



AUDIENCIA

INTRODUCCIÓN Y ESTRUCTURA

CAPÍTULO UNO: EXPECTATIVAS

1.1 ACTIVOS

- 1.1.1 Sistemas de Información
- 1.1.2 Actores propios
- 1.1.3 Imagen y Prestigio
- 1.1.4 Productos
- 1.1.5 Bienes muebles

1.2 ENTORNO

- 1.2.1 Entorno Físico
- 1.2.2 Actores ajenos
- 1.2.3 Entorno legal: Regulaciones y Contratos

CAPÍTULO DOS: RIESGOS

- 2.1 VULNERABILIDAD, DEBILIDAD, OPORTUNIDAD
 - 2.1.1 La publicación de vulnerabilidades
- 2.2 NOMENCLATURAS
- 2.3 AMENAZAS
- 2.4 AMENAZAS TERCARIAS
 - 2.4.1 Ataques
 - 2.4.2 Accidentes
 - 2.4.3 Errores
- 2.5 AMENAZAS SECUNDARIAS
 - 2.5.1 Selección o diseño incorrecto de las medidas de seguridad
 - 2.5.2 Implantación incorrecta de las medidas de seguridad
 - 2.5.3 Defectos en las medidas de seguridad
 - 2.5.4 Operación incorrecta de las medidas de seguridad
 - 2.5.5 Defectos o ausencia de pruebas de las medidas de seguridad
- 2.6 AMENAZAS PRIMARIAS
 - 2.6.1 Organización insegura
 - 2.6.2 Responsabilidades de Seguridad mal definidas o ejercidas
 - 2.6.3 Carencia de Normativas de Seguridad
- 2.7 EL RIESGO Y SU MEDIDA
 - 2.7.1 Incidentes y su coste
 - 2.7.2 Retorno de inversión en seguridad

CAPÍTULO TRES: MEDIDAS

- 3.1 SOFTWARE Y SISTEMAS SEGUROS
 - 3.1.1 Toma de requerimientos
 - 3.1.2 Selección y Adquisición
 - 3.1.3 Análisis
 - 3.1.4 Diseño
 - 3.1.5 Construcción de software seguro
 - 3.1.6 Pruebas
 - 3.1.7 Implantación
 - 3.1.8 Mantenimiento

3.2 TÉCNICAS QUE MITIGAN AMENAZAS TERCARIAS

- 3.2.1 Eliminación de Oportunidades
- 3.2.2 Redundancia
- 3.2.3 Control de Accesos lógico y físico
- 3.2.4 Cifrado
- 3.2.5 Camuflaje
- 3.2.6 Reserva
- 3.2.7 Seguros
- 3.2.8 Inventario y Marcado
- 3.2.9 Blindaje
- 3.2.10 No hacer nada

3.3 TÉCNICAS QUE MITIGAN AMENAZAS SECUNDARIAS Y PRIMARIAS

- 3.3.1 Divulgar y Concienciar
- 3.3.2 Control de Calidad: Auditoría, Puesta a prueba, Vigilancia
- 3.3.3 Normativa
- 3.3.4 Medidas legales

3.4 TECNOLOGÍAS

- 3.4.1 Eliminación de oportunidades
- 3.4.2 Redundancia
- 3.4.3 Control de Accesos lógico y físico
- 3.4.4 Cifrado
- 3.4.5 Camuflaje
- 3.4.6 Reserva
- 3.4.7 Inventario y Marcado
- 3.4.8 Blindaje
- 3.4.9 Control de calidad

3.5 ENTORNO DOMÉSTICO

CAPÍTULO CUATRO: MODELO DE MADUREZ DE SEGURIDAD

- 4.1 NIVEL INICIO - 1
- 4.2 NIVEL RECONOCIMIENTO - 2
- 4.3 NIVEL DEFINICIÓN - 3
- 4.4 NIVEL GESTIÓN - 4
- 4.5 NIVEL ÓPTIMO - 5

ANEXOS

- 5.1 EJEMPLO DE NORMATIVA
 - 5.1.1 Política de Seguridad
 - 5.1.2 Norma de Seguridad
 - 5.1.3 Política de Uso Aceptable
 - 5.1.4 Acuerdo de Interconexión con Terceros
 - 5.1.5 Plan de Continuidad de Operaciones

- 5.2 CERTIFICACIONES DE SEGURIDAD
- 5.3 SERVICIOS COMERCIALES DE SEGURIDAD
- 5.4 PARA SABER MÁS
 - 5.4.1 General
 - 5.4.2 Pruebas
 - 5.4.3 Hackers
 - 5.4.4 Fuentes de información sobre ataques y debilidades
 - 5.4.5 Software seguro
 - 5.4.6 Directorios
 - 5.4.7 Esteganografía y Marcas de Agua
 - 5.4.8 Auditoría
 - 5.4.9 Herramientas
 - 5.4.10 Análisis forense
 - 5.4.11 Páginas crackeadas
 - 5.4.12 Autoridades de Certificación
 - 5.4.13 En español

- 5.5 EL FRAUDE 419 O NIGERIANO
- 5.6 COMPAÑÍAS DE SEGURIDAD DE LA INFORMACIÓN EN ESPAÑA