CONSELLO DA AVOGACÍA GALEGA

FORMACIÓN
Consello da Avogacía Galega

CURSO DE CIBERSEGURIDADE

Versión xuño 2023

FORMACIÓN
Consello da Avogacía Galega

ÍNDICE

Presentación **2**

Memoria **2**

Características do curso 3
Obxectivos do curso 4
Matrícula e inscricións 4
Certificación académica 4
Equipo 5
Como estudar este curso 5
Probas 6
Foro 7

Programa do curso **8**

Presentación

O mundo vive unha das súas grandes revolucións, a revolución tecnolóxica, de fondo calado na vida dos cidadáns, que deu paso á globalización. A globalización é, por tanto, un termo directamente vinculado ás altas tecnoloxías da comunicación. Non hai un espazo máis global que o ciberespazo.

Pola súa parte, o uso das Tecnoloxías da Información e Comunicación (TICs), aínda que facilita a vida política, social, cultural e económica das persoas, potenciou os efectos da delincuencia tradicional, que atopou un novo lugar onde desenvolverse e expandir os seus efectos e, por ende, os seus beneficios.

Cuantitativamente, a ciberdelincuencia é o crime máis extendido nas sociedades avanzadas, e a impunidade é, con creces, a maior de todos os tipos penolóxicos previstos no Código penal.

A ciberseguridade é un termo que se refire ao conxunto de medidas e técnicas que teñen como obxectivo protexer os sistemas informáticos e os datos que se manexan neles, fronte a posibles ameazas ou ataques cibernéticos.

Memoria

Desde o punto de vista xurídico, a ciberseguridade consiste no conxunto de normas e principios legais que regulan a protección dos sistemas informáticos e da información que se atopa almacenada neles. Isto inclúe o tratamento e protección de datos persoais, a prevención e persecución de delitos informáticos, a responsabilidade civil en caso de vulneración de sistemas, e outros aspectos relacionados coa seguridade da información no ámbito dixital.

Os retos para a avogacía no ámbito da ciberseguridade son diversos, entre eles:

- Coñecemento técnico: para poder entender e aplicar as normas de ciberseguridade, os avogados deben ter un coñecemento sólido dos aspectos técnicos e tecnolóxicos dos sistemas informáticos.
- Actualización constante: a ciberseguridade é un ámbito que evoluciona constantemente, polo que os avogados e as avogadas deben estar ao tanto das últimas tendencias e novidades para poder aplicar adecuadamente as normas.
- Interdisciplinariedade: a ciberseguridade é un ámbito que implica a

colaboración de distintas disciplinas, como a informática, a seguridade, a privacidade e o dereito. Por iso, os profesionais da avogacía deben ser capaces de traballar en equipo con expertos doutras áreas.

- Marco normativo complexo: a regulación da ciberseguridade é complexa e diversa, o que fai que os avogados deban ter un coñecemento detallado das distintas normas e regulamentacións aplicables.
- Delincuencia dixital: o aumento da delincuencia dixital e o hacking ético esixen que os avogados teñan coñecementos sólidos na materia e mantéñanse ao tanto das novas ameazas para poder protexer adecuadamente aos seus clientes.

Polo tanto, o obxectivo deste curso é proporcionar aos avogados e ás avogadas os coñecementos necesarios para comprender os riscos da ciberseguridade e aplicar os mecanismos necesarios para protexer os sistemas informáticos e a información confidencial dos seus clientes.

Este curso, impartido polo Consello da Avogacía Galega, parte dunha colaboración coa editorial Wolters Kluwer, que puxo a disposición do Consello o seu servizo de desenvolvemento de contidos formativos especializados, permitíndonos chegar a un maior número de profesionais no ámbito territorial de Galicia.

A modalidade formativa en liña facilitará que os contidos estean dispoñibles 24/7, sen límite de tempo.

Características do curso

Extensión:	★★★★★☆☆☆☆☆
Profundidade:	★★★★★★☆☆☆☆
Flexibilidade:	★★★★★★★★☆☆

Organiza: Consello da Avogacía Galega, en colaboración cos colexios de avogados de Galicia e coa participación da editorial Wolters Kluwer.

Coordina: Secretaría Técnica CAG.

Dirixido a: profesionais da avogacía galega.

Modalidade: en liña, ou E-learning, desde a web http://avogacia.gal/formacion .

Lingua do curso: castelán.

Lingua da plataforma: castelán ou galego, configurable por cada usuario no seu perfil.

Número de horas lectivas: 30.

Prazo de matrícula: matrícula aberta até o remate do curso.

Lugar de matrícula: na aula virtual do Consello da Avogacía Galega, http://avogacia.gal/formacion.

Prezo: 30 € - Colexiados/as exercentes, non exercentes e alumnos/as do Máster da Avogacía.

Remate do curso: 15 de decembro do 2023.

Superación do curso: para a obtención do certificado é obrigatoria a superación de todos os cuestionarios do curso.

Obxectivos do curso

Capacitar aos profesionais para o desenvolvemento dun programa de cumprimento normativo penal que supoña a prevención, detección e reacción ante comportamentos delituosos.

Matrícula e inscricións

A matrícula realizarase polos propios interesados a través da plataforma formativa do Consello, http://avogacia.gal/formacion.

O pagamento da matrícula dá acceso inmediato aos contidos do curso.

Certificación académica

Este curso está homologado polo Consello da Avogacía Galega. Tras completar o estudo de todos os módulos teóricos en liña e trala superación de todos os cuestionarios de autoavaliación, poderase descargar automaticamente e imprimir un certificado cun código seguro de verificación que garante a autenticidade do mesmo.

Equipo

O equipo responsable do presente curso está formado polos seguintes profesionais:

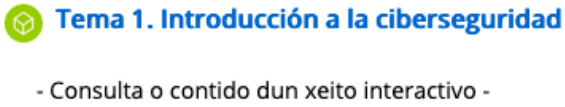
Persoa	Tarefa
JOSÉ MARÍA LOZOYA PÉREZ AVOGADO ESPECIALIZADO EN DEREITO DAS TIC Membro da Xunta de Goberno do ICA Pontevedra	**Titoría**
SERGIO ARAMBURU GUILLÁN AVOGADO Secretario técnico do Consello da Avogacía Galega	**Coordinación do curso**
VERÓNICA PAJÓN JACOBE DOCUMENTALISTA Xestora de Formación no Consello da Avogacía Galega	**Xestión e maquetación**

Como estudar este curso

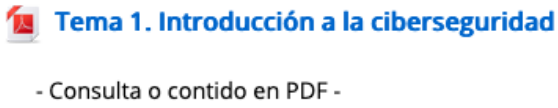
A actividade formativa será ofrecida mediante o uso da plataforma Moodle. Temas, lexislación e material de apoio en permanente actualización. Ademais, prestarase titoría en liña coas coordinadoras do curso mediante un sistema de foros.

Ao entrar na plataforma, pódense visualizar os diferentes temas organizados por pestanas. Dentro de cada un dos temas, atópanse contidos formativos de diferente tipo:

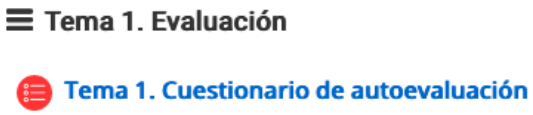
- **Formación interactiva.**



- **Formación en PDF.**



- **Cuestionarios de autoavaliación.**



Os contidos teóricos ofrécense :

- Mediante *paquetes SCORM*, que permiten seguir a formación cunha presentación guiada, con animacións e un formato máis interactivo.
- Mediante documentos en formato PDF, que se poden descargar e imprimir, pero que non permiten realizar os exercicios nin outras actividades interactivas[1].

O temario poderá complementarse con recursos documentais de apoio e/ou conferencias en liña. Informarase ao alumnado debidamente sobre cada novidade.

Probas

Ao final de cada tema se realizará unha proba de autoavaliación consistente nun cuestionario de tipo test, que se corrixe automaticamente e que debe ser aprobado para a obtención do diploma acreditativo da superación do curso. **É importante realizar unha lectura comprensiva dos temas e completar o estudo co material adicional antes da realización das probas.**

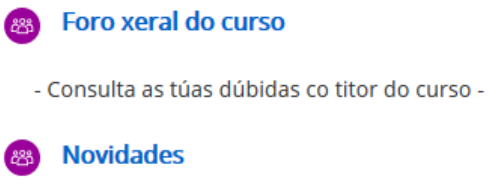
[1] Recomendamos, porén, que os materiais non se impriman porque están en permanente actualización e poden ser variados.

Foro

Os foros son unha **ferramenta de debate** onde os estudantes e as titoras poden ter conversacións extensas sen necesidade de estar conectados ao mesmo tempo.

É a través dos foros onde se deben formular as dúbidas sobre o temario, e onde se dan os debates e discusións dos temas do curso. Son unha parte esencial para o desenvolvemento do curso e constitúen espazos onde, ademais de resolverse dúbidas, serven para cambiar impresións e consultar as dificultades que cada un atope.

O alumnado dispón dun foro xeral do curso na parte xeral, na zona superior da aula virtual; aquí as titoras poderán, por exemplo, propor temas de discusión relacionados con conceptos do programa teórico e con temas de actualidade. É importante a participación do alumno/a, compartindo opinións, propoñendo temas de debate, etc.



Ademais do foro xeral, o alumno/a poderá acceder ao foro de novidades. A diferenza do primeiro, o uso deste quedará reservado a administradores e formadores do curso. Nel publicaranse novidades de interese para o alumnado, como actualización de contidos, publicación de novas de actualidade e outros recursos que se consideren relevantes.

****Na plataforma está publicado un sinxelo manual de uso no que se explica como navegar pola aula virtual e como utilizar os recursos dispoñibles**

Programa do curso

1. INTRODUCIÓN Á CIBERSEGURIDADEE

1.1. Presentación

1.2. Concepto

1.3. Internet

1.4. Sistemas de seguridade

1.5. Dificultades de seguridade

1.6. Tipoloxías delituosas I

1.7. Tipoloxías delituosas II

1.8. Riscos actuais

1.9. Respostas de seguridade

1.10. Seguridade global

1.11. Lei de Ciberseguridade 5G I

1.12. Lei de Ciberseguridade 5G II

1.13. Lei de Ciberseguridade 5G III

1.14. Consideracións

1.15. Resumo

1.16. Bibliografía

2. INTRODUCIÓN AOS SISTEMAS INFORMÁTICOS E REDES

2.1. Presentación

2.2. ARPANET

2.3. USENET

2.4. Internet

2.5. Servizo web

2.6. URL

2.7. Correo electrónico

2.8. Ciberataques puros

2.9. Conexións de Internet I

2.10. Conexións de Internet II

2.11. Linguaxe

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. Resumo

2.24. Bibliografía

3. AMEAZAS EXISTENTES EN INTERNET

3.1. Presentación

3.2. Introdución

3.3. Estratexia Nacional de Ciberseguridade 2019 I. Antecedentes e principios rectores

3.4. Estratexia Nacional de Ciberseguridade 2019 II. Liñas de acción

3.5. Ciberataques

3.6. Software malicioso ou malware

3.7. Virus informáticos

3.8. Vermes informáticos

3.9. Troianos

3.10. Ransomware

3.11. Adware e Spyware

3.12. Spam

3.13. Ataque de denegación de servizo (DoS)

3.14. Ameazas persistentes avanzadas (APT)

3.15. Cookies

3.16. Resumo

3.17. Bibliografía

4. ENXEÑARÍA SOCIAL

4.1. Presentación

4.2. Orixe da Enxeñaría Social

4.3. Concepto da Enxeñaría Social

4.4. Principios da Enxeñaría Social

4.5. Medios de ataque de Enxeñaría Social I

4.6. Técnicas de Enxeñaría Social I: Phising

4.7. Técnicas de Enxeñaría Social II: Modalidades de Phising

4.8. Técnicas de Enxeñaría Social III: Pretexting

4.9. Técnicas de Enxeñaría Social IV: Quid pro quo, baiting, tailgating

4.10. Enxeñaría Social nas redes sociais

4.11. Realización dos ataques de Enxeñaría Social

4.12. Prevención dos ataques de Enxeñaría Social

4.13. Resumo

4.14. Bibliografía

5. ATAQUES E CONTROIS PARA PROTEXER ACTIVOS

5.1. Presentación

5.2. Introdución

5.3. Inventarios de activos

5.4. Política e normativa: Normativa interna

5.5. Política e normativa: Cumprimento legal

5.6. Control de acceso

5.7. Copias de seguridade

5.8. Protección anti-malware

5.9. Actualizacións

5.10. Seguridade da rede

5.11. Información en tránsito

5.12. Xestión de soportes

5.13. Rexistro de actividade: Sistemas de monitorización

5.14. Produtos de ciberseguridadee

5.15. Resumo

5.16. Bibliografía

6. ANÁLISE DE VULNERABILIDADES

6.1. Presentación

6.2. Riscos e ameazas en Internet

6.3. Vulnerabilidades e ameazas I

6.4. Vulnerabilidades e ameazas II

6.5. Procesos de análises e xestión de riscos I

6.6. Procesos de análises e xestión de riscos II

6.7. Fuga de información

6.8. Risco reputacional I

6.9. Risco reputacional II

6.10. Redes sociais

6.11. Conceptos I

6.12. Conceptos II

6.13. Fraudes

6.14. Nube

6.15. Clases de nubes

6.16. Wifis e redes externas

6.17. Resumo

6.18. Bibliografía

7. ANÁLISE DE RISCOS E XESTIÓN DE INCIDENTES DESDE UNHA PERSPECTIVA TÉCNICA

7.1. Presentación

7.2. Definición

7.3. Tipoloxía de riscos

7.4. Clasificación de riscos

7.5. Riscos sociais

7.6. Análise de riscos I

7.7. Análise de riscos II

7.8. Risco informático

7.9. Impactos de riscos

7.10. Métodos de ataque

7.11. Ferramentas de ataque I

7.12. Ferramentas de ataque II

7.13. Medidas tecnolóxicas

7.14. Medidas humanas

7.15. Resumo

7.16. Bibliografía

8. XESTIÓN DOS INCIDENTES DE SEGURIDADE NA REDE

8.1. Presentación

8.2. Ciberseguridade e establecemento de medidas na empresa

8.3. Incidente de ciberseguridade na empresa I

8.4. Incidente de ciberseguridade na empresa II

8.5. Xestión do incidente I

8.6. Xestión do incidente II

8.7. Factores de risco para a empresa e medidas de seguridade integrais

8.8. Comunicación adecuada e demais pasos para unha resposta eficaz

8.9. Decálogo da xestión da ciberseguridade I

8.10. Decálogo da xestión da ciberseguridade II

8.11. Decálogo da xestión da ciberseguridade III

8.12. Decálogo da xestión da ciberseguridade IV

8.13. Decálogo da xestión da ciberseguridade V

8.14. Seguridade, vixilancia, resiliencia e consciencia

8.15. Stakeholders e divulgación de información sobre incidentes

8.16. Resumo

8.17. Bibliografía

9. FERRAMENTAS PARA PROTEXER A INFORMACIÓN

9.1. Presentación

9.2. Antivirus

9.3. Antivirus de escritorio e antivirus en liña

9.4. Analizadores de URLs

9.5. Protección de dispositivos

9.6. Teléfonos móbiles

9.7. Contrasinais

9.8. Uso e creación de contrasinais fortes

9.9. Utilización incorrecta de contrasinais

9.10. Suplantación da identidade

9.11. Seguridade perimetral

9.12. Sistemas IDS

9.13. Sistemas proxy

9.14. RGPD e LOPDGDD

9.15. Resumo

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 e de clave privada

10.6. Claves e cifrado

10.7. Criptografía de clave pública e firma dixital

10.8. Problemas na contorna de clave pública e certificado dixital

10.9. Listaxe de firmas e devasas

10.10. Funcionamento da devasa

10.11. Execución da devasa e as súas vantaxes I

10.12. Execución da devasa e as súas vantaxes II

10.13. Execución da devasa e os seus inconvenientes

10.14. Resumo

10.15. Bibliografía