Cuadro de evaluación de riesgos

Implementado desde el [fecha] hasta el [fecha]

No	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Propietario del riesgo	Consecuencia	Probabilidad	Riesgo	Controles existentes
1	*administrador del sistema*	*gerente de RRHH*	*ingeniería social*	*nivel inadecuado de conocimientos y/o concianciación de los empleados*	*gerente de RRHH*	*1*	*1*	*2*	
2									
3									
4	*ordenadores portátiles*	*usuario*	*robo*	*equipos móviles sujetos a robo*	*gerente de TI*	*1*	*1*	*2*	
5									
6									
7									

8	aplicación de software	gerente de TI	errores de aplicación	conexiones de red pública desprotegidas	gerente de TI	2	1	3	
9	aplicación de software	gerente de TI	vandalismo	control de cambio inadecuado	gerente de TI	2	0	2	
10	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
11	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	

Categorías de activos

Los siguientes son ejemplos de activos de información que se pueden encontrar en la organización.
Esta no es una lista definitiva. Cada organización debe especificar sus propios activos que sean importantes p

Personas

- Alta dirección (miembros del directorio, de la junta fiscalizadora, gerentes de unidades de negocio)
- Mandos intermedios
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Aplicaciones y bases de datos

- Software de aplicaciones (con licencia)
- Programas de distribución libre, programas compartidos
- [illegible]
- [illegible]
- [illegible]

Documentación (en papel o formato electrónico)

- Contratos
- Correspondencia con clientes y socios
- Archivos
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

TI, comunicaciones y demás equipamiento

- Ordenadores de escritorio
- Ordenadores portátiles
- CD de instalación
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

- Dispositivos PDA
- Impresoras
- Escáners
- Fotocopiadoras
- Cintas de respaldo
- Medios de almacenamiento móviles
- Equipos de medición
- Equipos de fax
- Alarmas
- Vehículos
- Tarjetas y lectoras de tarjetas
- Cajas fuertes
- Llaves

Infraestructura

- Oficinas
- Archivos
- Depósitos
- Cajas fuertes
- Gabinetes

Servicios tercerizados

- Suministro de energía eléctrica
- Vínculos de comunicación
- Mantenimiento de equipo de TIC
- Mantenimiento de sistemas de información
- Servicios de correo y mensajería
- Auditores
- Consultores
- Instituciones de supervisión

Catálogo de amenazas

La siguiente es una lista de amenazas. Esta no es una lista definitiva. Cada organización puede agreg

Modificación accidental de datos del sistema de información
Errores de aplicaciones
Explosión de bomba
Amenaza de bomba
Incumplimiento de relaciones contractuales
Incumplimiento de leyes
Falla en los vínculos de comunicación
Identidad de usuario camuflada
Daños provocados por actividades de terceros
Daños ocasionados durante pruebas de intrusión
Destrucción de registros
Deterioro de medios
Revelación de claves
Escuchas encubiertas
Fraudes
Fallas en equipos
Falsificación de registros
Incendio
Inundación
Fraude
Espionaje industrial
Intercepción de información
Interrupción del suministro eléctrico
Fuga o revelación de información
Pérdida de servicios soporte
Errores de mantenimiento
Código malicioso
Uso erróneo de herramientas de auditoría
Uso erróneo de sistemas de información
Otros desastres (causados por el hombre)
Otros desastres (naturales)
Contaminación
Ingeniería social
Huelgas
Descarga de un rayo
Ataques terroristas
Robo
Acceso no autorizado al sistema de información
Modificación no autorizada de registros
Instalación no autorizada de software
Acceso no autorizado a la red
Acceso físico no autorizado
Uso no autorizado de materiales patentados
Uso no autorizado de software
Uso de códigos no autorizados o no probados
Error de usuario

Catálogo de vulnerabilidades

La siguiente es una lista de vulnerabilidades.
Esta no es una lista definitiva. Cada organización puede agregar vulnerabilidades por situaciones esp

Sesiones activas después del horario laboral
Colocación de cables
Interfaz de usuario complicada
Claves criptográficas accesibles a personas no autorizadas
Eliminación de soportes de almacenamiento sin borrado de datos
Poderes de gran alcance
Inadecuada capacidad de gestión
Inadecuado control de cambios
Inadecuado nivel de conocimiento y/o concienciación de empleados
Mantenimiento inadecuado
Inadecuada gestión de redes
Inadecuada separación de tareas
Inadecuada supervisión de proveedores externos
Inadecuada supervisión del trabajo de los empleados
Inadecuados derechos de usuario
Información disponible para personas no autorizadas
Falta de evidencia en envío o recepción de mensajes
Falta de control en datos de entrada y salida
Inadecuada o falta de implementación de auditoría interna
Falta de validación de datos procesados
Ubicación susceptible a desastres naturales
Ubicación susceptible a pérdidas de agua
Equipamiento móvil proclive a ser robado
Redes accesibles a personas no autorizadas
Falta de desactivación de cuentas de usuario luego de finalizado el emplec
Falta de separación de entornos de prueba y operativos
Bases de datos con protección desactualizada contra códigos maliciosos
Sobredependencia en un dispositivo o sistema
Elección inadecuada de datos de prueba
Susceptibilidad del equipamiento a la humedad y a la contaminación
Susceptibilidad del equipamiento a la temperatura
Susceptibilidad del equipamiento a alteraciones en el voltaje
Única copia, sólo una copia de la información
Cuentas de usuario generadas por sistema en las que las contraseñas permanecen sin moc
Sistemas desprotegidos ante acceso no autorizado
Acceso no autorizado a instalaciones
Nivel de confidencialidad no definido con claridad
Reglas criptográficas no definidas con claridad
Reglas organizacionales no definidas con claridad
Requisitos para desarrollo de software no definidos con claridad
Reglas para control de acceso no definidos con claridad
Reglas para trabajo afuera de las instalaciones no definidas con claridad
Copiado sin control
Descargas de Internet sin control
Uso no controlado de sistemas de información

Software no documentado
Empleados desmotivados o disconformes
Conexiones de red pública sin protección
Uso de equipamiento obsoleto
Claves inseguras
Malas condiciones higiénicas