TEMÁTICA TECNICO SEGURIDAD CONTROL DE INCIDENTES

1. RECOPILAR INFORMACIÓN DE INCIDENTES DE SEGURIDAD DIGITAL SEGÚN CRITERIOS TÉCNICOS, MARCOS DE REFERENCIA Y MODELO DEL NEGOCIO.
2. FRAMEWORKS CSIRT: NIST SP 800-61 REV 2, MODELOS DE IMPLEMENTACIÓN DE CSIRT, SERVICIOS REACTIVOS, SERVICIOS CORRECTIVOS, SERVICIOS PROACTIVOS.
3. MODELOS DE ADMINISTRACIÓN Y GESTIÓN DE REDES DE DATOS: MODELO DE GESTIÓN DE REDES TMN (ITU), MODELO DE GESTIÓN DE REDES FCAPS (ISO), MONITOREO, CONTROL, NMS, MIB, AGENTE DE MONITOREO, SNMP, WMI.
4. FUNDAMENTACIÓN DEL ANÁLISIS DE RIESGOS Y VULNERABILIDADES: RIESGOS, METODOLOGÍAS DE ANÁLISIS Y EVALUACIÓN DEL RIESGO, MATRIZ DE RIESGOS, AMENAZAS, ATAQUES, VECTORES DE ATAQUE, SISTEMAS DE CLASIFICACIÓN DE VULNERABILIDADES (CVE, CWE, CAPEC), VALORACIÓN DE VULNERABILIDADES CVSS.
5. MALWARE: CONCEPTO, CLASIFICACIÓN, TAXONOMÍA (VIRUS, TROYANOS, GUSANOS, SPYWARE, RANSOMWARE, OTROS)

1. REGISTROS DE SEGURIDAD: DEFINICIÓN DE LOGS, TIPOS DE LOGS, IDENTIFICAR LOS LOGS DENTRO DE LOS DIFERENTES TIPOS DE SISTEMAS OPERATIVOS (WINDOWS, LINUX, UNIX, EQUIPOS DE SEGURIDAD, SISTEMAS DETECTORES DE INTRUSOS, BASES DE DATOS).
2. PLATAFORMAS DE AUDITORÍAS DE LOGS: NIST SP 800-92, CORRELACIONADORES DE EVENTOS, REVISIÓN DE PATRONES DE ATAQUE, METODOLOGÍAS, REVISIÓN DE ARCHIVOS DE LOGS
3. VALIDAR EL IMPACTO DE INCIDENTES DE SEGURIDAD CON BASE EN CRITERIOS TÉCNICOS Y HERRAMIENTAS DE MONITOREO DE ACUERDO CON EL MODELO DEL NEGOCIO.
4. PARAMETRIZACIÓN DE HARDWARE Y SOFTWARE: CONFIGURACIÓN DE PARÁMETROS DE HARDWARE Y SOFTWARE DE SEGURIDAD DIGITAL Y MONITOREO DE RED; ESPECIFICACIONES TÉCNICAS, ESTÁNDARES Y NORMAS DE SEGURIDAD.
5. SEGURIDAD EN SISTEMAS OPERATIVOS: SISTEMAS DE FICHERO, PERMISOS Y ATRIBUTOS EN FICHEROS, GESTIÓN DE USUARIOS Y ADMINISTRACIÓN DE GRUPOS, PLANIFICACIÓN DEL RENDIMIENTO DEL SISTEMA OPERATIVO Y CONFIGURACIÓN SEGURA, MODELOS DE CONTROL DE ACCESO: CONTROL DE ACCESO OBLIGATORIO (MANDATORY ACCESS CONTROL, MAC), MODELO DE CONTROL DE ACCESO DISCRECIONAL (DISCRETIONARY ACCESS CONTROL, DAC), CONTROL DE ACCESO BASADO EN ROLES (ROLE-BASED ACCESS CONTROL, RBAC).
6. MECANISMOS DE SEGURIDAD: CRIPTOGRAFÍA, INTRODUCCIÓN, CRIPTOGRAFÍA CLÁSICA Y MODERNA, ALGORITMOS SIMÉTRICOS, ALGORITMOS ASIMÉTRICOS, FIRMA Y CERTIFICADOS DIGITALES, DISTRIBUCIÓN DE LLAVES, TOKENS, SMATCARDS, BIOMETRÍA. APLICACIONES DE SEGURIDAD EN REDES: KERBEROS, PGP, SSH, SENSIBILIZACIÓN PARA IMPLEMENTACIÓN, PROTOCOLOS/SSL/TLS//S-MIME, PKI, IPSEC, ESTENOGRAFÍA.

1. DETECCIÓN DE INCIDENTES DE SEGURIDAD: MONITOREAR Y VERIFICAR LOS ELEMENTOS DE CONTROL CON EL FIN DE DETECTAR UN POSIBLE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN.
2. SEGURIDAD PERIMETRAL: PARAMETRIZAR FIREWALLS, NEXT GENERATION FIREWALL (NGF), APPLIANCE APLICACIÓN, FIRMA DE CONEXIONES, IDENTIFICADORES DE APLICACIONES.
3. COPIAS DE SEGURIDAD: TIPOS, INCREMENTAL, DIFERENCIAL, TOTAL.
4. AUDITORIA Y TRAZABILIDAD DE SEGURIDAD INFORMÁTICA: REALIZAR VERIFICACIONES PERIÓDICAS DEL ESTADO DE LA PLATAFORMA DE GESTIÓN DE INCIDENTES, ANTIVIRUS, GESTIÓN Y MONITOREO DE RED, COPIAS DE SEGURIDAD Y BACKUPS.
5. GESTIÓN DE EVENTOS E INCIDENTES: CIRTS, CERT, CENTROS DE GESTIÓN DE RESPUESTA A INCIDENTES, PLATAFORMAS DE MONITOREO DE EVENTOS DE SEGURIDAD, CICLO DE GESTIÓN DE INCIDENTES (PREPARACIÓN, DETECCIÓN Y ANÁLISIS, NOTIFICACIÓN, DOCUMENTACIÓN Y GESTIÓN DEL CONOCIMIENTO).
6. OPERAR HERRAMIENTAS DE CONTROL DE LA SEGURIDAD DIGITAL PARA MITIGAR LOS RIESGOS SEGÚN PROCEDIMIENTOS TÉCNICOS DE LA POLÍTICA DE SEGURIDAD DIGITAL.
7. DOCUMENTAR INCIDENTES DE SEGURIDAD DIGITAL SEGÚN CRITERIOS TÉCNICOS Y MARCO DE REFERENCIA.
8. DOCUMENTACIÓN: ESTÁNDARES Y MODELOS DE REFERENCIA PARA DOCUMENTAR PROCESOS DENTRO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
9. DOCUMENTACIÓN DE RECOLECCIÓN DE EVIDENCIAS