Esquema de Seguridad – Administración de Riesgos

Etapa 1 : Identificación de Riesgos

Activo : Aplicación Exactian
Ubicación : Externo (Servidores de Amazon)

Vulnerabilidades:
- Ausencia de un gestor de contraseñas
- Ausencia de un control 'captcha' en el inicio de sesión

Amenazas:
1) Ciberataque que robe contaseñas
2) Ciberataque de ingreso de bots (DOS)

Ubicación de las Amenazas:

		Físico	Lógico
Intento de Amenaza	Accidental		
	Deliberado		Ambas

Etapa 2: Análisis de Riesgos

Rango de frecuencias (Prob. de Agresión)		Rango de Impacto (Prob. de Éxito)	
0 - 10	Baja	0 - 25	Baja
10 - 40	Media	25 - 50	Media
40 - 70	Alta	50 - 75	Alta
70 - 100	Muy Alta	75 - 100	Muy Alta

Tabla de Análisis

Amenaza	Prob. de Agresión		Prob. de Éxito		Frecuencia de Pérdida	Pérdida Potencial	Pérdida Esperada
(1)	Media	30%	Alta	70%	21%	$100k	$21k
(2)	Media	30%	Muy Alta	90%	27%	$50k	$13.5k

P/ la amenaza (1):

- Prob de agresión media (30%) porque es algo que ocurre mas o menos 4 veces al año.
- Prob de éxito alta (70%) porque se ve comprometida información sensible de los usuarios, clientes y proveedores.
- Pérdida potencial de $100K porque se corresponde con pérdida de tiempo para solucionar el problema y con el deterioro de la imágen.
- Expresión del Riesgo:
"El riesgo de que ocurra un ciberataque que robe contraseñas debido a la ausencia de un gestor de contraseñas y que esto afecte a la aplicación Exactian es de 21% y genera una pérdida anual de $21k."

P/ la amenaza (2)

- Prob de agresión media (30%) porq ocurre 4 veces al año.
- Prob de éxito muy alta (90%) porq provocaría un corte de los servicios por un tiempo indeterminado.
- Pérdida potencial de $50K porque provoca una interrupción que afecta al servicio pero no a los datos, y un deterioro de la imagen.
- "El riesgo de que ocurra un ciberataque DOS debido a la ausencia de un control 'captcha' y que esto afecte a la aplicación Exactial es de 27% y provocaría $13.5k de pérdidas anuales".

Consecuencias de la amenaza (1)

- Primarias:
  - Interrupción del servicio a corto plazo
  - Pérdida de la información o manipulación
- Secundarias:
  - Pérdida de la confianza de los clientes

Consecuencias de la amenaza (2)

- Primarias
  - Interrupción del servicio a corto/mediano plazo
  -
- Secundarias
  - Incapacidad para continuar con las funciones de control de contratistas
  - Pérdida de confianza de los clientes.

Etapa 3: Manejo del Riesgo

(1) Ciberataque que robe contraseñas

- Estrategia Genérica: Prevenir
  Implementar un gestor de contraseñas
- 1ra Línea - Prevención: ↗
  2da Línea - Detección: Mecanismo de detección de tráfico
  3ra Línea - Recuperación: Soporte técnico
- Políticas
  Permisiva: Se prohibe el uso de gestores de contraseñas externos al [redacted] de la empresa.
  Prohibitiva: Se permite recuperar la contraseña mediant