

LISTA DE VERIFICACIÓN #22

SEGURIDAD CIBERNÉTICA

He aquí un ejemplo de una lista de verificación usando un escala de 0-5 para impacto y probabilidad.

ESCALA DE IMPACTO	ESCALA DE PROBABILIDAD
0 Impact is negligible	0 Improbable que ocurra
1 Las operaciones de la empresa no son afectadas	1 Probable que ocurra menos de una vez al año
2 Las operaciones de la empresa estarán afectadas por poco tiempo, algunos gastos serán incurridos, la confianza de los clientes y del público no es afectada significativamente.	2 Probable que ocurra una vez al año
3 Gran pérdida de operaciones; el impacto en la confianza del público y la clientela es significativo	3 Probable que ocurra una vez al mes
4 El efecto es desastroso; todas las operaciones están descontinuadas por un tiempo extenso, es necesario reconstruir todos los sistemas operacionales y reemplazar los datos.	4 Probable que ocurra una vez por semana
5 El efecto es catastrófico; los sistemas mas críticos están desconectados por un tiempo extenso, los datos están irreparablemente dañados; la salud y la seguridad pública han sido afectadas.	5 Probable que ocurra diariamente

AMENAZAS	IMPACTO (0-5)	PROBABILIDAD (0-5)	TOTAL (IMPACTO X PROBABILIDAD)
AMENAZAS GENERALES			
Error humano:			
1. Destrucción accidental, modificación, revelación, o clasificación incorrecta de información.			
2. Ignorancia: conciencia inadecuada o falta de guías de seguridad, falta de documentación propia, falta de conocimiento.			
3. Volumen de trabajo: muchos o pocos administradores del sistema; usuarios bajo mucha presión.			
4. Usuarios puede que inadvertidamente den información sobre seguridad a asaltantes.			
5. Configuración incorrecta del sistema.			
6. Las normas de seguridad no son adecuadas o no son enforzadas.			
SABOTAJE			
1. Falta de honradez: Fraude, robo, desfalco, venta de información confidencial de la empresa.			
2. Manipulación social:			
<ul style="list-style-type: none"> Es posible que los asaltantes usen el teléfono haciéndose pasar por empleados para que los usuarios o administradores le den los nombres de usuarios, contraseñas, números de identificación de los módems, etc. Los asaltantes puede que persuadan a los usuarios a ejecutar programas como el "caballo de Troya". 			
3. Abusos de privilegios o confianza.			

AMENAZAS	IMPACTO (0-5)	PROBABILIDAD (0-5)	TOTAL (IMPACTO X PROBABILIDAD)
4. Uso sin autorización de terminales abiertos o computadoras personales.			
5. Mezclando datos de prueba y producción o ambientales.			
6. Introducción de "software" y "hardware" no autorizadas.			
7. Bombas de tiempo: Software programado para dañar un programa en cierto día.			
8. Errores de diseño en el sistema operacional: Algunos sistemas no fueron diseñados para tener mucha seguridad.			
9. Errores en el diseño del protocolo del internet: Algunos protocolos no fueron diseñados para tener mucha seguridad. Las debilidades del protocolo en TCP/IP puede resultar en: <ul style="list-style-type: none"> • Selección de rutas, DNS "spoofing", adivinando la secuencia de TCP, acceso no autorizado. • Sesiones secuestradas/repetición de una transacción, los datos son cambiados o copiados durante la transmisión. • Denegación del servicio debido a bombardeo ICMP. Inundación TCP_SYN. Grandes paquetes PING, etc. 			
10. Bomba lógica: Software programado para causar daño a un sistema bajo ciertas condiciones.			
11. Viruses en programas, documentos, anexos de correo electrónico (e-mail).			
AMENAZAS DE IDENTIFICACIÓN Y AUTORIZACIÓN			
1. Programas de ataque pasando como programas normales (caballos de Troya).			
2. "Hardware" de ataque pasando como "hardware" comercial normal.			
3. Asaltantes externos pasando como usuarios válidos o clientes.			
4. Asaltantes internos pasando como usuarios válidos o clientes.			
5. Asaltantes pasando como personal de ayuda y soporte.			
FIABILIDAD DE AMENAZAS AL SERVICIO			
1. Desastres naturales serios: incendio, humo, agua, terremoto, tormentas/huracanes/tornados, interrupción de servicio eléctrico, etc.			
2. Desastres naturales menos serios, de corta duración, o que causan poco daño.			
3. Desastres causados por humanos: guerra, terrorismo, bombas, disturbios civiles, elementos químicos dañinos, accidentes radiológicos, etc.			
4. Fallo de equipo debido a defectos en los mecanismos, cables, o sistemas de comunicación.			
5. Fallo de equipo debido a polvo aerotransportado, interferencia electromagnética, o electricidad estática.			

AMENAZAS	IMPACTO (0-5)	PROBABILIDAD (0-5)	TOTAL (IMPACTO X PROBABILIDAD)
<p>6. Rechazo de servicio:</p> <ul style="list-style-type: none"> • Abuso de la red cibernética: Mal uso de protocolos para confundir o despistar o engañar los sistemas. • Sobrecarga del servidor (procesos, espacio de intercambio, memoria, directorios "tmp", servicios de sobrecarga). • Bombardeo del correo electrónico. • Transferencia o recibo de Applets, controles ActiveX, macros, archivos Postscript, etc, maliciosos. 			
<p>7. Sabotaje: Daño de información deliberado y malicioso a las funciones procesoras de información..</p> <ul style="list-style-type: none"> • Destrucción física de aparatos y cables de la interfaz de la red. • Destrucción física de aparatos de computación o de sistemas de comunicación. • Destrucción de aparatos electrónicos y medios de comunicación mediante armas de radiación eletromagnéticas (pistolas HERF o EMP/T). • Robo. • Sobrecargas eléctricas o desconexión de energía eléctrica. • Virusos o gusanos. 			
AMENAZAS A LA PRIVACIDAD			
<p>1. Esuchando clandestinamente:</p> <ul style="list-style-type: none"> • Escuchando clandestinamente/ radiación Van Eck. • Adquiriendo información clandestina mediante un "clip-on", gusanos telefónicos, sensores inductivos, o. • Adquiriendo información clandestina de la red electrónica: Monitorizando datos delicados y privados que haya en la red interna sin que la persona a cargo de estos datos se dé cuenta. • Subversión del DNS para desviar correo electrónico y otra circulación. • Espiando las señales de radio. • Analizando los desperdicios en busca de documentos confidenciales, etc. 			
AMENAZAS A LA INTEGRIDAD Y EXACTITUD			
<p>1. Causantes externos de daño malicioso y deliberado a los procesos de información.</p>			
<p>2. Causantes internos de daño malicioso y deliberado a los procesos de información.</p>			
<p>3. Modificar la información deliberadamente.</p>			
AMENAZAS AL CONTROL DE ACCESO			
<p>1. Intentos de aprender las contraseñas (conseguir acceso a los archivos de contraseñas, tratar de usar contraseñas viejas, en blanco, por defecto, o esas que apenas se cambian) .</p>			
<p>2. Obtener acceso exterior a los archivos de contraseñas o rebuscando en la red Cibernética.</p>			
<p>3. Atacar programas que permitan acceso exterior a los sistemas de computadoras (puertas traseras visibles a la red interior)</p>			

AMENAZAS	IMPACTO (0-5)	PROBABILIDAD (0-5)	TOTAL (IMPACTO X PROBABILIDAD)
4. Atacar programas que permitan acceso interior a los sistemas de computadoras (puertas traseras visibles a la red interior)			
5. Módulos de mantenimiento no seguros, puertas traseras de los creadores.			
6. Módems conectados con facilidad que permitan expansión sin control de la red interna.			
7. Errores en la codificación del programa que permitan posibilidades de infiltración. (Estas infiltraciones pueden ser usadas desde el exterior. Esta amenaza aumenta según el software se complica.)			
8. Acceso físico al sistema sin autorización.			
AMENAZAS DE RECHAZOS			
1. Los recipientes de información confidencial puede que se nieguen a acusar recibo.			
2. Los remitentes de información confidencial puede que se nieguen a admitir su origen.			
AMENAZAS LEGALES			
1. Incumplimiento con los requisitos legales y regulatorios.			
2. No aceptar responsabilidad por las acciones de usuarios internos que abusan el sistema y perpetúan actos ilegales (por ejemplo, incitan el prejuicio racial, juegan a la fortuna, blanquean dinero, o distribuyen material pornográfico o de actos de violencia).			
3. No aceptar responsabilidad si un usuario interno ataca otros sitios.			