GAIASTECH

Programa de Capacitación | 10 horas de duración

Conéctate de xeito seguro: *ciberseguridade para PEMEs Galegas*

1, 8, 15, 22, 29/10/2025 | 16:30 – 18:30 H | ONLINE

IMPARTE:
dooingIT

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
USC Universidade de Santiago de Compostela
CECOCIB Cátedra Economía de la Ciberseguridad USC-INCIBE

FEDER Fondo Europeo de Desenvolvemento Rexional

GAIASTECH

#ProgramaDCapacitación

Conéctate de xeito seguro: *ciberseguridade para PEMEs Galegas*

1, 8, 15, 22, 29/10/2025 | 16:30 – 18:30 H | ONLINE

Quen organiza?

Programa de capacitación organizado en colaboración entre a Amtega e a Cátedra de Economía da Ciberseguridade USC-INCIBE.

CECOCIB Cátedra Economía de la Ciberseguridad USC-INCIBE

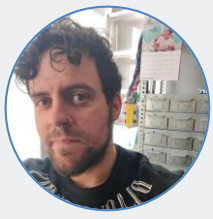
AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

Quen imparte?

dooingIT

dooingIT é unha empresa de servizos de ciberseguridade fundada en 2019 co obxectivo de democratizar a ciberseguridade e facela accesible a todo tipo de públicos, sectores e tamaños de empresa. Ademais de ofrecer servizos técnicos e normativos de ciberseguridade, dooingIT desenvolve produtos accesibles para todos, como: AKIRA, análise automática de vulnerabilidades; LeakGuard, servizo de ciberintelixencia ou Academy, programa de concienciación en ciberseguridade para todos os públicos.

Paz Cariñena



Bernardo Viqueira

FEDER Fondo Europeo de Desenvolvemento Rexional

Conéctate de xeito seguro: *ciberseguridade para PEMEs Galegas*

GAIASTECH

#ProgramaDCapacitación

1, 8, 15, 22, 29/10/2025 | 16:30 – 18:30 H | ONLINE

Obxectivos do curso

Introdución á ciberseguridade e ameazas actuais. Descubre como funcionan as ameazas cibernéticas e que podes facer hoxe para protexerte de ataques cada vez máis organizados e sofisticados.

Enxeñaría social: como nos enganan. Aprende a identificar e evitar trampas como o phishing ou o vishing, que se aproveitan da confianza humana para roubar información.

Malware: máis alá dun antivirus. Coñece como actúa o malware, os seus métodos de infección e as claves para protexerte máis aló do típico antivirus.

Ciberseguridade para PEMEs: Riscos Reais, Solucións ao Teu Alcance. Se tes unha pequena ou mediana empresa, esta sesión axudarache a protexela con ferramentas eficaces e accesibles.

Erros comúns de configuración: a porta aberta ao cibercrime. Evita as vulnerabilidades máis frecuentes revisando configuracións clave e adoptando boas prácticas que marcan a diferenza.

Tras finalizar o curso celebrarase unha sesión de titoría presencial, tamén orientada a fomentar o networking entre os participantes

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
USC Universidade de Santiago de Compostela
CECOCIB Cátedra Economía de la Ciberseguridad USC-INCIBE

FEDER Fondo Europeo de Desenvolvemento Rexional

Conéctate de xeito seguro: *ciberseguridade para PEMEs Galegas*

GAIASTECH

#ProgramaDCapacitación

1, 8, 15, 22, 29/10/2025 | 16:30 – 18:30 H | ONLINE

Para quen?

- Para o **público xeral**, **persoas traballadoras**, **empresarias** ou **autónomas** que traballen no seu día a día con **sistemas de información**. Sesión de carácter **divulgativo** orientada á **concienciación** e **boas prácticas** na **seguridade na información.**

Máis información

- **Prazas limitadas**: 15 prazas
- A capacitación é de un total de 10h, 2 horas por cada sesión
- Celebrarase unha **sesión de titoría presencial** ao finalizar a capacitación
- Para emitir un certificado de participación será **obrigatorio asistir como mínimo ao 80% das sesións.**

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
USC Universidade de Santiago de Compostela
CECOCIB Cátedra Economía de la Ciberseguridad USC-INCIBE

GAIASTECH

#ProgramaDCapacitación

1ª SESIÓN

1 DE OUTUBRO | CIBER RISCO. A QUE NOS ENFRONTAMOS

1. **Introdución ao concepto de ciber risco e formas en que poden afectar ás persoas.**
2. **Que buscan os ciber delincuentes de nós. A supply chain do ciber crime.**
3. **Os incidentes de seguridade. Tipos de incidente e boas prácticas para axudarnos a protexernos.**

Obxectivos específicos

- Esta sesión está deseñada para proporcionar ás persoas participantes unha **comprensión integral das ameazas cibernéticas actuais** e como protexernos contra elas.
- As persoas participantes aprenderán sobre as **diversas formas en que os ciber riscos poden afectar a individuos e organizacións** e a importancia de estar preparados para afrontalos.
- Exploraremos os **obxectivos dos ciber delincuentes** e que buscan obter de nós. Discutiremos como os atacantes utilizan diversas tácticas para acceder á información valiosa e os motivos detrás destes ataques. Analizaremos a "supply chain" do ciber crime e a madurez da profesionalización do malware, destacando como os ciber criminais evolucionaron e se organizaron para levar a cabo ataques máis sofisticados.
- Finalmente, abordaremos **os diferentes tipos de incidentes de seguridade** e as **medidas de protección** que se poden implementar para previr e mitigar estes incidentes. A sesión concluirá cunha discusión sobre as mellores prácticas e estratexias para manter a seguridade no entorno dixital.
- Remataremos a exposición cunha **demostración** para que os asistentes poidan ser conscientes do "preto" que temos o risco, moitas veces sen darnos conta. Inclúese a demostración da ferramenta de ciber intelixencia LeakGuard e o acceso gratuito temporal para as primeiras 5 persoas inscritas.

GAIASTECH

#ProgramaDCapacitación

2ª SESIÓN

8 DE OUTUBRO | ATAQUES DE ENXEÑARÍA SOCIAL

1. **Que son os ataques de enxeñaría social.**
2. **Tipos de ataques: phishing, vishing, smishing e outros "-ing".**
3. **Técnicas de manipulación que utilizan os ciberdelincuentes.**
4. **Identificación de sinais dun ataque de enxeñaría social e medidas de prevención.**

Obxectivos específicos

- Nesta sesión abordaremos en profundidade os **ataques de enxeñaría social**, unha das técnicas máis utilizadas polos ciberdelincuentes para manipular ás persoas e obter acceso a información confidencial ou sistemas protexidos.
- A diferenza dos ataques puramente técnicos, estes baseánse na **manipulación psicolóxica, o engano e a creación de urxencia ou medo**. Coñecer como operan estes atacantes e identificar os seus métodos é **clave para non converterse nunha vítima**. Analizaremos exemplos reais de **phishing**, **vishing**, **smishing** e outros métodos similares, explicando como recoñecer os sinais dun ataque en diferentes canles: correo electrónico, chamadas telefónicas, mensaxería instantánea ou redes sociais.
- Tamén se proporcionarán **ferramentas prácticas para responder ante un intento de fraude** e minimizar o impacto se o ataque chega a materializarse.
- A sesión rematará con **consellos de prevención e resposta**, destacando a importancia da cautela, a verificación da información e a formación continua como principais escudos fronte a estas ameazas.

GAIASTECH

#ProgramaDCapacitación

3ª SESIÓN

15 DE OUTUBRO | FALANDO DE MALWARE

1. **Conceptos básicos sobre o malware e os tipos de malware.**
2. **Métodos de infección e sinais ás que debemos prestar atención.**
3. **Boas prácticas para previr infeccións ou para responder ante unha.**
4. **Caso práctico e sesión de preguntas das persoas participantes**

Obxectivos específicos

- Nesta sesión explicaremos **que é o malware**, por que representa unha ameaza crítica para a seguridade dixital e que tipos existen, **desde virus e troianos ata ransomware ou spyware.**
- A través de **exemplos reais**, aprenderemos como estes programas maliciosos afectan tanto a sistemas como a persoas usuarias, e por que o uso dun **antivirus**, aínda sendo útil, **non é suficiente por si só**. Tamén exploraremos os **métodos máis habituais de infección** —correos electrónicos, descargas, webs comprometidas ou dispositivos USB— e os sinais que poden indicar que un sistema está comprometido.
- Ofreceranse **recomendacións prácticas para previr estas infeccións**, como manter o software actualizado, detectar comportamentos sospeitosos e saber reaccionar ante un posible ataque. A sesión incluirá un caso práctico e tempo para preguntas, co obxectivo de reforzar os coñecementos adquiridos.

GAIASTECH

#ProgramaDCapacitación

4ª SESIÓN

22 DE OUTUBRO | SOLUCIÓNS E FERRAMENTAS DE CIBERSEGURIDADE PARA PEMES

1. **A importancia da ciberseguridade en pemes**
2. **Ferramentas esenciais de ciberseguridade sen grandes investimentos**
3. **Boas prácticas e estratexias orientadas ás pemes**
4. **A concienciación como ferramenta para converternos en firewall humano**
5. **Caso práctico de uso de AKIRA como ferramenta de análise de vulnerabilidades**

Obxectivos específicos

- Nesta sesión abordaremos os **principais retos en ciberseguridade que afectan ás pequenas e medianas empresas**, que, malia compartir riscos coas grandes corporacións, contan con menos recursos para facerlles fronte.
- Analizaremos **por que as pemes son obxectivo frecuente dos ciberataques** e presentaremos **ferramentas esenciais** —moitas delas accesibles e de baixo custo— que poden mellorar a súa protección sen grandes investimentos.
- Falaremos de **solucións** como **firewalls**, **software antimalware**, sistemas de **copia de seguridade**, **detección de intrusos e autenticación multifactor**. Ademais, afondaremos en boas prácticas organizativas como a avaliación de riscos, a formación continua do persoal ou o uso de servizos na nube.
- A sesión incluirá un **caso práctico coa ferramenta AKIRA** e un informe de vulnerabilidades para as primeiras empresas inscritas, ofrecendo así recursos concretos e aplicables desde o primeiro día.

GAIASTECH

#ProgramaDCapacitación

5ª SESIÓN

29 DE OUTUBRO | TOP 10 CONFIGURACIÓNS INCORRECTAS E COMPORTAMENTOS ERRÓNEOS EN CIBERSEGURIDADE

1. **Erros habituais na configuración de sistemas e aplicacións**
2. **A importancia das persoas como barreira de protección**
3. **Exemplos prácticos e rolda de preguntas.**
4. **Inclúe informe de vulnerabilidades gratis con AKIRA para as 5 primeiras empresas inscritas.**

Obxectivos específicos

- Nesta sesión abordaremos un dos **erros máis frecuentes** pero tamén máis perigosos en ciberseguridade: as **configuracións incorrectas** e os **comportamentos inseguros**. Analizaremos como deixar opcións por defecto en aplicacións ou sistemas, ou outorgar privilexios excesivos aos usuarios, pode abrir portas para que os atacantes accedan facilmente á nosa información.
- Explicaremos **conceptos clave** como a **política de mínimo privilexio** e a necesidade dunha **revisión periódica de permisos e accesos.**
- Tamén trataremos outros **aspectos críticos** como a **falta de actualizacións**, a **reutilización de contrasinais** ou a **ausencia de vixilancia na rede,** así como o uso **correcto da autenticación multifactor (MFA).**
- A sesión pretende axudar ás organizacións a **identificar e corrixir estes erros comúns**, poñendo o foco na importancia da revisión constante e na formación das persoas como elementos centrais dunha seguridade eficaz.

GAIASTECH

#ProgramaDCapacitación

INSCRICIÓNS

1, 8, 15, 22, 29/10/2025 | 16:30 – 18:30 H | ONLINE

Información importante sobre a xestión da capacitación:

- A inscrición ao curso é de balde **por orde de inscrición.**
- **Número de prazas limitadas: 15 prazas**
- A capacitación é de un total de 10h, 2 horas por cada sesión.
- Para emitir un certificado de participación á capacitación será **obrigatorio asistir como mínimo a 80% horas das totais.**
- A asistencia será controlada ao inicio e ao remate da sesión e requirirase unha participación activa en cada sesión.

Inscríbete!