ANÁLISIS Y GESTIÓN DE RIESGO

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

El proceso de análisis de riesgo genera habitualmente un documento al cual se le conoce como matriz de riesgo.

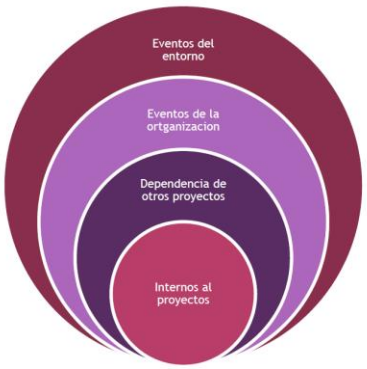
		PROBABILIDAD				
		Raro	Poco probable	Posible	Muy probable	Casi seguro
CONSECUENCIAS	Despreciable	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy alto
	Catastróficas	Medio	Alto	Alto	Muy alto	Muy alto

EJEMPLO DE MATRIZ DE VALORACIÓN DEL RIESGO CUALITATIVA

La clasificación del riesgo permite realizar una mejor identificación de los riesgos inherentes a los procesos de la Organización, ya que delimita los parámetros a seguir por el responsable. Esta sería una posible clasificación:

- Riesgo estratégico
- Riesgo operativo
- Riesgo de control
- Riesgo financiero
- Riesgo de tecnología
- Riesgo de incumplimiento
- Riesgo de fraude
- Riesgo de ambiente laboral

¿Que riesgos analizar? Esta imagen es de gran ayuda para visualizar los "anillos del riesgo" a los cuales se expone una Organización:



ANILLOS DEL RIESGO

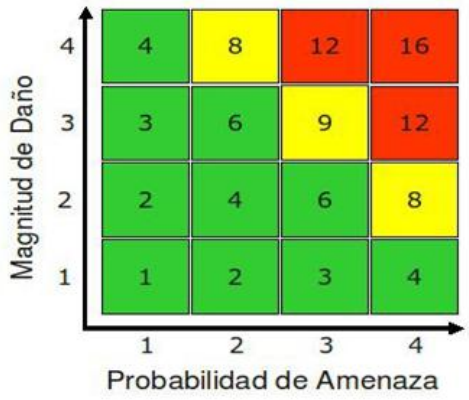
La ponderación del riesgo consiste en establecer los niveles adecuados de calificación, tanto de la probabilidad como del impacto, para determinar realmente el nivel de vulnerabilidad en la Organización ante situaciones previsibles. También se debe tener en cuenta los factores de riesgo enunciados durante el proceso de identificación.

- **Probabilidad de ocurrencia:** para determinar este ítem se debe considerar los controles utilizados hasta el momento y la efectividad de los mismos, así como, la frecuencia en la que ocurren los riesgos y en la que se van a analizar.
- **Impacto:** en este ítem se evalúan las consecuencias en caso que el hecho que originó el riesgo se materialice. También analiza el grado en que afecta los objetivos de los procesos involucrados o, inclusive de manera general a la Organización.

La Matriz se basa en el método de Análisis de Riesgo, usando la formula

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente. El Riesgo, es el producto de la multiplicación Probabilidad de Amenaza por Magnitud de Daño, y está agrupado en tres rangos, para su interpretación, se aplica diferentes colores.



EJEMPLO DE MATRIZ DE VALORACIÓN DEL RIESGO CUANTITATIVA

Para estimar la Probabilidad de amenazas, se trabaja con un valor que está relacionado con el recurso más vulnerable de los elementos de información.

Dependiendo de los valores de la **Probabilidad de Amenaza** y la **Magnitud de Daño**, la Matriz calcula el producto de ambos variables y visualiza el grado de riesgo.

Dependiendo del color de cada celda, podemos sacar conclusiones no solo sobre el nivel de riesgo que corre cada elemento de información de sufrir un daño significativo, causado por una amenaza, sino también sobre las medidas de protección necesarias.

Algunos Ejemplos (Ver Imagen **MATRIZ DE RIESGO**):

- Proteger los datos de RR.HH, Finanzas contra virus
- Proteger los datos de Finanzas y el Coordinador contra robo
- Evitar que se compartan las contraseñas de los portátiles
- Proteger el Personal (Coordinador y Personal técnico) contra Virus de computación

Matriz de Análisis de Riesgo		Probabilidad de Amenaza					
Elementos de Información	Magnitud de Daño	Criminalidad		Sucesos físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir contraseñas	No cifrar datos críticos
		3	4	2	3	4	3
Datos e Información							
RR.HH	3	9	12	6	9	12	9
Finanzas	4	12	16	8	12	16	12
Sistema e Información							
Computadoras	2	6	8	4	6	8	6
Portátiles	3	9	12	6	9	12	9
Personal							
Coordinador	4	12	16	8	12	16	12
Personal técnico	3	9	12	6	9	12	9

MATRIZ DE RIESGO

Después de efectuar el análisis debemos determinar las acciones a tomar respecto a los riesgos residuales que se identificaron. Las acciones pueden ser:

- Controlar el riesgo: Fortalecer los controles existentes y/o agregar nuevos controles.
- Eliminar el riesgo: Eliminar el activo relacionado y con ello se elimina el riesgo.
- Compartir el riesgo: Mediante acuerdos contractuales parte del riesgo se traspasa a un tercero.
- Aceptar el riesgo: Se determina que el nivel de exposición es adecuado y por lo tanto se acepta.