Gestión del Riesgo. ISO 31000:2018

Escuela Superior de Guerra "General Rafael Reyes Prieto" Colombia

Estamos en ACREDITACIÓN INSTITUCIONAL

ISO 31000:2018

Gestión del Riesgo

La norma ISO **31000** define la **Gestión** de **Riesgos** como todas aquellas acciones coordinadas para dirigir y controlar los **riesgos** a los que puedan estar abocadas las organizaciones.

Ventajas

Organización

- Seguridad a colaboradores y clientes
- Gestión de los riesgos
- Cultura de prevención
- Mejora en los sistemas de gestión

Partes interesadas

- Seguridad en grupos de interés
- Eficacia en situación de emergencia
- Acciones ante riesgos o amenazas

Mercado

- Credibilidad y prestigio
- Seguridad y confianza
- competitividad

Historia ISO 31000:2018 – gestión del riesgo

2009

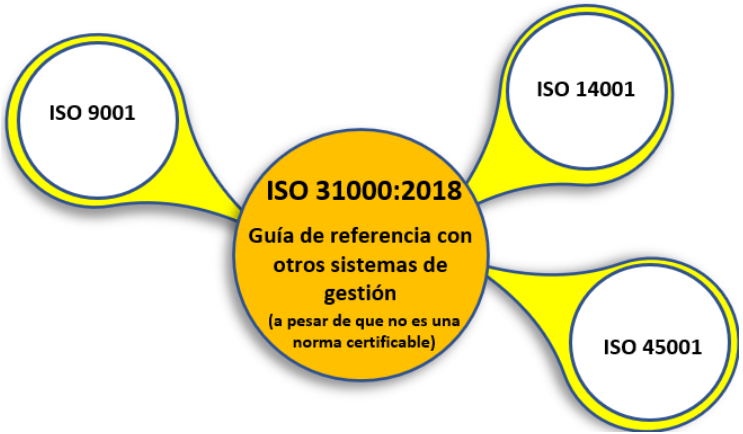
En noviembre de este año, la Organización Internacional de Normalización (ISO) publicó la norma ISO 31000:2009, Gestión de Riesgos - Principios y Directrices, una norma de gestión de nuevo destinado a ayudar a las organizaciones de todos los tipos y tamaños de gestionar el riesgo en la empresa.

2018

ofrece una guía más clara, breve y concisa que ayuda a las organizaciones a utilizar principios de gestión de riesgos para mejorar la planificación y tomar mejores decisiones y se presenta con mayor firmeza, como guía de referencia en lo relativo al riesgo para los estándares de ISO que dan lugar a otros sistemas de gestión, tales como ISO 9001, 14001, 45001, etc.

2005 2010 2015 2020

Alineamiento más importantes



Referente a otras normas:

ISO 9001
Sistemas de gestión de la calidad — Requisitos

ISO 14001
Sistemas de Gestión Ambiental

ISO 45001
Sistemas de gestión de la seguridad y salud en el trabajo

ISO 27001
Sistemas de Gestión de Seguridad de la Información

¿¿En que se Diferencia a otras Normas de Gestión del Riesgo?

Esta **se centra en los principios** de gestión de riesgos **en lugar de requisitos** específicos.

Ello permite adaptar los procesos de gestión de riesgos a necesidades específicas.

Se basa en un enfoque de mejora continua, alentando a las organizaciones a revisar y mejorar regularmente sus procesos de gestión de riesgos con el tiempo.

DEFINCIÓN DE RIESGO ISO 31000:2018

RIESGO: Efecto de la incertidumbre sobre los objetivos

Gestión del riesgo.
Actividades coordinadas para dirigir y controlar la organización con relación al riesgo

ISO 31000:2018
Tipos de incertidumbre

Aleatoria	Reconoce la variación intrínseca de varios fenómenos y no puede ser reducida mediante nuevas investigaciones p.e Lanzar los dados
Epistémica	Falta de conocimiento que se puede reducir mediante la recopilación de más datos, perfeccionamiento de modelos y mejora de técnicas de muestreo

La incertidumbre puede reducirse pero no eliminarse por completo

Fuente: ISO31010

3 Términos y definiciones

3.1 Riesgo

"Efecto de la incertidumbre"

es el **estado**, incluso parcial,
de deficiencia de información
relacionada con la comprensión
o conocimiento de un evento,
su consecuencia o su probabilidad

Término común y definición esencial para las normas de sistemas de gestión que se proporcionan en Anexo SL de Directivas ISO/IEC

¿Qué dicen las demás normas sobre el Riesgo?

ISO 9001:2015 define el “pensamiento basado en el riesgo”. El concepto de pensamiento basado en el riesgo siempre ha estado implícito en la norma ISO-9001, aunque en esta nueva versión se fortalece y se incorpora a todo el Sistema de Gestión de la Calidad. Este concepto se ve reforzado en los requisitos de establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de la Calidad.

Además en la ISO 9000:2015 - fundamentos y vocabulario (3.7.4)
la definición de riesgo coincide con la de la ISO 31000

¿Qué dicen las demás normas sobre el Riesgo?

ISO 20000-1:2018

coincide con la misma definición de la ISO 31000, pero está orientada a los servicios de TI.

BS ISO/IEC 27005

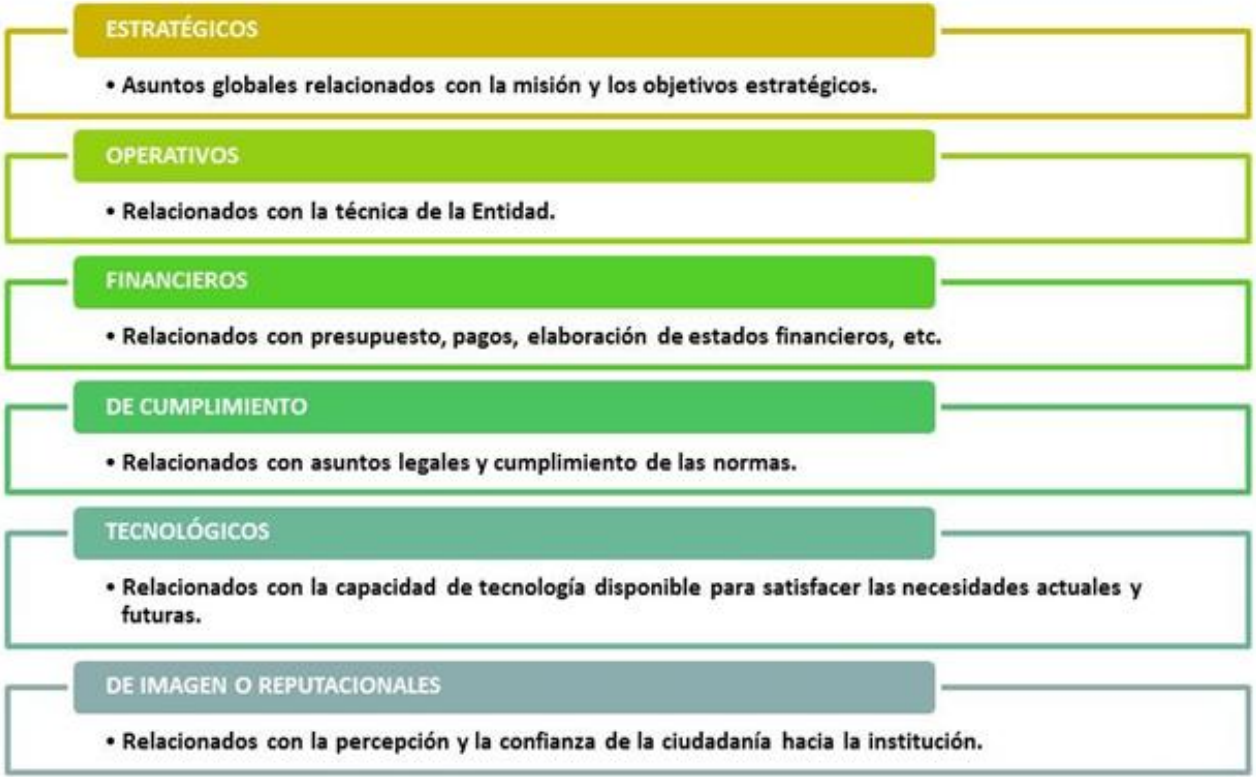
Information Security risk management : La probabilidad de que una amenaza explote una vulnerabilidad de un activo o grupo de activos (item 3: Term and definitions)

Definiciones importantes

GRC (Governance- Risk Management – Compliance): **Son los tres pilares** de una organización que trabajan en conjunto para lograr el cumplimientode los objetivos de la organización.

RIESGO:
De acuerdo a la ISO 31000:2009,
Risk management – Principles and guidelines
se define como el “Efecto de la incertidumbre sobre los objetivos”.

ISO 31000: TIPOS DE ESCENARIOS DE RIESGO



Fuente: http://www.krio.es/tipos-de-escenarios-de-riesgo/

ISO-31000:2018 Estructura

- Prólogo Introducción
- 1. Objeto y campo de aplicación
- 2. Referencias normativas
- 3. Términos y definiciones
- 4. Principios
- 5. Marco de referencia
- 6. Bibliografía

1. Principios

- Crea valor.
- Está integrada en los procesos de la organización.
- Forma parte de la toma de decisiones.
- Trata explícitamente la incertidumbre.
- Es sistemática, estructurada y adecuada.
- Está basada en la mejor información posible.
- Está hecha a medida.
- Tiene en cuenta factores humanos y culturales.
- Es transparente e inclusiva.
- Es dinámica, iterativa y sensible al cambio.
- Facilita la mejora continua de la organización.

2. Marco de referencia

El proceso de la **ISO 31000** implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.

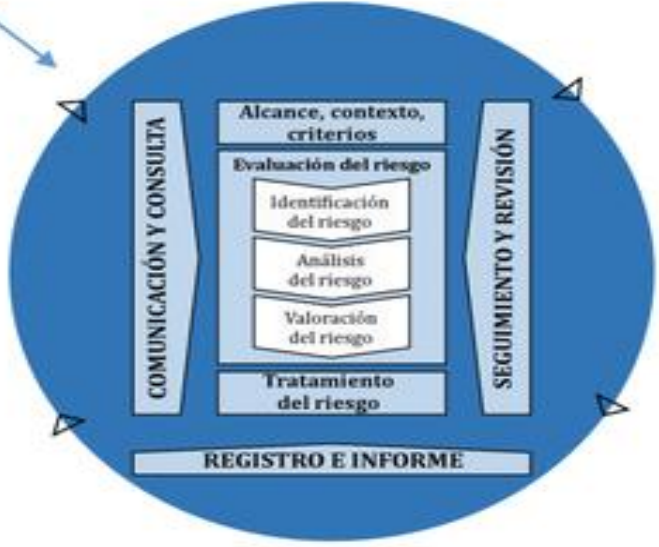
Además, la norma establece que el tratamiento del riesgo no solo debe centrarse en **mitigar amenazas**, sino también en **identificar y potenciar riesgos positivos** que puedan convertirse en oportunidades.

Evolución del enfoque de la Gestión de Riesgos	
Visión tradicional	Visión integral
Riesgo: Probabilidad y consecuencia de un evento capazde producir una pérdida	Riesgo: Efecto de la incertidumbre sobre los objetivos

Principios, Marco de Referencia y Proceso

Principios (capítulo 4)

Marco de referencia (capítulo 5)



Proceso (capítulo 6)

4. PRINCIPIOS

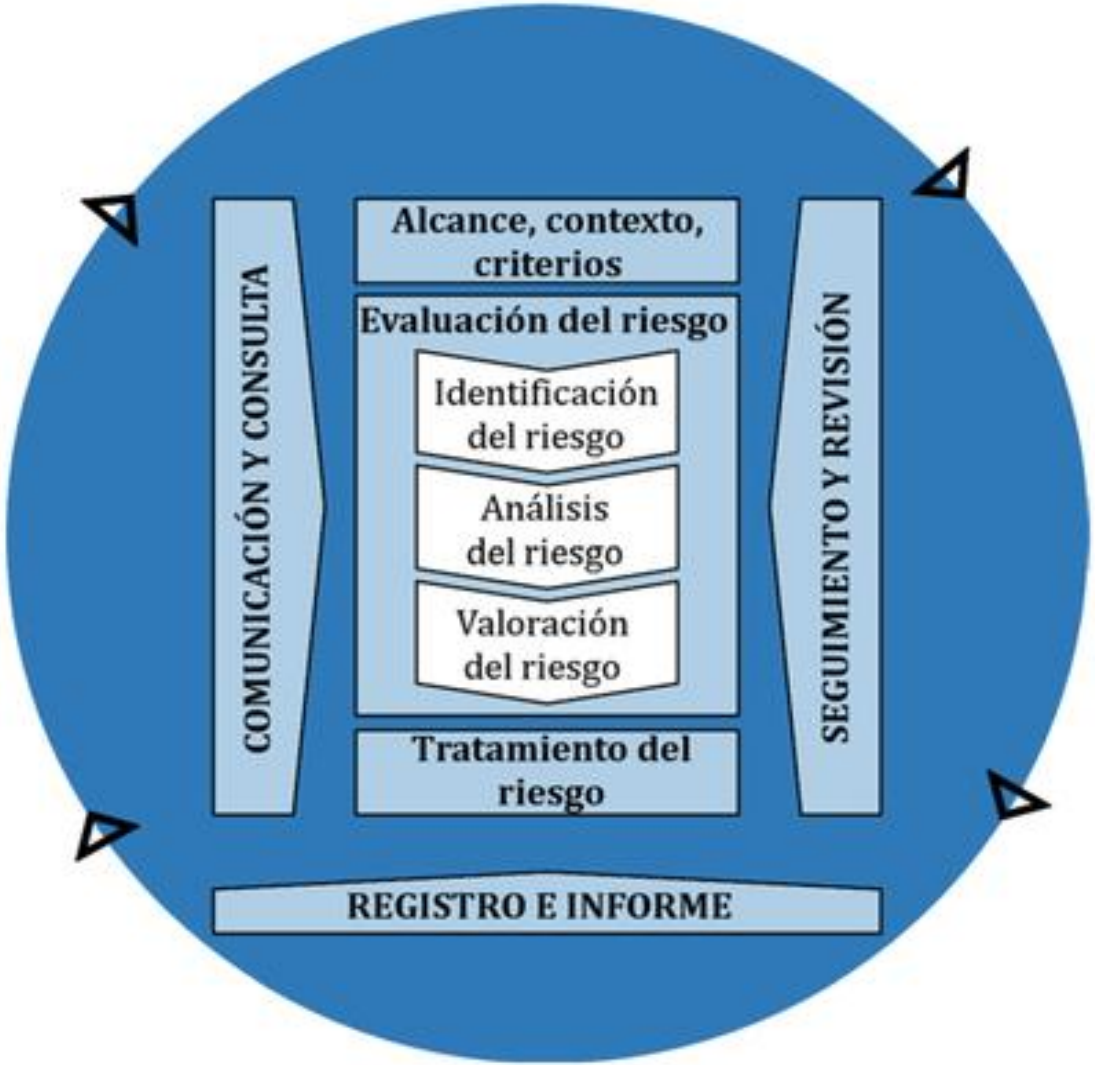
(Directrices generales del sistema de gestión)

5.1 MARCO DE REFERENCIA

(Estructura que soporta el sistema)

Su propósito es el de asistir en la integración del sistemas de gestión del riesgo en todas sus actividades y funciones significativas.
Su eficacia dependerá de su integración en la administración de la organización, incluyendo la toma de decisiones, asignar recursos, comunicación de beneficios, valoración de su eficacia, seguimiento y mejora continua teniendo en cuenta su idoneidad, adecuación y eficiencia.

6.1 Generalidades



Proceso

(metodología para el tratamiento eficaz de los riesgos)

Implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo

Metodologías de análisis de riesgos

Metodologías de gestión del riesgo

- AS/NZS 4360
- ISO 31000
- APPCC
- ARO

Metodologías de cuantificación

- **Cualitativos** (Brainstorming, Cuestionario y entrevistas estructuradas, Evaluación para grupos multidisciplinarios, Técnica Delphi)
- **Semicuantitativos**
- **Cuantitativos** (Análisis de probabilidad, Análisis de consecuencias, Simulación computacional

Formas verbales

Debe	• Indica un requisito
Debería	• Indica una recomendación
Puede	• Indica un permiso, una posibilidad o capacidad

Proceso de gestión del riesgo

PROCESO GESTIÓN DE RIESGOS

Alcance, contexto y criterios

PROCESO GESTIÓN DE RIESGOS

Evaluación del riesgo - Identificación

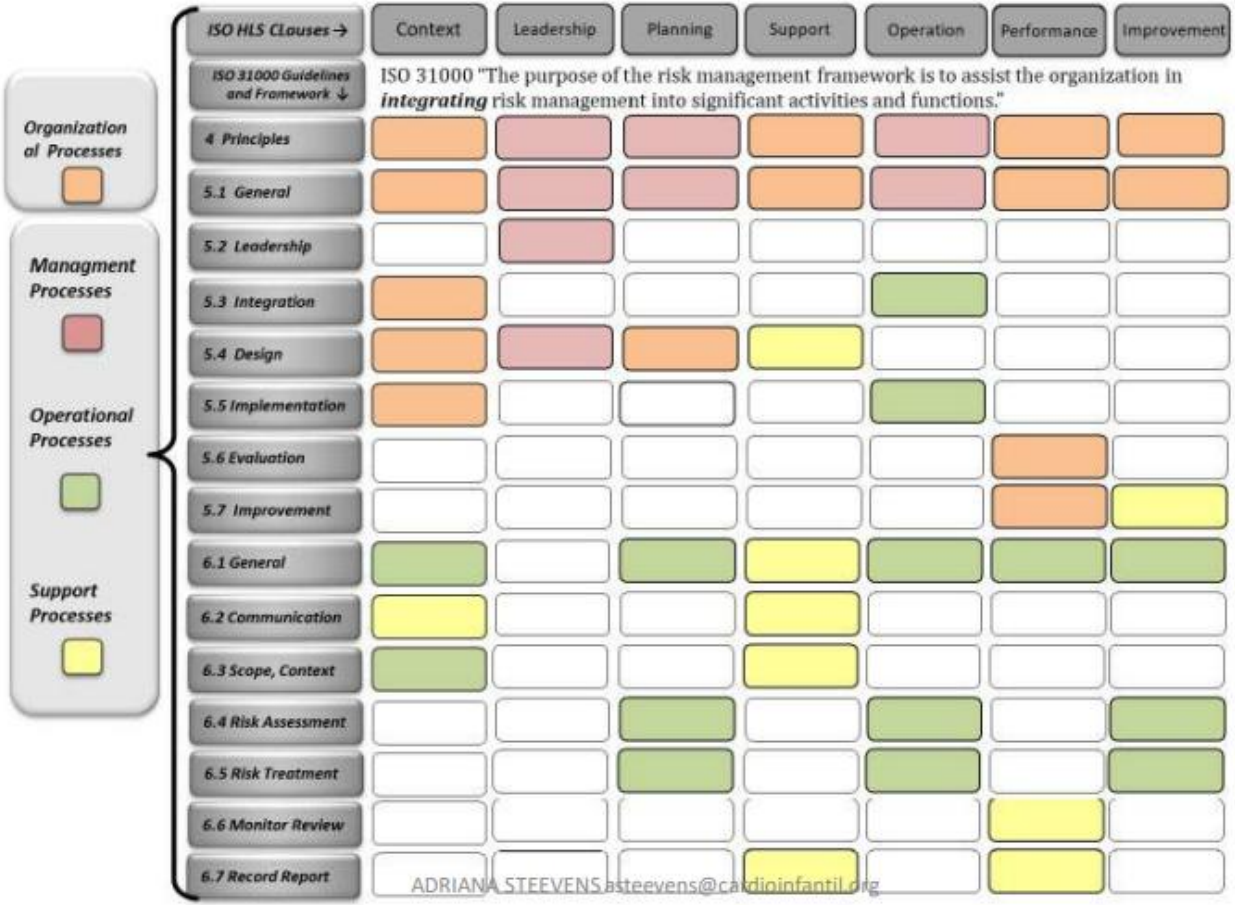
Identificar fuentes de incertidumbre y predecir sus efectos

Qué ha sucedido en el pasado y como puede relacionarse con el futuro

Analizar interacciones y dependencias

Risk management – Guidelines on using ISO 31000 in management systems

relation between HLS and ISO 31000



ADRIANA STEEVENS asteevens@cardioinfantil.org

PROCESO GESTIÓN DE RIESGOS

Evaluación del riesgo - Análisis

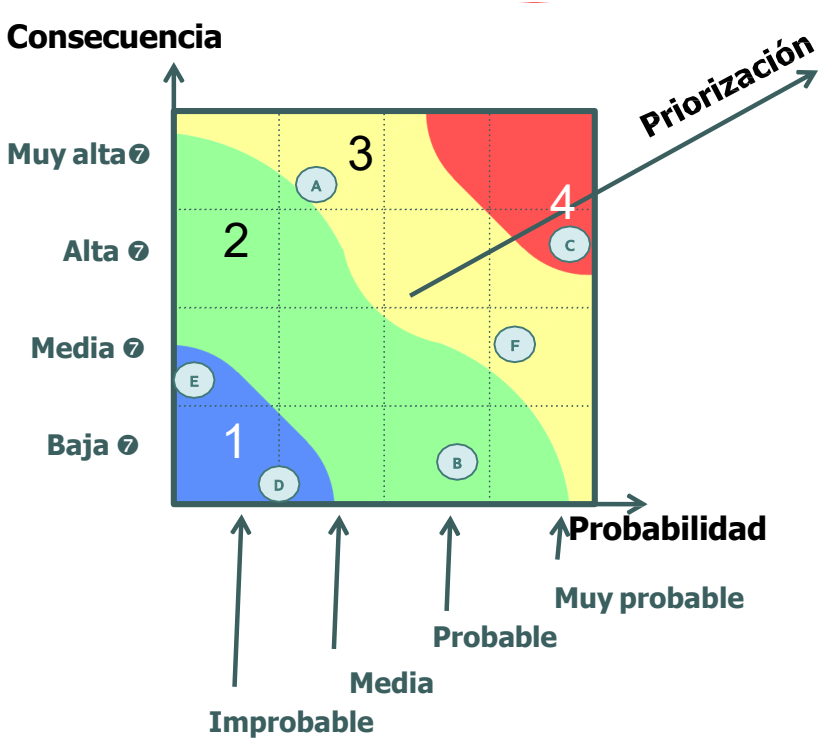
Considerar

Puede estar incluenciada por sesgos, percepción creencias, juicios de personas involucradas

Probabilidad de los eventos y de las consecuencias	Naturaleza y la magnitud de las consecuencias	complejidad y la interconexión	Factores relacionados con el tiempo y la volatilidad	Eficacia de los controles existentes	Niveles de sensibilidad y de confianza.

PROCESO GESTIÓN DE RIESGOS

Evaluación del riesgo - Valoración



TÉCNICAS DE EVALUACIÓN DE RIESGO

Tipos de técnicas

- Lluvia de ideas
- Lista de verificación
- Análisis de peligros y puntos críticos de control
- Análisis de escenarios
- Análisis de modo y efecto de falla EMEF
- Entrevista estructurada
- Análisis primario de peligros
- Valoración del riesgo ambiental
- Análisis de impacto al negocio
- Análisis de árbol de fallas
- Delphi
- Estudio de peligros y operatividad HAZOP
- Estructura que pasa si SWIFT
- Análisis de causa raíz
- Análisis de árbol de eventos

TÉCNICAS DE EVALUACIÓN DE RIESGO

Tipos de técnicas

- Análisis de causa y consecuencia
- Árbol de decisión
- Mantenimiento enfocado en la confiabilidad
- Simulación Monte Carlos
- Matriz de consecuencia y probabilidad
- Análisis de causa/efecto
- Análisis de confiabilidad humana
- Análisis de circuito furtivo
- Redes bayesianas
- Análisis de costo/beneficio
- Análisis de capas de protección LOPA
- Análisis de esquema de corbatín Bow Tie
- Análisis de Markov
- Índices de riesgo
- Análisis de decisión por criterios múltiples

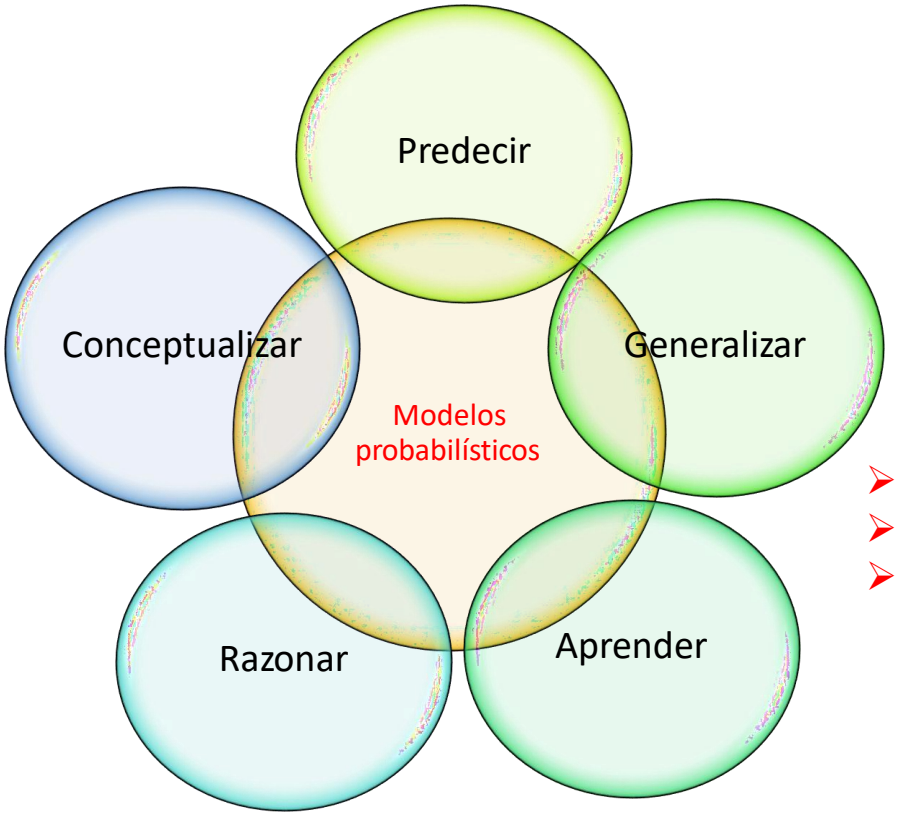
ACTIVIDAD EN GRUPO

Realizar un glosario dentro de un README.md en el repositorio de curso, definiendo de manera sintética cada uno de las técnicas referenciadas anteriormente y citando un ejemplo en el marco de la ciberseguridad y ciberdefensa.

Consignar el trabajo dentro de la subcarpeta “TECNICAS” de la carpeta “TRABAJOS” de este repositorio. Dentro de una carpeta con nombre “GRUPO_X” donde grupo X es por ejemplo GRUPO_1

TÉCNICAS DE EVALUACIÓN DE RIESGO

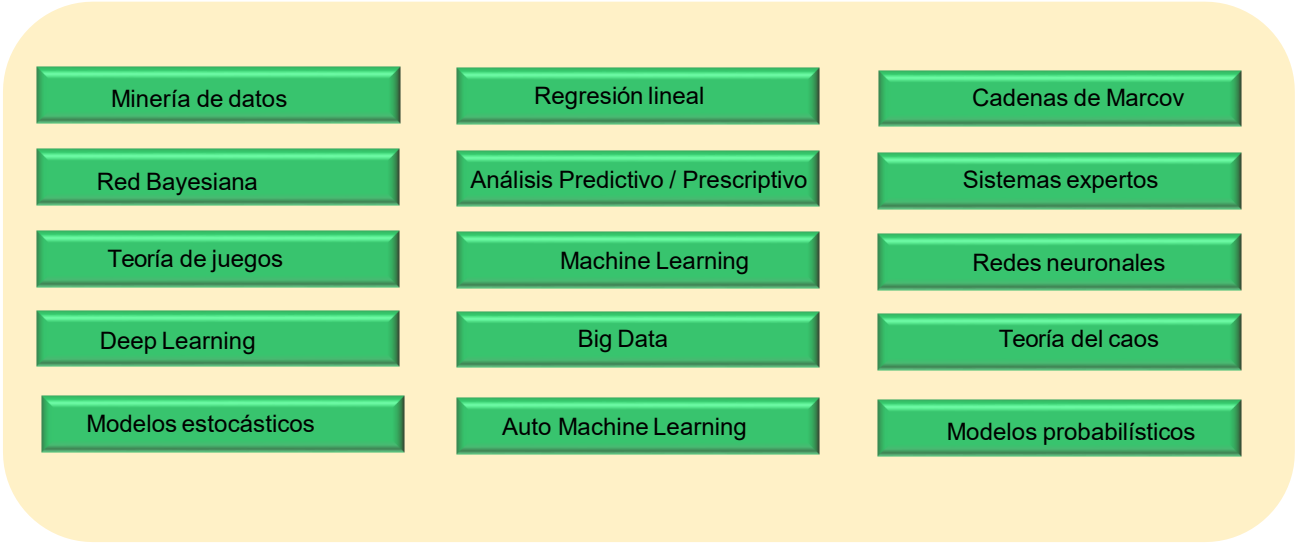
Necesidad de soportarse en modelos probabilísticos



- ***Datos***
- ***Parámetros***
- ***Función de Error***

TÉCNICAS AVANZADAS

EVALUACION DE RIESGO



https://github.com/jaiderospina/GESTION_RIESGO/tree/main/TECNICAS

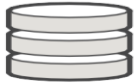
TÉCNICAS EVALUACIÓN DE RIESGOS

Modelos predictivos

ACCESS AND EXPLORE DATA → PREPROCESS DATA → DEVELOP PREDICTIVE MODELS → INTEGRATE ANALYTICS WITH SYSTEMS

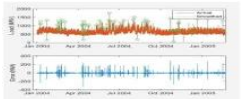
Files

Databases



Sensors

Working with Messy Data

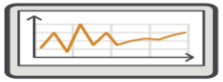


Data Reduction/ Transformation

Feature Extraction

Model Creation
e.g. Machine Learning

Parameter Optimization



Model Validation

Desktop Apps

Enterprise Scale Systems

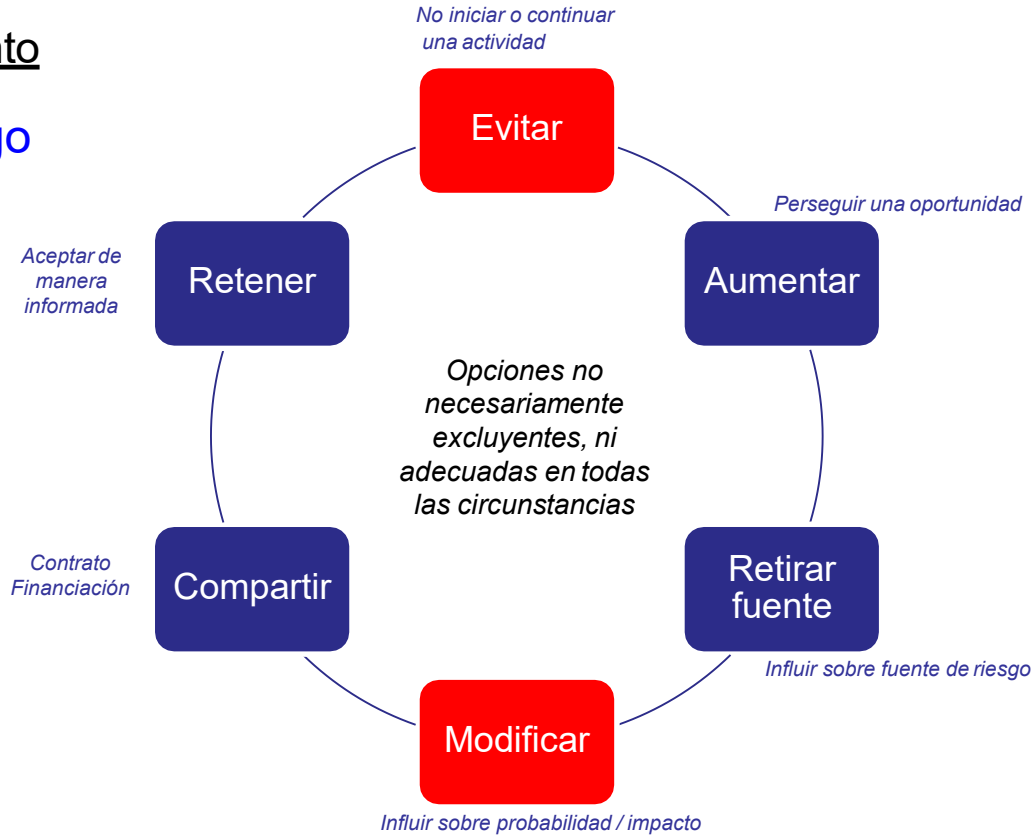
MATLAB Excel
Java C/C++ .exe
.NET .dll Python

Embedded Devices and Hardware

PROCESO GESTIÓN DE RIESGOS

Opciones de tratamiento

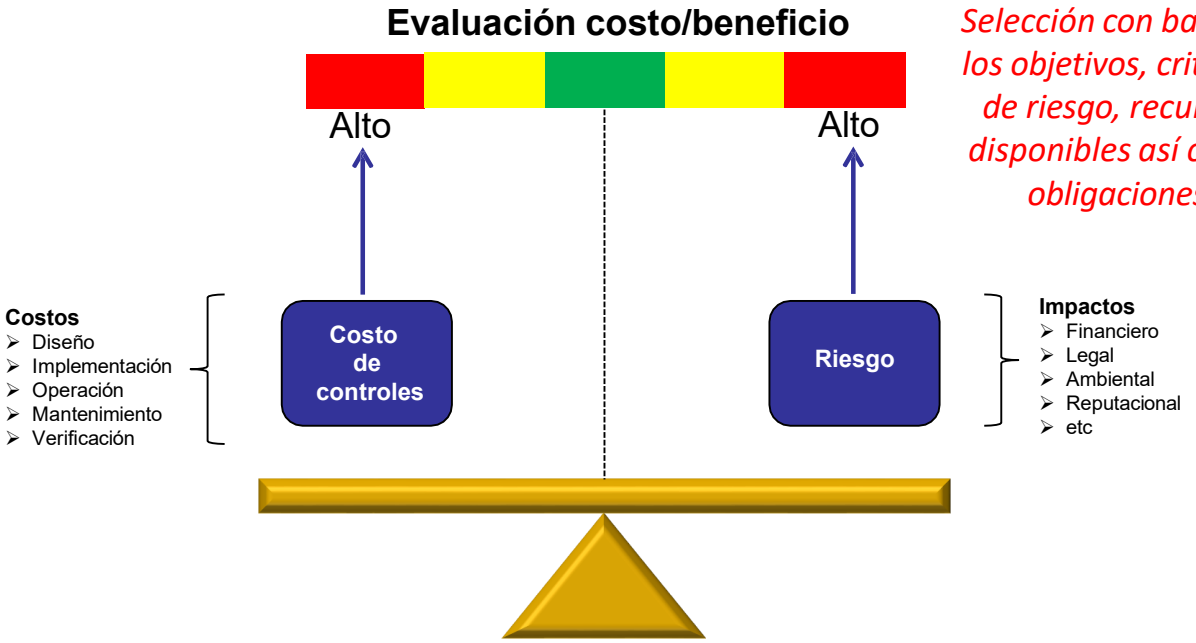
Tratamiento del riesgo



PROCESO GESTIÓN DE RIESGOS

Tratamiento del riesgo

Selección de las opciones para tratamiento



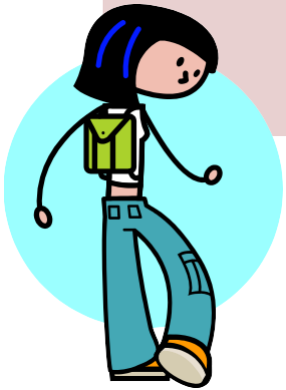
Selección con base en los objetivos, criterios de riesgo, recursos disponibles así como obligaciones

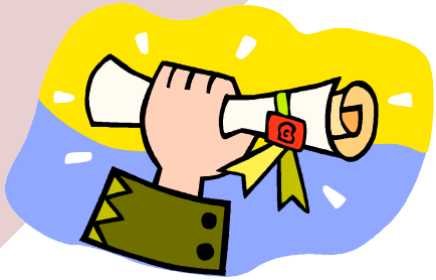
VALORACIÓN DEL RIESGO

Identificar el Riesgo

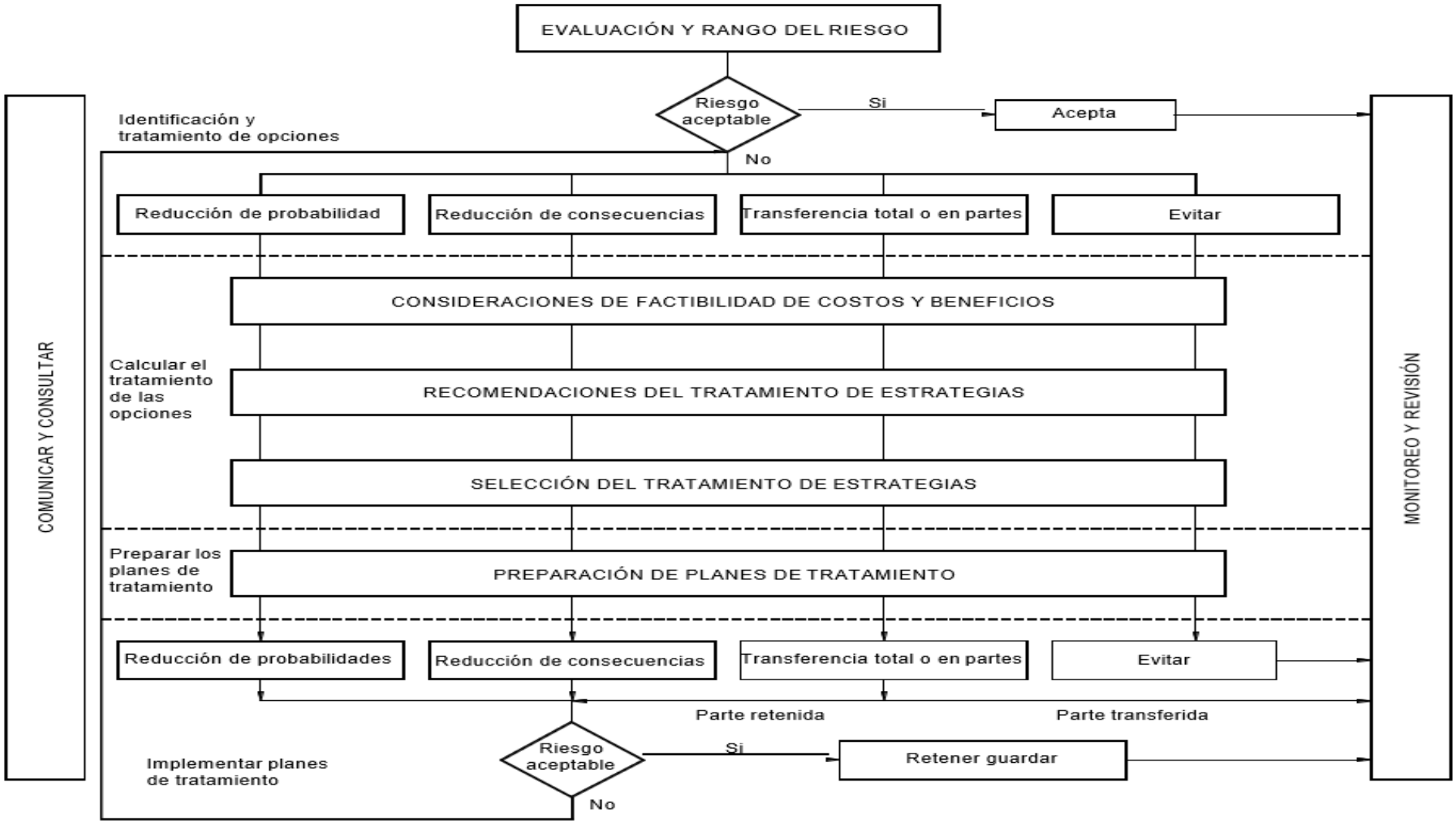
Analizar el Riesgo

Evaluar el Riesgo



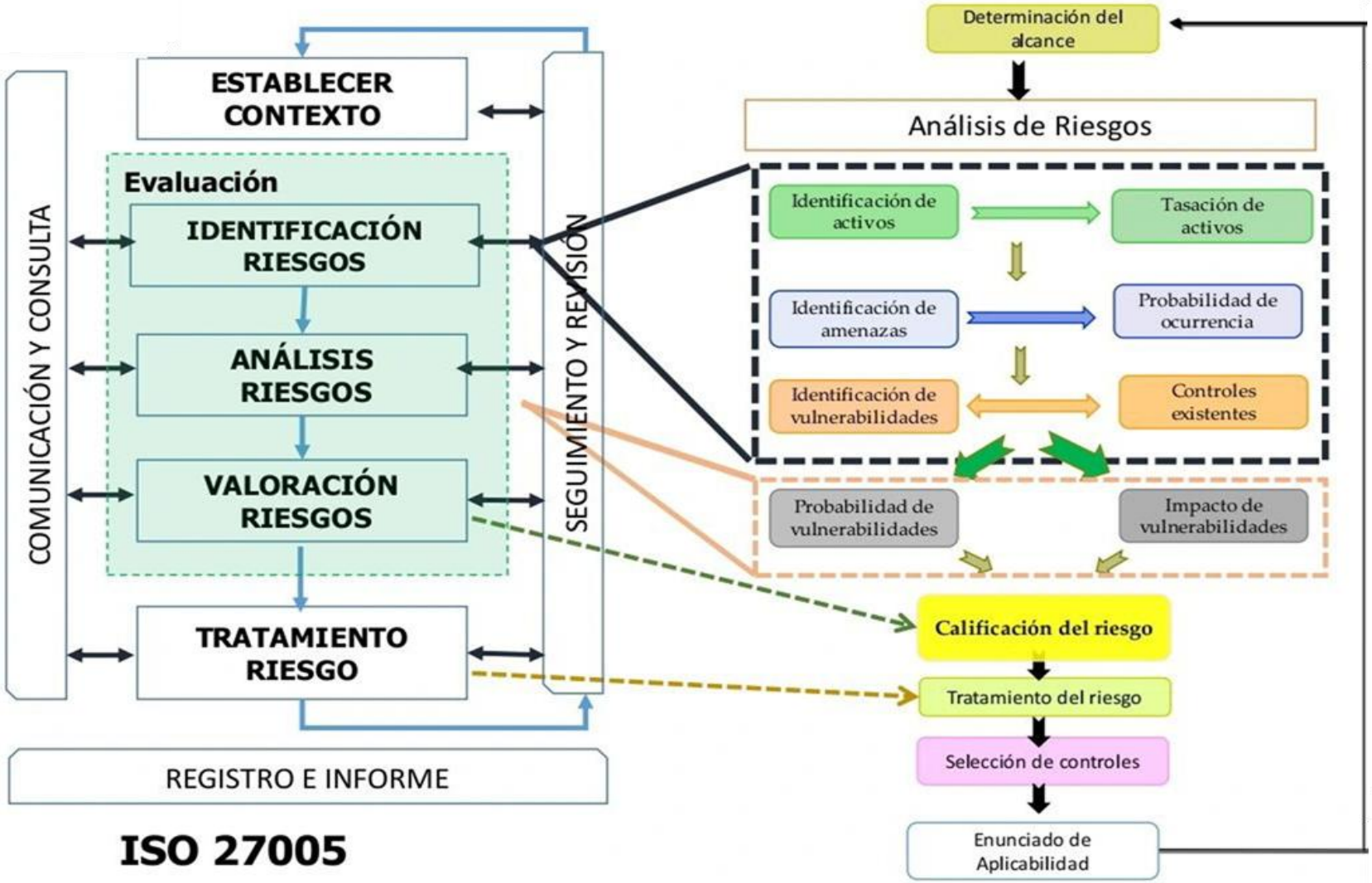



feedback


EVALUACIÓN Y RANGO DEL RIESGO
Riesgo aceptable
Si
Acepta
No
Identificación y tratamiento de opciones
Reducción de probabilidad
Reducción de consecuencias
Transferencia total o en partes
Evitar
CONSIDERACIONES DE FACTIBILIDAD DE COSTOS Y BENEFICIOS
Calcular el tratamiento de las opciones
RECOMENDACIONES DEL TRATAMIENTO DE ESTRATEGIAS
SELECCIÓN DEL TRATAMIENTO DE ESTRATEGIAS
Preparar los planes de tratamiento
PREPARACIÓN DE PLANES DE TRATAMIENTO
Reducción de probabilidades
Reducción de consecuencias
Transferencia total o en partes
Evitar
Parte retenida
Parte transferida
Riesgo aceptable
Si
Retener guardar
Implementar planes de tratamiento
No
COMUNICAR Y CONSULTAR
MONITOREO Y REVISIÓN

ISO 27005

Gestión de Riesgo en Seguridad de Información



Aceptación de los Riesgos Residuales

Sistema de Gestión de Seguridad de la Información

Riesgo Tratado

Riesgo tratado con controles

Riesgo Inherente

Todos los riesgos sin tener en cuenta los controles

Riesgo Residual

Riesgo remanente después del tratamiento de riesgos

Los dueños de los riesgos deben estar conscientes de los riesgos residuales y aceptar la responsabilidad por estos.

CIT

ISO 27005

https://prezi.com/otmtpm2wnmpc/

Referencias

https://www.ealde.es/iso-31000-para-que-sirve/

https://github.com/jaiderospina/GESTION_RIESGO/tree/main

www.ro-sas.com

Estamos en ACREDITACIÓN INSTITUCIONAL

Escuela Superior de Guerra "General Rafael Reyes Prieto" Colombia

GRACIAS

Escuela Superior de Guerra | @EsdegCol | Escuela Superior de Guerra | Escuela Superior de Guerra | Escuela Superior de Guerra | Esdegdigital

www.esdegue.edu.co

ISO 9001:2015
ISO 21001:2018
BUREAU VERITAS Certification

La ***Escuela Superior de Guerra "General Rafael Reyes Prieto"*** está certificada bajo las normas internacionales **ISO 9001:2015** e **ISO**

UNIDOS PROYECTAMOS LIDERAZGO