

SEGURIDAD. Curso 2023-2024

Laboratorio 6 – Gestión de Riesgos

Sesión 1

Contexto y análisis de riesgo potencial (5 puntos)

	Gestión de Riesgos	Puntos
Contexto	1. Valoración del contexto, objetivos y organigrama de la organización.	0,5
I. Análisis de riesgo potencial	2. Caracterización de 1 activo primario : - Identificación y justificación del activo. - Valoración (estimación del valor) del activo.	1
	3. Caracterización de 5 amenazas relacionadas con el activo primario: - Identificación y justificación de cada amenaza. - Valoración de la degradación de cada amenaza. - Valoración de la probabilidad de cada amenaza.	1,5
	4. Determinación del impacto potencial de las 5 amenazas sobre el activo seleccionado (en función del valor del activo y degradaciones de las amenazas).	1
	5. Determinación del riesgo potencial de las 5 amenazas sobre el activo seleccionado (en función de impacto y probabilidad).	1

1. Contexto, objetivos y organigrama

EJÉRCITO DE UCRANIA

► **Contexto**

- Entorno geopolítico volátil.
- Importancia información clasificada e infraestructura crítica.
- Aumento de la digitalización de operaciones militares.

► **Objetivos**

- Identificar y evaluar amenazas contra el país.
- Desarrollar capacidades de defensa.
- Proteger información clasificada e infraestructura crítica.
- Mejorar la resiliencia contra ataques cibernéticos.

► **Organigrama**

- Fuerzas de tierra, mar, aire y ciberespacio...

2. Caracterización 1 activo primario

► Identificación

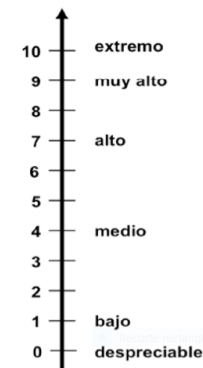
- Personal militar

► Justificación

- Fuerza kinética operativa responsable de las capacidades
- Únicos cualificados para lanzar operaciones militares

► Valoración

- Disponibilidad → Valor extremo (10)
- Integridad → Valor muy alto (9)
- Confidencialidad → Valor muy alto (9)
- Autenticidad → Valor muy alto (9)
- Trazabilidad → Valor alto (8)
- Total → Valor muy alto (9)



valor		criterio
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

3. Caracterización de 5 amenazas

► **Identificación**

1. Terremoto, inundación, tormenta o epidemia
 - Tipo natural
2. Fallo de equipamiento o infraestructura
 - Tipo industrial o defecto de fábrica
3. Ataque de ingeniería social o desinformativo
 - Tipo deliberado cibernético
4. Atentado terrorista
 - Tipo deliberado kinético
5. Error en el manejo de armas o equipamiento
 - Tipo accidental

3. Caracterización de 5 amenazas

► Degradación

- 1. Terremoto, inundación, tormenta o epidemia
 - Significativamente degradado (80%)
- 2. Fallo de equipamiento o infraestructura
 - Medianamente degradado (60%)
- 3. Ataque de ingeniería social o desinformativo
 - Significativamente degradado (80%)
- 4. Atentado terrorista
 - Totalmente degradado (100%)
- 5. Error en el manejo de armas o equipamiento
 - Parcialmente degradado (40%)

Modelación cualitativa
Pérdida del valor
Levemente degradado
Parcialmente degradado
Medianamente degradado
Significativamente degradado
Totalmente degradado

Modelación cuantitativa
Pérdida del valor
20%
40%
60%
80%
100%

3. Caracterización de 5 amenazas

► Probabilidad

1. Terremoto, inundación, tormenta o epidemia
 - Muy baja (MB)
2. Fallo de equipamiento o infraestructura
 - Baja (B)
3. Ataque de ingeniería social o desinformativo
 - Alta (A)
4. Atentado terrorista
 - Alta (A)
5. Error en el manejo de armas o equipamiento
 - Baja (B)

Probabilidad cualitativa			
Código	Probabilidad	Frecuencia	Ocurrencia
MA	Muy alto	Casi seguro	Fácil
A	Alto	Muy alta	Medio
M	Medio	Posible	Difícil
B	Bajo	Poco probable	Muy difícil
MB	Muy bajo	Muy rara	Extremad. difícil

4. Determinación de impacto potencial

- ▶ **Escala propia para impacto potencial**
 - ▶ **Muy Bajo**, **Bajo**, **Medio**, **Alto**, **Muy Alto** y **Extremo**

Impacto		Degradación				
		20%	40%	60%	80%	100%
Valor	Extremo	M	A	MA	E	E
	Muy alto	M	M	A	MA	E
	Alto	B	M	M	A	MA
	Medio	MB	B	M	M	A
	Bajo	MB	MB	B	M	M
	Despreciable	MB	MB	MB	B	M

4. Determinación de impacto potencial

► Estimación impacto potencial por amenazas

► Muy Bajo, Bajo, Medio, Alto, Muy Alto y Extremo

Impacto		Degradación				
		20%	40%	60%	80%	100%
Valor	Extremo					
	Muy alto		A5. Error manejo de armas o equipamiento Impacto p. Medio	A2. Fallo equipamiento o infraestructura Impacto p. Alto	A1. Desastre natural A3. Ingeniería social Impacto p. Muy alto	A4. Atentado terrorista Impacto p. Extremo
	Alto	Valor del activo crítico... En nuestro caso era valor <u>muy alto</u> (9)				
	Medio					
	Bajo					
	Despreciable					

5. Determinación de riesgo potencial

- ▶ **Escala propia para riesgo potencial**
 - ▶ **Muy Bajo**, **Bajo**, **Medio**, **Alto**, **Muy Alto** y **Extremo**

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	Extremo	M	A	MA	E	E
	Muy alto	M	M	A	MA	E
	Alto	B	M	M	A	MA
	Medio	MB	B	M	M	A
	Bajo	MB	MB	B	M	M
	Muy Bajo	MB	MB	MB	B	M

5. Determinación de riesgo potencial

► Estimación riesgo potencial por amenaza

► Muy Bajo, Bajo, Medio, Alto, Muy Alto y Extremo

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	Extremo	M	A	MA	A4. Atentado Terrorista <u>Riesgo p. Extremo</u>	E
	Muy alto	A1. Desastre natural <u>Riesgo p. Medio</u>	M	A	A3. Ingeniería social <u>Riesgo p. Muy alto</u>	E
	Alto	B	A2. Fallo equipamiento o infraestructura <u>Riesgo p. Medio</u>	M	A	MA
	Medio	MB	A5. Error manejo de armas o equipamiento <u>Riesgo p. Bajo</u>	M	M	A
	Bajo	MB	MB	B	M	M
	Muy Bajo	MB	MB	MB	B	M

Sesión 2

Análisis de riesgo residual (2 puntos)

	Gestión de Riesgos	Puntos
2. Análisis de riesgo residual	6. Caracterización de 5 salvaguardas actualmente activas: ▪ Justificación de inclusión de cada salvaguarda en el análisis. ▪ Valoración de la tipología y eficacia de cada salvaguarda.	I
	7. Determinación del impacto y riesgo residual de cada amenaza considerando la eficacia de las 5 salvaguardas desplegadas: ▪ Valoración de la degradación residual de cada amenaza. ▪ Valoración del impacto residual de cada amenaza. ▪ Valoración de la probabilidad residual de cada amenaza. ▪ Valoración del riesgo residual de cada amenaza.	I

6. Caracterización de salvaguardas

1. **Entrenamiento y concienciación en ciberseguridad**

- ▶ Reconocer y evitar ataques de ingeniería social
- ▶ Tipo: Concienciación Eficacia: 80%

2. **Protocolos de manipulación de equipos**

- ▶ Establecer políticas de seguridad para el manejo de equipos y armas
- ▶ Tipo: Administrativa Eficacia: 90%

3. **Sistemas de alerta temprana y vigilancia**

- ▶ Detectar sospechosos y ataques terroristas
- ▶ Tipo: Detección Eficacia: 60%

4. **Apoyo psicológico y social para el personal militar**

- ▶ Proporcionar soporte profesional ante ataques deliberados o situaciones de estrés
- ▶ Tipo: Corrección Eficacia: 70%

5. **Mantenimiento y refuerzo de infraestructuras críticas**

- ▶ Mejorar la seguridad y resistencia para reducir defectos y vulnerabilidades
- ▶ Tipo: Preventiva Eficacia: 60%

7. Impacto y riesgo residual

► Degradación residual

1. Terremoto, inundación, tormenta o epidemia

- *Apoyo psicológico y social, Mantenimiento y refuerzo de infraestructuras*
- **Significativamente degradado (80%)** → **Medianamente degradado (60%)**

2. Fallo de equipamiento o infraestructura

- *Ninguna salvaguarda reduce la degradación de esta amenaza*
- **Medianamente degradado (60%)** → **Medianamente degradado (60%)**

3. Ataque de ingeniería social o desinformativo

- *Ninguna salvaguarda reduce la degradación de esta amenaza*
- **Significativamente degradado (80%)** → **Medianamente degradado (80%)**

4. Atentado terrorista

- *Apoyo psicológico y social, Mantenimiento y refuerzo de infraestructuras*
- **Totalmente degradado (100%)** → **Medianamente degradado (80%)**

5. Error en el manejo de armas o equipamiento

- *Ninguna salvaguarda reduce la degradación de esta amenaza*
- **Parcialmente degradado (40%)** → **Parcialmente degradado (40%)**

7. Impacto y riesgo residual

- Estimación impacto residual por amenazas
 - Muy Bajo, Bajo, Medio, Alto, Muy Alto y Extremo

Impacto		Degradación				
		20%	40%	60%	80%	100%
Valor	Extremo					
	Muy alto		A5. Error manejo de armas o equipamiento Impacto r. Medio	A2. Fallo equipamiento o infraestructura A1. Desastre natural Impacto r. Alto	A1. Desastre natural A3. Ingeniería social A4. Atentado terrorista Impacto r. Muy alto	A4. Atentado terrorista Impacto r. Extremo
	Alto	Valor del activo crítico no cambia... Sigue siendo <u>muy alto</u> (9)				
	Medio					
	Bajo					
	Despreciable					

7. Impacto y riesgo residual

► Probabilidad residual

1. Terremoto, inundación, tormenta o epidemia

- *Ninguna salvaguarda reduce la probabilidad de esta amenaza*
- **Muy baja (MB) → Muy baja (MB)**

2. Fallo de equipamiento o infraestructura

- *Protocolos de manipulación de equipos, Mantenimiento y refuerzo de infraestructuras*
- **Baja (B) → Muy baja (MB)**

3. Ataque de ingeniería social o desinformativo

- *Entrenamiento y concienciación en ciberseguridad*
- **Alta (A) → Baja (MB)**

4. Atentado terrorista

- *Sistemas de alerta temprana y vigilancia, Mantenimiento y refuerzo de infraestructuras*
- **Alta (A) → Baja (MB)**

5. Error en el manejo de armas o equipamiento

- *Protocolos de manipulación de equipos*
- **Baja (B) → Muy baja (MB)**

7. Impacto y riesgo residual

- Estimación riesgo residual por amenaza
 - Muy Bajo, Bajo, Medio, Alto, Muy Alto y Extremo

Riesgo Residual		Probabilidad				
		MB	B	M	A	MA
Impacto Residual	Extremo				A4. Atentado-terrorista <u>Riesgo potencial extremo</u>	
	Muy alto	A1. Desastre natural <u>Riesgo potencial medio</u>	A4. Atentado terrorista A3. Ingeniería social <u>Riesgo residual medio</u>		A3. Ingeniería social <u>Riesgo potencial muy alto</u>	
	Alto	A1. Desastre natural A2. Fallo equipamiento o infraestructura <u>Riesgo residual bajo</u>	A2. Fallo equipamiento o infraestructura <u>Riesgo potencial medio</u>			
	Medio	A5. Error manejo de armas o equipamiento <u>Riesgo residual muy bajo</u>	A5. Error manejo de armas o equipamiento <u>Riesgo potencial bajo</u>			
	Bajo					
	Muy Bajo					



Sesión 3

Tratamiento del riesgo y análisis (3 puntos)

	Gestión de Riesgos	Puntos
3. Tratamiento de riesgos (Reducción del riesgo)	8. Evaluación y tratamiento de riesgos (se decide reducir el riesgo): - Definición de las 4 zonas de riesgo con las amenazas detectadas. - Costes y beneficios de 1 tratamiento para cada amenaza. Tratamiento de cada amenaza (evitar, reducir, transferir o aceptar) en función de costes y beneficios.	1,5
4. Análisis de riesgo residual	9. Estimación análisis del riesgo residual actualizado: - Valoración de la degradación residual de cada amenaza. - Valoración del impacto residual de cada amenaza. - Valoración de la probabilidad residual de cada amenaza. - Valoración del riesgo residual de cada amenaza.	1
5. Tratamiento de riesgos (Aceptación del riesgo)	10. Evaluación y aceptación del riesgo residual resultante.	0,5

8. Tratamiento del riesgo

► Zonas de riesgo existente en el ejército de Ucrania

Riesgo Residual		Probabilidad				
		MB	B	M	A	MA
Impacto Residual	Extremo	Zona 4 de riesgo improbable pero alto impacto				
	Muy alto		A4. Atentado terrorista A3. Ingeniería social <u>Riesgo residual medio</u>			
	Alto	A1. Desastre natural A2. Fallo equipamiento o infraestructura <u>Riesgo residual bajo</u>				
	Medio	A5. Error manejo de armas o equipamiento <u>Riesgo residual muy bajo</u>				
	Bajo					
	Muy Bajo					

8. Tratamiento del riesgo

► **Costes/beneficios de un tratamiento posible por amenaza**

1. Terremoto, inundación, tormenta o epidemia
 - *Tratamiento:* Diseño e implantación de planes de evacuación
 - *Coste/Beneficio:* Muy poco costoso y reduce significativamente la degradación
2. Fallo de equipamiento o infraestructura
 - *Tratamiento:* Contratación de servicio de mantenimiento permanente
 - *Coste/Beneficio:* Muy costoso y reduce levemente la probabilidad
3. Ataque de ingeniería social o desinformativo
 - *Tratamiento:* Despliegue de mecanismos de filtrado de phishing (firewall e IDS)
 - *Coste/Beneficio:* Costoso y reduce significativamente la degradación
4. Atentado terrorista
 - *Tratamiento:* Construcción de zonas desmilitarizadas en cuarteles
 - *Coste/Beneficio:* Extremadamente costoso y reduce significativamente la probabilidad
5. Error en el manejo de armas o equipamiento
 - *Tratamiento:* Implantación de cursos de refresco o especialización
 - *Coste/Beneficio:* Costoso y reduce levemente la probabilidad

8. Tratamiento del riesgo

► Tratamiento de cada amenaza

- | | | | |
|----|--|-----------------|------------|
| 1. | Terremoto, inundación, tormenta o epidemia | Prioridad media | MITIGAR |
| ▶ | <i>Tratamiento:</i> Diseño e implantación de planes de evacuación | | |
| ▶ | <i>Coste/Beneficio:</i> Muy poco costoso y reduce significativamente la degradación | | |
| 2. | Fallo de equipamiento o infraestructura | Prioridad media | ACEPTAR |
| ▶ | <i>Tratamiento:</i> Contratación de servicio de mantenimiento permanente | | |
| ▶ | <i>Coste/Beneficio:</i> Muy costoso y reduce significativamente la probabilidad | | |
| 3. | Ataque de ingeniería social o desinformativo | Prioridad alta | MITIGAR |
| ▶ | <i>Tratamiento:</i> Despliegue de mecanismos de filtrado de phishing (firewall e IDS) | | |
| ▶ | <i>Coste/Beneficio:</i> Costoso y reduce significativamente la degradación | | |
| 4. | Atentado terrorista | Prioridad alta | TRANSFERIR |
| ▶ | <i>Tratamiento:</i> Construcción de zonas desmilitarizadas en cuarteles | | |
| ▶ | <i>Coste/Beneficio:</i> Extremadamente costoso y reduce significativamente la probabilidad | | |
| 5. | Error en el manejo de armas o equipamiento | Prioridad baja | ACEPTAR |
| ▶ | <i>Tratamiento:</i> Implantación de cursos de refresco o especialización | | |
| ▶ | <i>Coste/Beneficio:</i> Costoso y reduce levemente la probabilidad | | |

9. Impacto residual

1. Terremoto, inundación, tormenta o epidemia

- ▶ Diseño e implantación de planes de evacuación → reduce significativamente la degradación
- ▶ Medianamente degradado (60%) → Levemente degradado (20%)

3. Ataque de ingeniería social o desinformativo

- ▶ Filtrado de phishing → reduce significativamente la degradación
- ▶ Significativamente degradado (80%) → Parcialmente degradado (40%)

Impacto residual actualizado		Degradación				
		20%	40%	60%	80%	100%
	Muy alto	<u>A1. Desastre natural</u>	A5. Error manejo de armas o equipamiento	A2. Fallo equipamiento o infraestructura A1. Desastre natural	A4. Atentado terrorista	
		Impacto r. Medio	<u>A3. Ingeniería social</u> Impacto r. Medio	Impacto r. Alto	A3. Ingeniería social Impacto r. Muy alto	

Valor del activo crítico no cambia...
Sigue siendo muy alto (9)

9. Riesgo residual

4. Atentado terrorista

- ▶ Transferencia en la protección de cuarteles → reduce significativamente la probabilidad
- ▶ Probabilidad Baja (B) → Probabilidad Muy Baja (MB)

Riesgo Residual actualizado		Probabilidad				
		MB	B	M	A	MA
Impacto Residual	Extremo					
	Muy alto	A4. Atentado terrorista ← Riesgo residual medio	A4. Atentado terrorista A3. Ingeniería social			
	Alto	A2. Fallo equipamiento o infraestructura A1. Desastre natural Riesgo residual bajo				
	Medio	A1. Desastre natural A5. Error manejo de armas o equipamiento Riesgo residual muy bajo	A3. Ingeniería social Riesgo residual bajo			
	Bajo					
	Muy Bajo					

10. Evaluación y aceptación del riesgo residual

- ▶ Siempre seguirán existiendo riesgos
- ▶ Aceptamos los riesgos actuales de la organización

Riesgo Residual actualizado		Probabilidad				
		MB	B	M	A	MA
Impacto Residual	Extremo					
	Muy alto	<u>A4. Atentado terrorista</u> Riesgo residual medio				
	Alto	<u>A2. Fallo equipamiento o infraestructura</u> Riesgo residual bajo				
	Medio	<u>A1. Desastre natural</u> <u>A5. Error manejo de armas o equipamiento</u> Riesgo residual muy bajo	<u>A3. Ingeniería social</u> Riesgo residual bajo			
	Bajo					
	Muy Bajo					

Javier Pastor Galindo <javierpg@um.es>

Gregorio Martínez Pérez <gregorio@um.es>

SEGURIDAD. Curso 2023-2024

Laboratorio 6 – Gestión de Riesgos