Seguridad Informática

Análisis de Riesgos

Visión del riesgo

Riesgos identificados

Riesgos “ocultos”

Algunos conceptos

Activo. recurso, producto, proceso, dato y todo aquello que tenga un valor para la organización.

Vulnerabilidad. ausencia o debilidad de un control que puede ser explotado.

Amenaza. evento cuya ocurrencia podría impactar en forma negativa en la organización.

Algunos conceptos

Impacto. Conjunto de posibles efectos negativos.

Riesgo. es la probabilidad de que una amenaza explote una vulnerabilidad, combinado con el impacto que ocasionaría.

Contramedida. cualquier tipo de medida que permita detectar, prevenir o minimizar el riesgo asociado con la ocurrencia de una amenaza específica.

Algunos ejemplos

Daño Físico: Fuego, agua, vandalismo, pérdida de energía y desastres naturales.

Acciones Humanas: Acción intencional o accidental que pueda atentar contra la productividad.

Fallas del Equipamiento: Fallas del sistema o dispositivos periféricos.

Ataques Internos o Externos: Hacking, Cracking y/o cualquier tipo de ataque.

Pérdida de Datos: Divulgación de secretos comerciales, fraude, espionaje y robo.

Errores en las Aplicaciones: Errores de computación, errores de entrada, buffers overflows

Preguntas a responder

¿Qué puede pasar? (Amenaza)

¿Si pasa, qué tan malo puede ser? (Impacto de la amenaza)

¿Qué tan seguido puede pasar? (Frecuencia de la amenaza)

¿Qué tan seguro estoy de las respuestas anteriores? (Falta de Certeza, Incertidumbre)

¿Qué puedo hacer? (Mitigar el riesgo)

¿Cuánto me costará? (Siempre calculado en forma anualizado)

¿Dicho costo es efectivo? (Relación costo beneficio)

El análisis de riesgos

Es un proceso que comprende la identificación de:

- los activos informáticos
- sus vulnerabilidades y
- sus 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, mitigar o transferir la ocurrencia de un riesgo.

El análisis de riesgos

- Forma parte del BCM (Business Continuity Management) o Programa de Gestión de Continuidad de Negocio.
- Forma parte de la AI
- Permite identificar riesgos
- Permite justificar dictámenes y recomendaciones
- Asignar riesgos a las observaciones

El análisis de riesgo

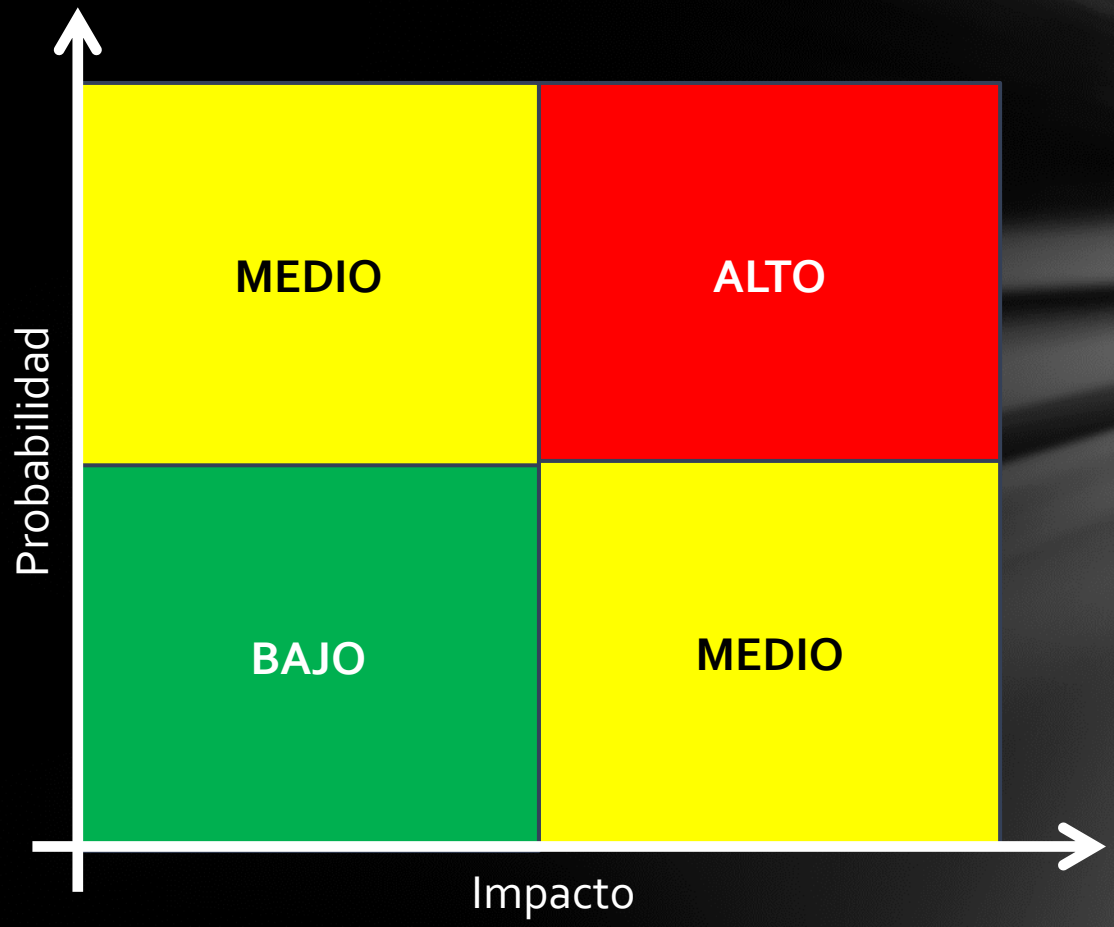
Es la base para la toma de decisiones relacionadas con la seguridad:

- Estrategia.
- Políticas de Seguridad.
- Plan de Continuidad del Procesamiento.

El Directorio o CEO es responsable directo de la gestión de riesgos de sistemas.

El Análisis de Riesgos de Sistemas debe ser actualizado periódicamente (sugerido anualmente).

El análisis de riesgo



Acciones y actividades generales

- Identificar los activos informáticos
- Identificar las amenazas
- Identificar la probabilidad de ocurrencia de las amenazas
  - Datos históricos
  - Experiencia
  - Estadísticas
- Ordenar las amenazas en función de su probabilidad de ocurrencia
- Ordenar los activos en función de su impacto/riesgo en la continuidad del sistema informático
- Cotizar los activos informáticos
  - Proformas de proveedores
- Confeccionar la Matriz

Acciones ISO 27001

- Identificación de los activos
- Identificación de los requisitos legales y de negocios que son relevantes para la identificación de los activos
- Valoración de los activos identificados
- Teniendo en cuenta los requisitos legales identificados de negocios y el impacto de una pérdida de confidencialidad, integridad y disponibilidad.
- Identificación de las amenazas y vulnerabilidades importantes para los activos identificados.
- Evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Cálculo del riesgo.
- Evaluación de los riesgos frente a una escala de riesgo preestablecidos.

Veamos una Matriz de Análisis de Riesgos

Activo	Valor Reposición	Incendio	Robo	Sabotaje	Virus	TOTALES
Servidor de BD	$ 50.000,00	57,00%	10,00%	12,00%	18,00%	
		$ 28.500,00	$ 5.000,00	$ 6.000,00	$ 9.000,00	**$ 48.500,00**
UPS	$ 6.500,00	71,00%	13,00%	15,00%	5,00%	
		$ 4.615,00	$ 845,00	$ 975,00	$ 325,00	**$ 6.760,00**
Router	$ 50.000,00	45,50%	8,00%	9,00%	17,50%	
		$ 22.750,00	$ 4.000,00	$ 4.500,00	$ 8.750,00	**$ 40.000,00**
Antena satelital	$ 6.500,00	51,00%	21,00%	23,00%	0,00%	
		$ 3.315,00	$ 1.365,00	$ 1.495,00	$ 0,00	**$ 6.175,00**
PC Gerente Gral	$ 12.500,00	63,00%	7,00%	7,00%	18,00%	
		$ 7.875,00	$ 875,00	$ 875,00	$ 2.250,00	**$ 11.875,00**
						$ 113.310,00
TOTALES		**$ 67.055,00**	**$ 12.085,00**	**$ 13.845,00**	**$ 20.325,00**	**$ 113.310,00**

Escala

0 - 3	Bajo
> 3 - 7	Medio
> 7 - 10	Alto

¿Qué obtengo de un AR?

Riesgos a:

- Aceptar
- Mitigar
- Transferir

Pero NUNCA debe ser:

- Rechazado
- Eliminado
- Ignorado

Regulaciones

- Comunicación A 4609 del BCRA
- ISO/IEC 27001
- ISO/IEC 27005
- BASILEA y BASILEA II
- AS/NZS 4360:1999
- Risk IT Framework
- Ley de Sarbanes Oxley (SOX)

Metodologías AR

- CRAMM – CCTA Risk Analysis and Management Method
- MAGERIT – Metodología de Análisis y Gestión de riesgos de los sistemas de información.
- OCTAVE – Operationally Critical threat, Asset, and Vulnerability Evaluation
- NIST 800-30
- ISO/IEC 13335

Entre otros….

Y para terminar…

"Cualquier toma de decisión, es una decisión de riesgo".

"Si tomas riesgos, puedes fallar. Pero si no tomas riesgos, seguramente fallarás. El riesgo mayor de todos es no hacer nada".

"Si no sabes para donde vas, entonces cualquier camino te llevará allí".

"Asumiremos los riesgos. Lo qué siempre ha sido no siempre será, necesariamente, para siempre".