. Relación entre Riesgo, controles y objetivos del SGCN

DEFINICIONES E IDENTIFICACION DE RIESGO Y AMENZA

DEFINICIONES E IDENTIFICACION DE RIESGO Y AMENAZA

RIESGO (ISO 22301)

Riesgo

Efecto de incertidumbre **sobre los objetivos**

Apetito por el Riesgo

Cantidad y tipo de riesgo que una organización está dispuesta a conseguir o conservar y debe estar **aprobado por la alta dirección** y documentado.

Evaluación de Riesgo

Proceso general de identificación, **análisis evaluación de Riesgo**

Gestión de Riesgo

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, **es un proceso continuo**

DEFINICIONES E IDENTIFICACION DE RIESGO Y AMENAZA

ISO 31000

Probabilidad

Grado al que es probable que se produzcan un evento

Consecuencia

Resultado de un evento

Impacto

Consecuencia evaluada de un resultado en particular

PLANIFICACIÓN Y OPERCIÓN DEL RIESGO EN SGCN

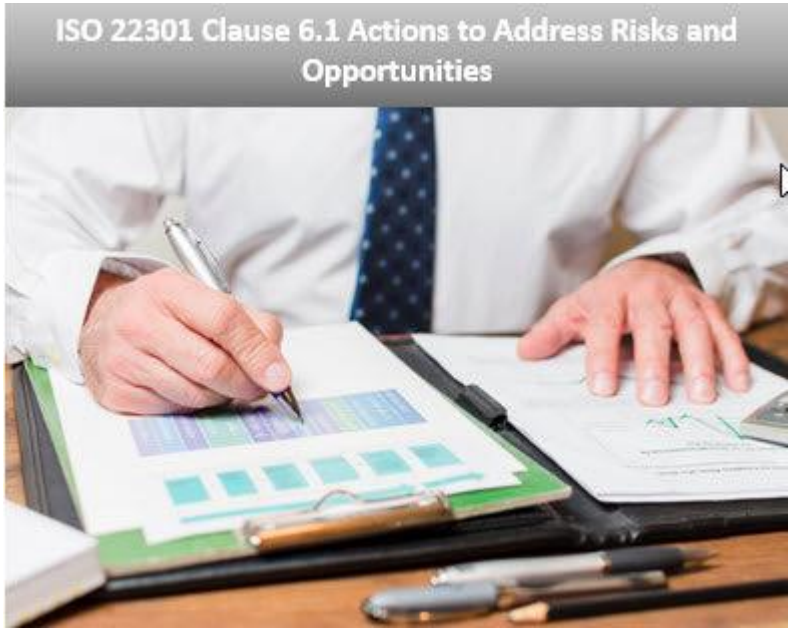
PLANIFICACIÓN Y OPERCIÓN DEL RIESGO EN SGCN

CONSIDERACIONES AL ANALIZAR EL RIESGO Y LA OPORTUNIDAD

Norma ISO 22301, clausula 6.1

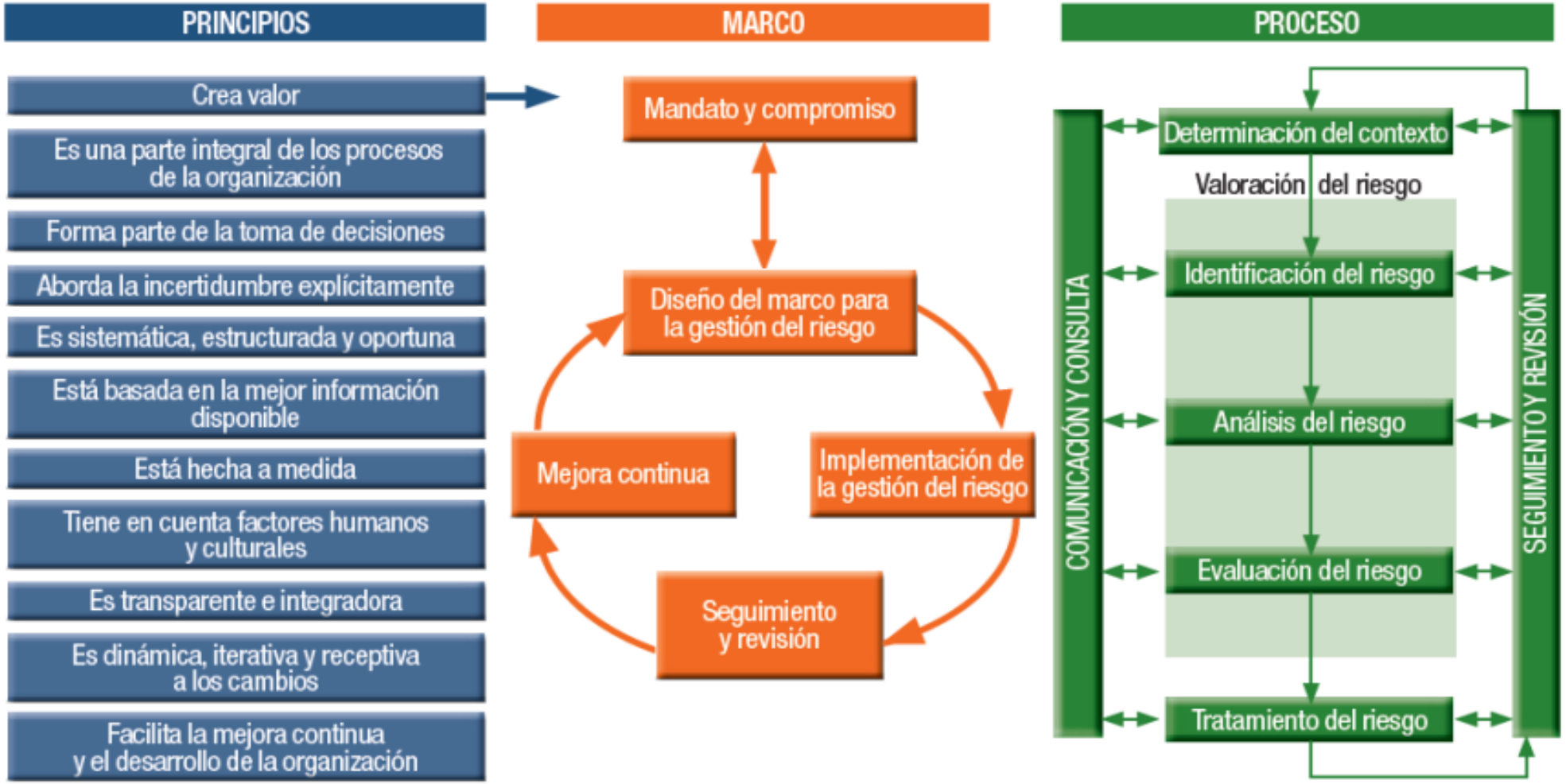
El pensamiento basado en Riesgo es esencial para lograr un sistema en gestión de calidad eficaz. El concepto de pensamiento basado en riesgo ha estado implícito en ediciones anteriores, incluyendo:

- Acciones preventivas
- Análisis de no conformidades
- Acciones correctivas



PLANIFICACIÓN Y OPERCIÓN DEL RIESGO EN SGCN

PROCESO DE GESTIÓN DE RIESGO



ANÁLISIS Y EVALUACIÓN DEL RIESGO EN SGCN

ANÁLISIS Y EVALUACIÓN DEL RIESGO EN SGCN

DETERMINANDO RIESGOS Y OPORTUNIDADES

Norma ISO 22301, clausula 6.1.1

Al planificar el SGCN, la organización debe considerar las cuestiones referidas en el subcapítulo 4.1 y los requisitos mencionado en el subcapítulo 4.2 y determinar el Riesgo y oportunidades que necesitan abordarse para:

a) Garantizar resultados en el SGCN.
b) Prevenir o reducir los efectos no deseados.
c) Lograr la mejora continua

ANÁLISIS Y EVALUACIÓN DEL RIESGOS EN SGCN

DETERMINANDO RIESGOS Y OPORTUNIDADES

Norma ISO 22301, clausula 6.1.1

Las oportunidades pueden surgir como resultado de una situación favorable para lograr un resultado previsto, por ejemplo un conjunto de circunstancias que permita a la organización atraes clientes, desarrollar nuevos productos y servicios, reducir los residuos o mejorar la productividad. Las acciones para abordar las oportunidades también pueden incluir la consideración del Riesgo asociados. El riesgo es el efecto de la incertidumbre y dicha incertidumbre puede tener efecto positivos o negativos. Una desviación positiva que surge de un riesgo puede proporcionar una oportunidad, pero no todos los efecto positivos del Riesgo tiene como resultado oportunidades.

ANÁLISIS Y EVALUACIÓN DE Riesgo DEL SGCN

ABORDANDO RIESGOS Y OPORTUNIDADES

Norma ISO 22301, clausula 6.1.12

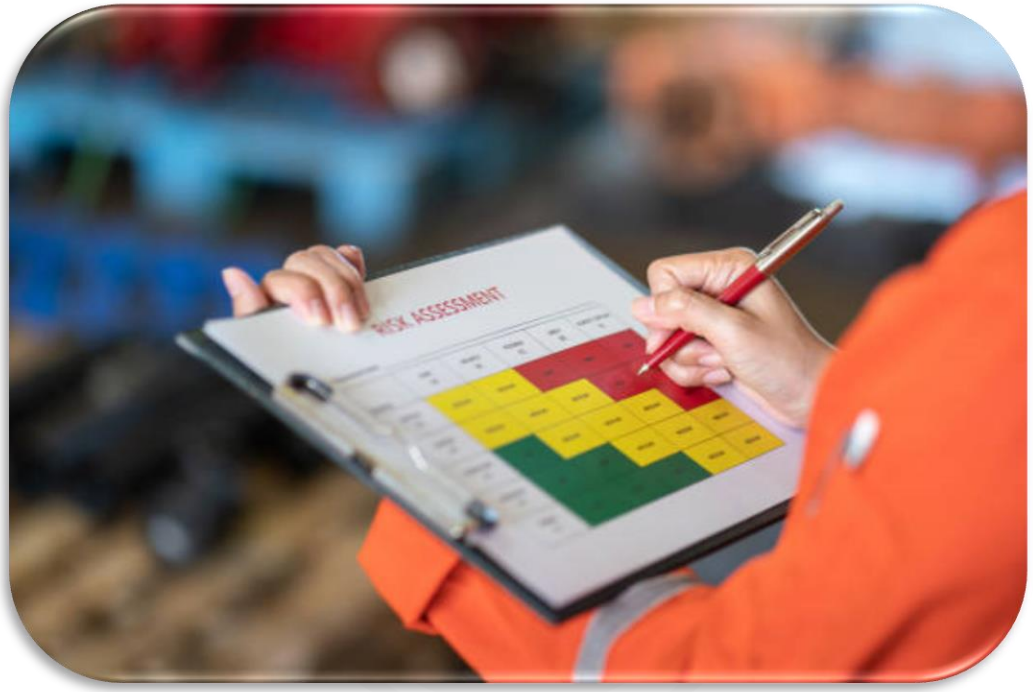
La empresa debe planificar:

a) Acciones para abordar el Riesgo y las oportunidades
b) La manera de integrar e implementar todas las acciones de los procesos en el SGCN
c) Evaluar la eficacia de las acciones

NOTA: Los Riesgo y las oportunidades se relacionan con la eficacia del sistema de gestión. El Riesgo relacionado con las disrupciones del negocio se abordan en el subcapítulo 8.2.

Ejemplo: Una organización evidencia su cumplimiento con el manual de gestión de Riesgo, matriz de Riesgo, mapa de Riesgo.

DETERMINACION DEL CRITERIO DEL Riesgo



DETERMINACION DEL CRITERIO DEL Riesgo

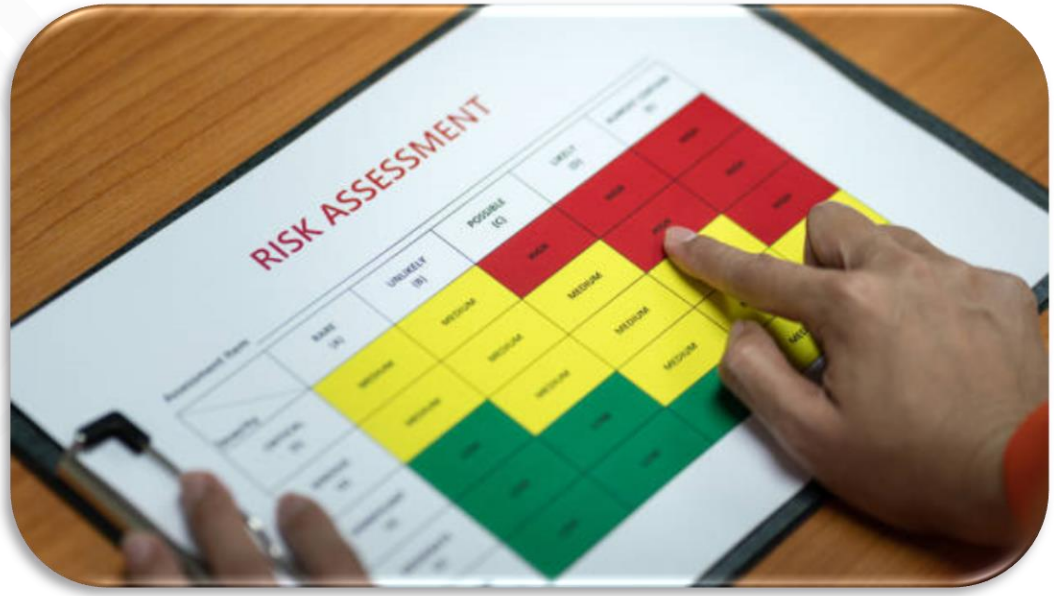
VALORACION DEL RIESGO

Norma ISO 22301, clausula 8.2.3

La organización deberá establecer, implementar y mantener un proceso formal documentado de evaluación del Riesgo que sistemáticamente identifica, analiza y evalúa el Riesgo de que se produzcan incidentes disruptivos a la organización.

La organizado debe:

- Identificar el Riesgo de la interrupción en la organización de actividades prioritarias y de los procesos, los sistemas, la información, las personas, los bienes, los socios externos y otros recursos que les sirve de apoyo.
- Evaluar el Riesgo
- Identificar los tratamientos acordes con objetivos del SGCN y de conformidad con el apetito por el Riesgo de la organización.
- Existir un proceso formal documentado (matriz de riesgo, mapa de riesgo)



DETERMINACION DEL CRITERIO DEL Riesgo

PROTECCION Y MITIGACION

Norma ISO 22301, clausula 8.2.3

Para identificar el Riesgo que requieren tratamiento, la organización deberá estudiar medidas proactivas que:

a) Reduzcan la posibilidad de una interrupción
b) Acorten el periodo de interrupción
c) Limiten el impacto de una interrupción y en la provisión de los productos y la presentación de los servicios principales de la organización.

La organización deberá elegir e implantar una tratamiento del Riesgo apropiados según su nivel de aceptación del riesgo.

DETERMINACION DEL CRITERIO DEL Riesgo

ANALISIS DE Riesgo

El análisis del Riesgo se define como el análisis de un entorno del Riesgo.
Cada riesgo se evalúa de acuerdo con:

- Las perdidas que pueden ocasionar.
- La probabilidad de ocurrencia
- El costo de las contra medidas para mitigar el riesgo
- La perdida probable si esas contras medidas fueron aplicadas.

Escenario 1	Posibles Causas/Amenaza	Consecuencias	Impacto
No disponibilidad	• Fuego • Inundación • Amenaza de bomba • Huelga • Manifestación • Fuga de gas • Huracán • Terremoto	• Se ha detenido la producción • Incapacidad para garantizar la logística de entrega • Incapacidad de facturar bienes entregados	3
			Probabilidad
			2
			Nivel del Riesgo
			6

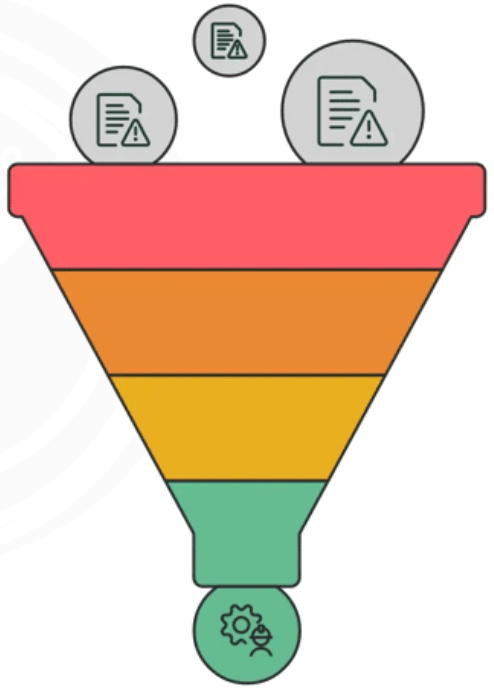
DETERMINACION DEL CRITIERO DEL RIESGO

EVALUACION DEL RIESGO

La evaluación del Riesgo es la comparación de los niveles del Riesgo estimados con los criterios de evaluación y los criterios de aceptación del Riesgo y priorizarlos

La estimación del Riesgo es necesaria antes de tomar una decisión sobre las posibles opciones para el tratamiento del Riesgo incluyendo:

- Si se tomaran medidas correctivas para reducir el nivel de riesgo calculado
- A Riesgo actual se le da prioridad.



Identificación de Riesgos
Identificar los riesgos tanto internos como externos de la organización.

Análisis de Riesgos
Evaluando la naturaleza y el impacto de los riesgos.

Valoración de Riesgos
Priorizando riesgos según su gravedad.

Tratamiento de Riesgos
Implementando medidas para mitigar riesgos.

pirani

DETERMINACION DEL CRITIERO DEL RIESGO

DECISION COMO RESULTADO DE LA EVALUACION DE RIESGO

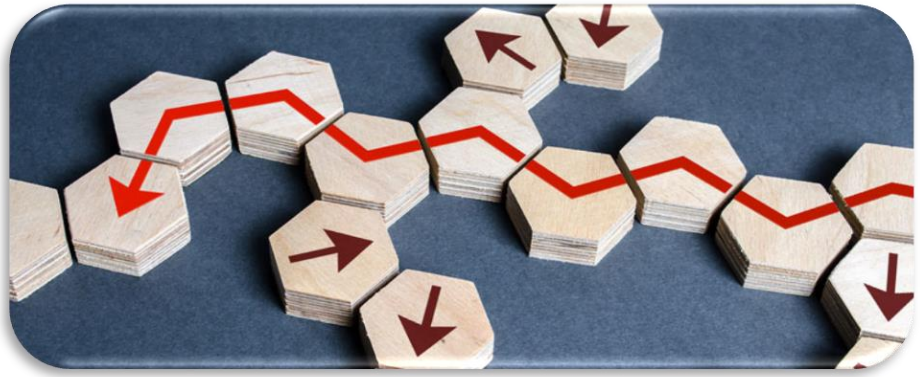
Las decisiones pueden incluir:

- Si un riesgo necesita tratamiento
- Prioridades de tratamiento
- Si una actividad debe llevarse a cabo
- Cual, de una cantidad de caminos debería seguirse

Amenaza	Valor de consecuencia (activo)	Probabilidad de ocurrencia de la amenaza	Nivel de riesgo	Orden de prioridad de la amenaza
Escenario A	5	2	10	2
Escenario B	2	4	8	3
Escenario C	3	5	15	1
Escenario D	1	3	3	5
Escenario E	4	1	4	4
Escenario F	2	4	8	3

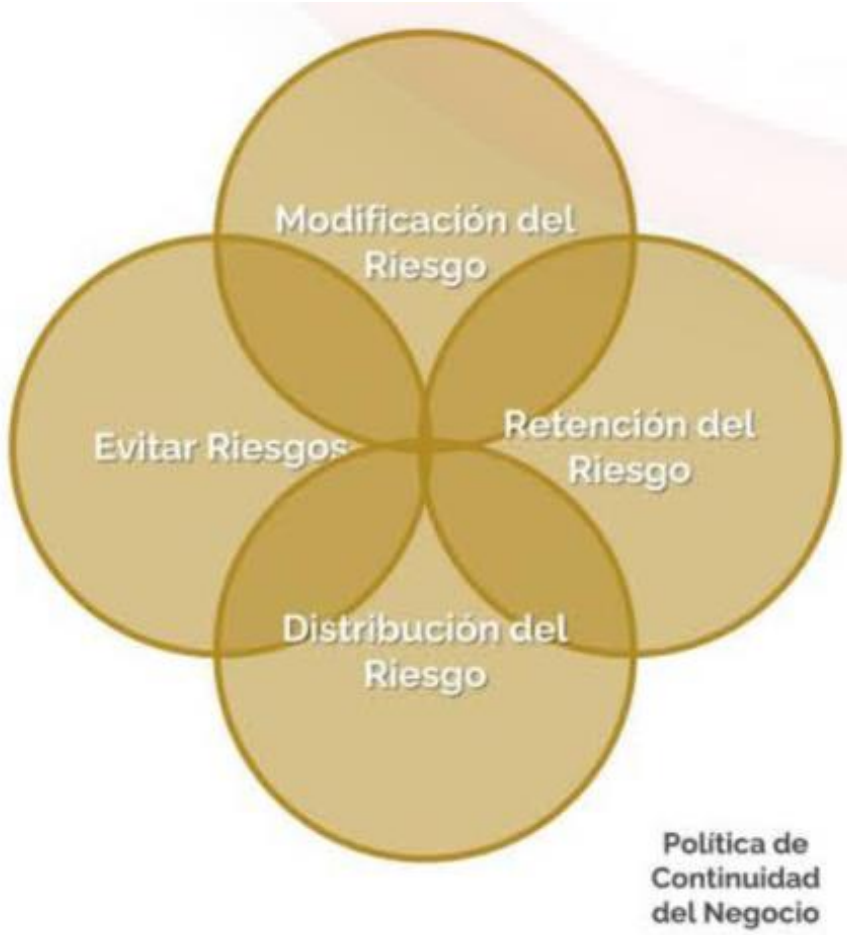
Nota: La decisión sobre las medidas a tomar después de la evaluación del riesgo se verá influida por el nivel de apetito por el riesgo de la organización

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO



TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

OPCIONES DE TRATAMIENTO



Modificación del Riesgo

- Presentar, retirar o modificar los controles de modo que el riesgo residual puede ser evaluado como aceptable

Retención del Riesgo

- La dirección decidió aceptar el nivel real de riesgo

Evitar del Riesgo

- Cancelación o modificación de una actividad o conjunto de actividades relacionadas con Riesgo

Distribución del Riesgo

- Decisión de compartir Riesgo con las partes externas: seguro o tercerización

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

OPCIONES DE TRATAMIENTO

Modificación del riesgo

- **Ejemplo 1:** Implementar un sistema de respaldo eléctrico (UPS) para reducir el impacto de cortes de energía en el centro de datos.
- **Ejemplo 2:** Instalar software de detección de intrusiones para disminuir la probabilidad de un ataque cibernético.
- **Ejemplo 3:** Reubicar servidores críticos en un área con menor riesgo de inundación, ajustando controles físicos. visual?

Retención del riesgo

- **Ejemplo 4:** Aceptar el riesgo de retrasos menores en la entrega de productos debido a tráfico urbano, porque el costo de mitigación sería mayor que el impacto.
- **Ejemplo 5:** Mantener la operación de un sistema heredado con vulnerabilidades conocidas, pero de bajo impacto, mientras se planifica su reemplazo.
- **Ejemplo 6:** Decidir no invertir en redundancia para un servicio secundario que no afecta procesos críticos.

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

OPCIONES DE TRATAMIENTO

Evitación del riesgo

- **Ejemplo 7:** Cancelar la apertura de una oficina en una zona con alta actividad sísmica y baja infraestructura de respaldo.
- **Ejemplo 8:** Eliminar un servicio en línea que expone datos sensibles y no cumple con requisitos regulatorios.
- **Ejemplo 9:** Suspender la producción de un producto cuya cadena de suministro depende de un único proveedor en un país políticamente inestable.

Distribución del riesgo

- **Ejemplo 10:** Contratar un seguro contra incendios para cubrir pérdidas en instalaciones críticas.
- **Ejemplo 11:** Externalizar la gestión de servidores a un proveedor de nube con acuerdos de nivel de servicio (SLA).
- **Ejemplo 12:** Compartir riesgos financieros mediante alianzas estratégicas con socios que cofinancian proyectos de continuidad.

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

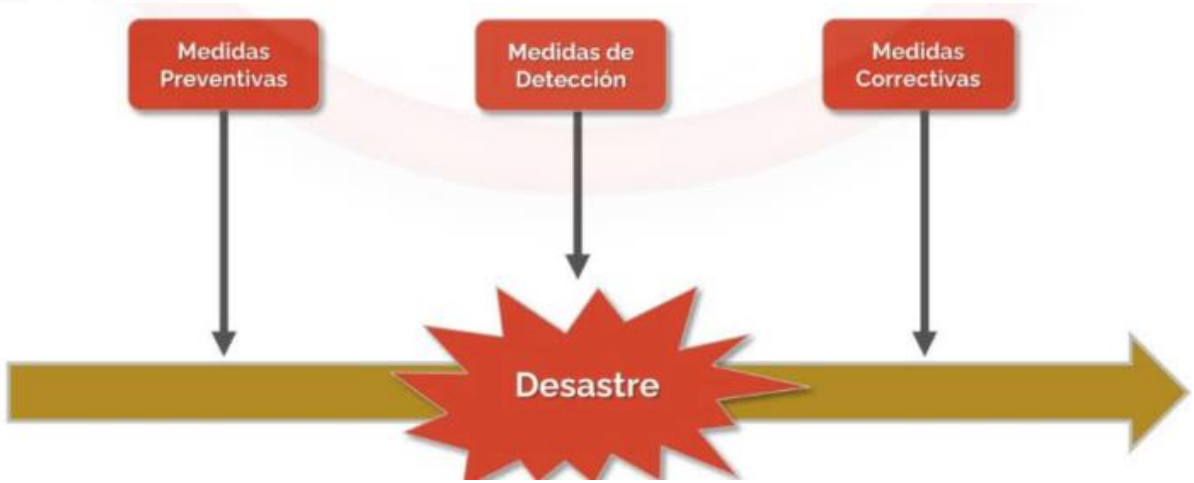
EVALUACION DE RIESGOS

Selección de medidas de protección y mitigación

- Los resultados de la evaluación del Riesgo ayudaran a guiar y determinar las medidas de gestión apropiadas y las prioridades de gestión del Riesgo y para aplicar las medidas de protección y mitigación para proteger contra el Riesgo.

- Las medidas pueden ser seleccionadas a partir de varias normas o pueden diseñarse nuevos controles para satisfacer las necesidades especificas de la organización

- La selección de medidas de protección y mitigación se detallan.



TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

APLICACIÓN DE MEDIDAS PREVENTIVAS

Medidas preventivas:

- Trabajar de manera proactiva
- Asegurarse de que su preparación es adecuada
- Desalentar o prevenir la aparición de problemas
- Debe estar basada sobre la mejora continua

Reducir la probabilidad y el posible impacto

- Gestión de Riesgo
- Protección física y lógica
- Gestión del cambio y de la configuración
- Mantenimiento del equipamiento

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

APLICACIÓN DE MEDIDAS DE DETECCIÓN

Medidas de detección:

- Detectar e identificar anomalías
- Dar indicación rápida
- No son discriminativas
- Deben ir seguidas de un procedimiento de escalada.

Reducir el impacto

Seguimiento

Alerta

Gestión de Incidentes

TRATAMIENTO Y ACEPTACIÓN DEL RIESGO

APLICACIÓN DE MEDIDAS DE CORRECTIVAS

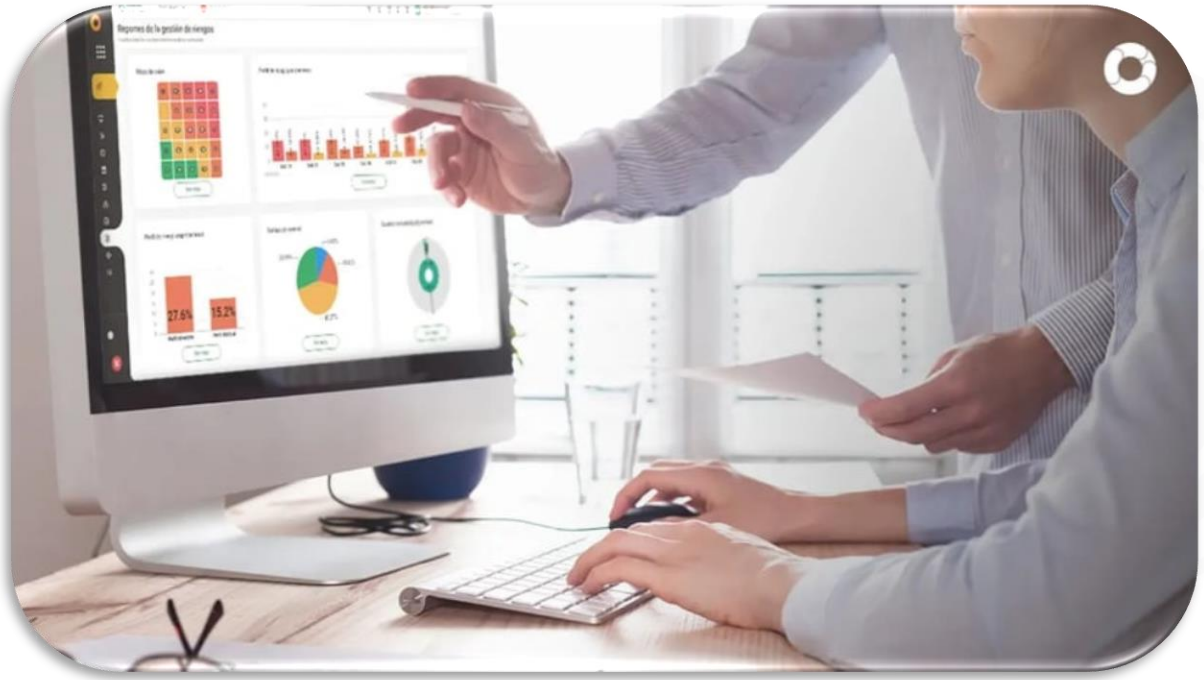
Medidas de correctivas:

- Trabajar a corto y largo plazo
- Deben seguir la gestión del cambio
- Muy probablemente necesitan la participación humana
- Deben incorporarse en la mejora continua

Mitigación de las consecuencias

- Planes de CN y RD (Recuperación ante desastres)
- Comunicación
- Copia de seguridad
- Seguimiento de No Conformidad

RIESGO, CONTROLES Y OBJETIVOS DEL SGCN



RIESGO, CONTROLES Y OBJETIVOS DEL SGCN

LOS OBJETIVOS Y LOS PLANES PARA ALCANZARLOS

Norma ISO 22301, clausula 6.2.
La alta dirección deberá asegurar de que los objetivos de continuidad del negocio son establecidos y comunicado para las funciones y los niveles pertinentes dentro de la organización.

Ejemplo: Una organización evidencia su cumplimiento con el documento donde se establezcan los objetivos definidos y realiza el seguimiento para su cumplimiento mediante reuniones periódicas.

RIESGO, CONTROLES Y OBJETIVOS DEL SGCN

LOS OBJETIVOS Y LOS PLANES PARA ALCANZARLOS

Norma ISO 22301, clausula 6.2.1

La organización debe establecer objetivos de continuidad del negocio en funciones y niveles relevantes

Los objetivos de CN debe:

a) Ser coherentes con la política de continuidad del negocio
b) Ser Medibles (si es posible)
c) Tomar en cuenta los requisitos aplicables (4.1 y 4.2)
d) Ser sujetos de seguimiento
e) Ser comunicados
f) Estar actualizados según corresponda

La organización debe tener información documentada sobre los objetivos de CN.

Riesgo, CONTROLES Y OBJETIVOS DEL SGCN

LOS OBJETIVOS Y LOS PLANES PARA ALCANZARLOS

Norma ISO 22301, clausula 6.2.2

Al planificar como lograr sus objetivos de continuidad del negocio, la organización debe determinar:

a) Lo que se hará
b) Que recursos se requerirán
c) Quien será responsable
d) Cuando se completara
e) Como se evaluaran los resultados.

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad