

Actividad 14 - Matriz de riesgos

En esta actividad vas a crear un mapa de riesgos utilizando la hoja de cálculo “Análisis de riesgos.xlsx”

1. Crear los riesgos:

A	B	C	D	E	F	G	H	I
Código	Activo	Tipo de activo	Amenaza	Tipo de amenaza	Impacto	Probabilidad	Riesgo potencial	
001	Base datos Trabajadores	Esencial. Dato de carácter personal	Divulgación de información personal de los trabajadores	Ataques intencionados. Divulgación de información. DIVULGACIÓN	CRÍTICO	ALTA	56,25	Extremo
002	Servidor	Equipamiento informático (hardware). grandes equipos	Incendio CPD	De origen industrial. Fuego. INCENDIO	CATASTRÓFICO	ALTA	75	Extremo
003	Gestión de usuarios	Servicios. gestión de identidades	Accesos no autorizados	Ataques intencionados. Suplantación de la identidad del usuario. USURPACIÓN DE DERECHO	CATASTRÓFICO	MUY ALTA	100	Extremo
004	Servidor	Software - Aplicaciones informáticas. servidor de aplicaciones	Ataque denegación de servicio	Ataques intencionados. Denegación de servicio. SATURACIÓN DEL SISTEMA INFORMÁTICO	CRÍTICO	ALTA	56,25	Extremo
005	Servidor	Equipamiento informático (hardware). grandes equipos	Corte suministro eléctrico	De origen industrial. Corte del suministro eléctrico. PÉRDIDA DE SUMINISTRO DE ENERGÍA	CATASTRÓFICO	BAJA	25	Grave
006	Servidor	Equipamiento informático (hardware). grandes equipos	Ataque malware	Ataques intencionados. Modificación deliberada de la información	CATASTRÓFICO	MUY ALTA	100	Extremo
007	CPD	Instalaciones. recinto	Incendio CPD	De origen industrial. Fuego. INCENDIO	CATASTRÓFICO	BAJA	25	Grave
008	registro entrada trabajadores	Datos / Información. datos de control de acceso	fichero dañado	De origen industrial. Corte del suministro eléctrico. PÉRDIDA DE SUMINISTRO DE ENERGÍA	CATASTRÓFICO	BAJA	25	Grave

2. Crear los controles:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
1	codigo	Activo	Amenaza	Salvaguarda	Tipo Salvaguarda	I	%I	IR	P	%P	PR	Riesgo residual			
2	001	Base datos Trabajadores	Divulgación de información personal de los trabajadores	Cifrado de base de datos	Protección de los datos/información. Cifrado de la información	7,5	15%	1,1	MÍNIMO	7,5	100%	7,5	ALTA	8,4	Tolerable
3	002	Servidor	Incendio CPD	Sistema prevención y extinción de incendios	Seguridad física – Protección de las instalaciones . Protección de las Instalaciones	10	10%	1,0	MÍNIMO	7,5	30%	2,3	MUY BAJA	2,3	Aceptable
4	003	Gestión de usuarios	Accesos no autorizados	Uso de Active Directory	Protecciones generales u horizontales. Control de acceso lógico	10	20%	2,0	MÍNIMO	10	10%	1,0	MUY BAJA	2,0	Aceptable
5	004	Servidor	Ataque denegación de servicio	ninguna		7,5	100%	7,5	CRÍTICO	7,5	100%	7,5	ALTA	56,3	Extremo
6	005	Servidor	Corte suministro electrico	Generaror-Sai	Seguridad física – Protección de las instalaciones . Aseguramiento de la disponibilidad	10	90%	9,0	CRÍTICO	2,5	100%	2,5	BAJA	22,5	Grave
7	006	Servidor	Ataque malware	Antivirus	Protecciones generales u horizontales. Herramienta contra código dañino	10	20%	2,0	MÍNIMO	10	5%	0,5	MUY BAJA	1,0	Aceptable
8	007	CPD	Incendio CPD	Sistema detección extinción de incendios	Seguridad física – Protección de las instalaciones . Protección de las Instalaciones	10	10%	1,0	MÍNIMO	2,5	100%	2,5	BAJA	2,5	Aceptable
9	008	registro entrada trabajadores	fichero dañado	restaurar copia de seguridad	Protección de los datos/información. Copias de seguridad de los datos (backup)	10	10%	1,0	MÍNIMO	2,5	100%	2,5	BAJA	2,5	Aceptable

3. Elabora mapas de riesgo potencial y residual:

RIESGO POTENCIAL						
PROBABILIDAD	10	MUY ALTA				C-003 C-006
	8	ALTA			C-001 C-004	C-002
	6	MODERADA				
	3	BAJA				C-005 C-007 C-008
	1	MUY BAJA				
RIESGO			MÍNIMO	LEVE	MEDIO	CRÍTICO
			1	3	6	8
			IMPACTO			

RIESGO RESIDUAL						
PROBABILIDAD	10	MUY ALTA				
	8	ALTA	C-001		C-004	
	6	MODERADA				
	3	BAJA	C-007 C008		C-005	
	1	MUY BAJA	C-002 C-003 C-006			
RIESGO			MÍNIMO	LEVE	MEDIO	CRÍTICO
			1	3	6	8
			IMPACTO			

4. Indica el Plan de tratamiento:

codigo	Activo	Amenaza	Nivel de riesgo	Prioridad	Tratamiento (Salvaguarda)	Descripcion tratamiento
001	Base datos Trabajadores	Divulgación de información personal de los trabajadores	Tolerable	MODERADA	Cifrado de base de datos	
002	Servidor	Incendio CPD	Aceptable	MUY BAJA	Sistema prevención y extinción de incendios	
003	Gestión de usuarios	Accesos no autorizados	Aceptable	BAJA	Uso de Active Directory	
004	Servidor	Ataque denegación de servicio	Extremo	MUY ALTA	ninguna	
005	Servidor	Corte suministro electrico	Grave	ALTA	Generaror-Sai	
006	Servidor	Ataque malware	Aceptable	MODERADA	Antivirus	
007	CPD	Incendio CPD	Aceptable	MODERADA	Sistema detección extinción de incendios	
008	registro entrada trabajadores fichero dañado		Aceptable	MODERADA	restaurar copia de seguridad	

Se pide:

1. Determina al menos 10 riesgos que afecten a los activos de una empresa ficticia sobre la que vas a realizar la gestión de riesgos (Hoja AR)
2. Elabora el mapa de riesgo potencial, indicando en qué lugar del mapa se sitúa cada uno de los riesgos (Hoja RP)
3. Para cada uno de los riesgos indicados, determina un control atenuante (salvaguarda) y como va a afectar en el Impacto y la Probabilidad de ocurrencia (Hoja GR)
4. Elabora el mapa de riesgo residual, indicando en qué lugar del mapa se sitúa cada uno de los riesgos después de aplicar las salvaguardas (Hoja RR)
5. Indica el plan de tratamiento de riesgos (Hoja PT)

Elabora un documento explicando los pasos seguidos, con capturas de pantalla y súbelo a la plataforma junto con la hoja de cálculo Análisis de riesgos.