NOMBRE :SANDRA CHOQUE GARNICA

PRACTICA N°2

Producto del análisis realizado a la financiera La Caridad, se identificaron los siguientes puntos:

1. La comunicación entre el edificio principal y su única sucursal se realiza mediante fibra óptica, además que se cuenta con un segundo proveedor de servicios ISP, para evitar cortes de servicio.

2. Producto de algunos inconvenientes con la generación de reportes, se optó por comprar una solución de pago incluyendo el soporte para esta generación de reportes en tiempos y formas más optimas, dicho software agilizó de gran forma este proceso en la institución.

3. Para la administración remota de todos los switches de la red interna, se tiene habilitado el protocolo telnet para hacer modificaciones de manera rápida.

4. En los últimos seis meses, se identificaron en los registros o logs del servidor web, peticiones de conexión provenientes de direcciones Ips que de acuerdo a una revisión la gran mayoría de ellas corresponden a ip registradas para países europeos.

5. Debido a presión de la alta dirección, la aplicación móvil fue lanzada a producción, únicamente siendo testeada con pruebas de caja blanca y caja negra.

6. Ninguna de las PCs permite la utilización de memorias USB, DVDs, o cualquier tipo de medio removible sin la habilitación y revisión por le oficial de seguridad de la información.

7. Recientemente finalizó el tiempo de licencia que se cancelaba por un software (DLP) que monitoreaba el tráfico, controlando que ningún documento digital etiquetado como confidencial pueda ser enviado por email, mensajería, etc.

8. Para asignar un activo de información (PC) a un nuevo funcionario, primeramente se procede a realizar la eliminación segura de toda la información que se almacenaba anteriormente en dicha PC (formato en bajo nivel).

TAREAS

1.- Seleccionando únicamente los puntos donde se pueda suscitar un incidente, identifique las amenazas, vulnerabilidades para poder realizar un análisis de riesgos siguiendo un enfoque metódico. (Utilice los 6 pasos aprendidos en clase)

1. **Determinar el alcance**

Proceso de gestión de la Financiera la caridad

Objetivo del análisis: Identificar los riesgos de seguridad informática que afectan a la financiera caridad.

2. Identificar y valorar los activos

Telecomunicacion (fibra)

Dispositivos (Servidor)

Software(pagina web)

Personal(responsable DB)

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	importancia
ID_03	fibra	infraestructura de comunicación	Dpto. Informática	Cable (físico)	Oficinas de la finaciera	muy alto
ID_04	Pagina web	plataforma de servicios a clientes	Dpto. Informática	Sistema(lógico)	Estaciones de trabajo	alto
ID_05	personal	información sensible de la financiera	Dpto. Informática	Sistema logico	financiera	medio
ID_07	servidor	aplicaciones web institucionales	Dpto. Informática	Servidor(físico)	financiera	

Fibra => D= 5 + I=4 C= 4 =>13/3=4,33=> ALTO

Pagina web=> D= 4 + I=4 C= 4 =>12/3=4 =>ALTO

PERSONAL=> D= 5 + I=4 C= 5=>14/3=4,667 =>muy alto

servidor=> D= 4 + I=4 C= 5=>14/3=4,667 =>muy alto

3. Identificar las amenazas

Inciso	Amenaza Identificada
3	Interceptación o manipulación de comunicaciones (por uso de Telnet sin cifrado).

4	Ataques de fuerza bruta, DDoS o explotación de vulnerabilidades
5	Errores de programación no detectados, vulnerabilidades de seguridad
7	Fuga de información confidencial

4. Identificar las vulnerabilidades y salvaguardas

Inciso	Vulnerabilidad
3	Uso de Telnet**,** un protocolo inseguro que transmite datos (incluyendo contraseñas) en texto claro
4	Servidor web expuesto , sin análisis de tráfico ni bloqueo de IP sospechosas
5	Aplicación móvil sin pruebas
7	Sin herramientas para prevenir filtración de documentos importantes

5. Evaluar el riesgo

ID	Descripción del riesgo	Probabilidad	Impacto				Riesgo
			Financiero	Imagen	Operativo	Total	
3	Datos de switchs del telnet	3	4	3	3	3	**10**

3	Ataques al servidor	4	4	4	4	4	**16**
5	Errores en la app	4	4	4	3	4	**14,66**
7	Perdida de información confidencial	**3**	**3**	**3**	**4**	**3**	**10**

6. **Trata de riesgo**

Inciso	**Acción recomendada**
3	Cambiar configuración para usar SSH (protocolo seguro). Capacitar al personal en buenas prácticas.
4	Implementar Firewall/WAF, filtrar IPs extranjeras, monitorear accesos
5	Realizar pentesting, corregir vulnerabilidades encontradas, actualizar versión de la app
7	Adquirir nueva solución DLP o implementar controles manuales estrictos (restricción de envíos, auditorías internas)