CONSELLO DA AVOGACÍA GALEGA

FORMACIÓN
Consello da Avogacía Galega

CURSO CIBERSEGURIDAD (30 HORAS, ONLINE)

PROGRAMA

1. INTRODUCCIÓN A LA CIBERSEGURIDAD

1.1. Presentación
1.2. Concepto
1.3. Internet
1.4. Sistemas de seguridad
1.5. Dificultades de seguridad
1.6. Tipologías delictivas I
1.7. Tipologías delictivas II
1.8. Riesgos actuales
1.9. Respuestas de seguridad
1.10. Seguridad global
1.11. Ley de Ciberseguridad 5G I
1.12. Ley de Ciberseguridad 5G II
1.13. Ley de Ciberseguridad 5G III
1.14. Consideraciones
1.15. Resumen
1.16. Bibliografía

2. INTRODUCCIÓN A LOS SISTEMAS INFORMÁTICOS Y REDES

2.1. Presentación
2.2. ARPANET
2.3. USENET
2.4. Internet
2.5. Servicio web
2.6. URL
2.7. Correo electrónico
2.8. Ciberataques puros
2.9. Conexiones de internet I
2.10. Conexiones de internet II
2.11. Lenguaje
2.12. Decimal I
2.13. Decimal II
2.14. Hexadecimal
2.15. Redes
2.16. Tipos
2.17. Clases

2.18. Dirección IP
2.19. Tipos
2.20. Protocolo TCP/IP
2.21. DNS
2.22. Dominios
2.23. Resumen
2.24. Bibliografía

3. AMENAZAS EXISTENTES EN INTERNET

3.1. Presentación
3.2. Introducción
3.3. Estrategia Nacional de Ciberseguridad 2019 I. Antecedentes y principios rectores
3.4. Estrategia Nacional de Ciberseguridad 2019 II. Líneas de acción
3.5. Ciberataques
3.6. Software malicioso o malware
3.7. Virus informáticos
3.8. Gusanos informáticos
3.9. Troyanos
3.10. Ransomware
3.11. Adware y Spyware
3.12. Spam
3.13. Ataque de denegación de servicio (DoS)
3.14. Amenazas persistentes avanzadas (APT)
3.15. Cookies
3.16. Resumen
3.17. Bibliografía

4. INGENIERÍA SOCIAL

4.1. Presentación
4.2. Origen de la Ingeniería Social
4.3. Concepto de la Ingeniería Social
4.4. Principios de la Ingeniería Social
4.5. Medios de ataque de Ingeniería Social I
4.6. Técnicas de Ingeniería Social I: Phising
4.7. Técnicas de Ingeniería Social II: Modalidades de Phising
4.8. Técnicas de Ingeniería Social III: Pretexting
4.9. Técnicas de Ingeniería Social IV: Quid pro quo, baiting, tailgating
4.10. Ingeniería Social en las redes sociales
4.11. Realización de los ataques de Ingeniería Social
4.12. Prevención de los ataques de Ingeniería Social
4.13. Resumen
4.14. Bibliografía

5. ATAQUES Y CONTROLES PARA PROTEGER ACTIVOS

5.1. Presentación
5.2. Introducción
5.3. Inventarios de activos
5.4. Política y normativa: Normativa interna
5.5. Política y normativa: Cumplimiento legal
5.6. Control de acceso
5.7. Copias de seguridad
5.8. Protección anti-malware
5.9. Actualizaciones
5.10. Seguridad de la red
5.11. Información en tránsito
5.12. Gestión de soportes
5.13. Registro de actividad: Sistemas de monitorización
5.14. Productos de ciberseguridad
5.15. Resumen
5.16. Bibliografía

6. ANÁLISIS DE VULNERABILIDADES

6.1. Presentación
6.2. Riesgos y amenazas en Internet
6.3. Vulnerabilidades y amenazas I
6.4. Vulnerabilidades y amenazas II
6.5. Procesos de análisis y gestión de riesgos I
6.6. Procesos de análisis y gestión de riesgos II
6.7. Fuga de información
6.8. Riesgo reputacional I
6.9. Riesgo reputacional II
6.10. Redes sociales
6.11. Conceptos I
6.12. Conceptos II
6.13. Fraudes
6.14. Nube
6.15. Clases de nubes
6.16. Wifis y redes externas
6.17. Resumen
6.18. Bibliografía

7. ANÁLISIS DE RIESGOS Y GESTIÓN DE INCIDENTES DESDE UNA PERSPECTIVA TÉCNICA

7.1. Presentación
7.2. Definición
7.3. Tipología de riesgos
7.4. Clasificación de riesgos
7.5. Riesgos sociales
7.6. Análisis de riesgos I
7.7. Análisis de riesgos II
7.8. Riesgo informático
7.9. Impactos de riesgos
7.10. Métodos de ataque
7.11. Herramientas de ataque I
7.12. Herramientas de ataque II
7.13. Medidas tecnológicas
7.14. Medidas humanas
7.15. Resumen
7.16. Bibliografía

8. GESTIÓN DE LOS INCIDENTES DE SEGURIDAD EN LA RED

8.1. Presentación
8.2. Ciberseguridad y establecimiento de medidas en la empresa
8.3. Incidente de ciberseguridad en la empresa I
8.4. Incidente de ciberseguridad en la empresa II
8.5. Gestión del incidente I
8.6. Gestión del incidente II
8.7. Factores de riesgo para la empresa y medidas de seguridad integrales
8.8. Comunicación adecuada y demás pasos para una respuesta eficaz
8.9. Decálogo de la gestión de la ciberseguridad I
8.10. Decálogo de la gestión de la ciberseguridad II
8.11. Decálogo de la gestión de la ciberseguridad III
8.12. Decálogo de la gestión de la ciberseguridad IV
8.13. Decálogo de la gestión de la ciberseguridad V
8.14. Seguridad, vigilancia, resiliencia y consciencia
8.15. Stakeholders y divulgación de información sobre incidentes
8.16. Resumen
8.17. Bibliografía

9. HERRAMIENTAS PARA PROTEGER LA INFORMACIÓN

9.1. Presentación
9.2. Antivirus
9.3. Antivirus de escritorio y antivirus online
9.4. Analizadores de URLs
9.5. Protección de dispositivos
9.6. Teléfonos móviles
9.7. Contraseñas
9.8. Uso y creación de contraseñas fuertes
9.9. Utilización incorrecta de contraseñas
9.10. Suplantación de la identidad
9.11. Seguridad perimetral
9.12. Sistemas IDS
9.13. Sistemas proxy
9.14. RGPD y LOPDGDD
9.15. Resumen
9.16. Bibliografía

10. CRIPTOGRAFÍA

10.1. Presentación
10.2. Modos de acceso
10.3. Criptografía
10.4. Criptosistemas
10.5. Criptografía de clave pública y de clave privada
10.6. Claves y cifrado
10.7. Criptografía de clave pública y firma digital
10.8. Problemas en el entorno de clave pública y certificado digital
10.9. Listado de firmas y cortafuegos
10.10. Funcionamiento del cortafuegos
10.11. Ejecución del cortafuegos y sus ventajas I
10.12. Ejecución del cortafuegos y sus ventajas II
10.13. Ejecución del cortafuegos y sus inconvenientes
10.14. Resumen
10.15. Bibliografía