cursos femxa.es

Xestión da seguridade informática na empresa

Curso en liña | Duración: 110 horas

Formación
con expertos na materia

Titulación
ao finalizar o curso con éxito

Gratuíto
Curso 100% subvencionado

Formación 100% subvencionada por:

XUNTA DE GALICIA | CONSELLERÍA DE EMPREGO, COMERCIO E EMIGRACIÓN

GOBIERNO DE ESPAÑA | MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL | SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE

Curso 100% gratuíto • Xestión da seguridade informática na empresa

Formación para persoas traballadoras e autónomas. Apúntate xa!

Xa podes apuntarte aos **cursos gratuítos** dirixidos a persoas traballadoras por conta allea, autónomas ou en ERTE de Galicia, cuxo obxectivo principal é mellorar as competencias e impulsar o talento profesional dos galegos e galegas co apoio continuo de titores especializados.

Esta formación impártese en **modalidade en liña** e con ela poderás:

- Ampliar coñecementos e habilidades.
- Mellorar a túa proxección laboral e mellorar o teu perfil profesional.
- Ter acceso a unha gran variedade de recursos e ferramentas para a aprendizaxe.

Esta formación está **100% subvencionada** pola **Xunta de Galicia e o Ministerio de Traballo e Economía Social.**

Obxectivo xeral do curso:

Xestionar a seguridade informática na empresa.

Todos os cursos inclúen un módulo transversal sobre igualdade de oportunidades entre mulleres e homes e sobre corresponsabilidade familiar e doméstica.

Temario

Curso de Xestión da seguridade informática na empresa

1. INTRODUCIÓN Á SEGURIDADE

1.1. Introdución á seguridade de información.

1.2. Modelo de ciclo de vida da seguridade da información.

1.3. Confidencialidade, integridade e dispoñibilidade. Principios de protección da seguridade da información.

1.4. Políticas de seguridade.

1.5. Tácticas de ataque.

1.6. Concepto de hacking.

1.7. Árbore de ataque.

1.8. Lista de ameazas para a seguridade da información.

1.9. Vulnerabilidades.

1.10. Vulnerabilidades en sistemas Windows.

1.11. Vulnerabilidades en aplicacións multiplataforma.

1.12. Vulnerabilidades en sistemas Unix e Mac OS.

1.13. Boas prácticas e salvagardas para a seguridade da rede.

1.14. Recomendacións para a seguridade da súa rede.

2. POLÍTICAS DE SEGURIDADE.

2.1. Introdución ás políticas de seguridade.

2.2. Por que son importantes as políticas?

2.3. Que debe conter unha política de seguridade.

2.4. O que non debe conter unha política de seguridade.

2.5. Como conformar unha política de seguridade informática.

2.6. Facer que se cumpran as decisións sobre estratexia e políticas.

3. AUDITORÍA E NORMATIVA DE SEGURIDADE.

3.1. Introdución á auditoría de seguridade da información e aos sistemas de xestión de seguridade da información.

3.2. Ciclo do sistema de xestión de seguridade da información.

3.3. Seguridade da información.

3.4. Definicións e clasificación dos activos.
3.5. Seguridade humana, seguridade física e da contorna.
3.6. Xestión de comunicacións e operacións.
3.7. Control de accesos.
3.8. Xestión de continuidade do negocio.
3.9. Conformidade e legalidade.

4. ESTRATEXIAS DE SEGURIDADE.

4.1. Menor privilexio.
4.2. Defensa en profundidade.
4.3. Punto de choque.
4.4. O elo máis débil.
4.5. Postura de fallo seguro.
4.6. Postura de negación establecida: o que non está prohibido.
4.7. Postura de permiso establecido: o que non está permitido.
4.8. Participación universal.
4.9. Diversificación da defensa.
4.10. Simplicidade.

5. EXPLORACIÓN DAS REDES.

5.1. Exploración da rede.
5.2. Inventario dunha rede. Ferramentas do recoñecemento.
5.3. NMAP E SCANLINE.
5.4. Recoñecemento. Limitar e explorar.
5.5. Recoñecemento. Exploración.
5.6. Recoñecemento. Enumerar.

6. ATAQUES REMOTOS E LOCAIS.

6.1. Clasificación dos ataques.
6.2. Ataques remotos en UNIX.
6.3. Ataques remotos sobre servizos inseguros en UNIX.
6.4. Ataques locais en UNIX.
6.5. Que facer se recibimos un ataque?

7. SEGURIDADE EN REDES ILANÁMBRICAS

7.1. Introdución.

7.2. Introdución ao estándar inalámbrico 802.11 – WIFI

7.3. Topoloxías.

7.4. Seguridade en redes Wireless. Redes abertas.

7.5. WEP.

7.6. WEP. Ataques.

7.7. Outros mecanismos de cifrado.

8. CRIPTOGRAFÍA E CRIPTOANÁLISIS.

8.1. Criptografía e criptoanálisis: introdución e definición.

8.2. Cifrado e descifrado.

8.3. Exemplo de cifrado: recheo dunha soa vez e criptografía clásica.

8.4. Exemplo de cifrado: criptografía moderna.

8.5. Comentarios sobre claves públicas e privadas: sesións.

9. AUTENTICACIÓN.

9.1. Validación de identificación en redes.

9.2. Validación de identificación en redes: métodos de autenticación.

9.3. Validación de identificación baseada en clave secreta compartida: protocolo.

9.4. Establecemento dunha clave compartida: intercambio de claves Diffie-Hellman.

9.5. Validación de identificación usando un centro de distribución de claves.

9.6. Protocolo de autenticación Kerberos.

9.7. Validación de identificación de clave pública.

9.8. Validación de identificación de clave pública: protocolo de interbloqueo.

Módulo transversal sobre igualdade de oportunidades entre mulleres e homes e sobre corresponsabilidade familiar e doméstica (10 horas de duración).

cursos femxa.es

Falamos?

900 100 957 (teléfono gratuíto)

hola@cursosfemxa.es

IMPORTANTE:

- Lembra que esta formación NON é bonificada, está 100% subvencionada.
- É necesario dispoñer de computador e de conexión a internet fluída para a realización destes cursos.
- Terán prioridade de praza as persoas con discapacidade.
- Hai un 10% de prazas para persoas traballadoras da Administración Pública.
- Todos os cursos inclúen un módulo transversal sobre igualdade de oportunidades entre mulleres e homes e sobre corresponsabilidade familiar e doméstica.

Formación 100% subvencionada por:

XUNTA DE GALICIA | CONSELLERÍA DE EMPREGO, COMERCIO E EMIGRACIÓN

GOBIERNO DE ESPAÑA | MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL | SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE