CIberTIC Galicia
Programa formativo de Ciberseguridade empresarial para a Industria 4.0

DESCRICIÓN DO CURSO

A ciberseguridade é unha das ramas tecnolóxicas que están a ter un maior auxe e da que máis se está a falar, ao decatarse todas as entidades que **un dos seus maiores valores é a información** e que, por tanto, **a mesma debe ser protexida e asegurada fronte a calquera intervención exterior**.

O presente programa formativo pretende introducir aos profesionais galegos nos principais aspectos relacionados coa ciberseguridade con respecto a temas como a protección de datos persoais ou propiedade intelectual, que afecta tanto a sociedade en xeral como, especialmente, ás entidades empresariais.

Coñecer as ameazas e posibles ataques que poden dirixirse cara os sistemas telemáticos dunha entidade, saber xestionar a seguridade dos datos na rede ou coñecer os perigos que se agochan no uso de dispositivos móbiles ou en mobilidade permitirá que as empresas acaden unha estratexia de seguridade da información que lles permita facer fronte ao crecente número de ameazas que están a xurdir, asegurando a protección dun dos bens máis prezados neste momento: a información.

PROGRAMA FORMATIVO

O curso estará formado por **9 módulos de formación cunha duración de 30h** que se complementan con **20h de talleres prácticos** en tres sesións realizadas in-company, en instalacións específicas.

Os módulos de formación serán os seguintes:

I. Introdución á Ciberseguridade na Industria 4.0 (2h)
II. Auditando a seguridade (2h)
III. Seguridade nas operacións IT (4h)
IV. Goberno da seguridade da información (4h)
V. Dominios ISO27K (4h)
VI. Marcos normativos e legais (2h)
VII. A importancia da continuidade de negocio e a xestión das incidencias (4h)
VIII. Ferramentas para xestionar a seguridade (4h)
IX. A seguridade nos programas de xestión e produción (ERP) (4h)

Os obradoiros prácticos de seguridade serán:

A. Seguridade nas redes inarámicas (5h)
B. Análise de vulnerabilidades (5h)
C. Obradoiro criptografía aplicada (10h)

PROGRAMA DETALLADO

I. Introdución á Ciberseguridade na Industria 4.0 (2h)

Moitas veces, cando se fala de ciberseguridade, o público asóciao a algo eminentemente técnico. Sen embargo, hai que recordar que a seguridade é non é un proceso que dependa exclusivamente dun departamento de informática, se non que debe partir da dirección.

No primeiro módulo do curso realízase unha introdución para conciencias de xeito xeral sobre a seguridade, e realmente ver a importancia desta materia na nova industria conectada, pero tendo en conta os requirimentos organizativos a nivel xeral.

Os contidos serán:

- Que é a seguridade da información
- Consecuencia da falta de seguridade
- Riscos habituais en correos, contrasinais, smartphones...
- Riscos en enxeñería social

II. Auditando a seguridade (2h)

Un dos puntos chave que existe á hora de asegurar un sistema é evidenciar aquelas debilidades que este teña, para así poder traballar segundo un modelo de mellora continua.

A auditoría axuda a que persoal independente e especializado detecte riscos que nós non veríamos por nós mesmos.

Os contidos serán:

- Ciclo PDCS
- Tipos de auditoría
- Métodos de auditoría
- Entendendo un informe de auditoría

III. Seguridade nas operacións IT (4h)

Aínda que a seguridade é unha necesidade global, e non debe estar supedita a IT, non se pode concibir a seguridade da información sen a seguridade informática. Por iso é necesario dar uns conceptos da seguridade nos procesos de IT, xestión de contas, etc.

Os contidos serán:

- Desenvolvemento de aplicacións
- Seguridade en redes
- Xestión de usuarios
- Outros procesos

IV. Goberno da seguridade da información (4h)

É importante entender que a seguridade ao 100% non existe. A misión dos profesionais en seguridade non é ter unha rede e seguridade asociada perfectas, se non xestionar da forma máis eficiente os recursos dispoñibles para reducir riscos detectados para o negocio.

Neste módulo preténdese introducir os conceptos de xestión da seguridade, modelo de xestión de riscos e aplicación en seguridade, tanto dende o punto de vista teórico, coma dende a experiencia práctica de aqueles que o fan coma actividade diaria.

Os contidos serán:

- Introdución ao valor da información, un ben intanxible
- Análise de Riscos
- Goberno e Organización
- Sistema de Xestión da Seguridade da Información
- Políticas, procedementos, guías e normas. Marco Normativo
- Metodoloxías e ferramentas. Normativas ISO

V. Dominios ISO27K (4h)

Dentro da Seguridade da Información, o marco común máis usual en Europa é a ISO 27001. Esta norma certificable axuda a que unha compañía controle os seus riscos de xeito global e poda implementar un Sistema de Xestión de Seguridade da Información (SXSI).

Os contido serán:

- Introdución á ISO 27001 e ás boas prácticas (ISO 27702)
- Seguridade organizativa
- Seguridade física
- Seguridade Legal
- Seguridade Técnica
- Certificación

VI. Marcos normativos e legais (2h)

Un punto crítico e que pode supoñer un gran prexuízo económico é o incumprimento de certos marcos normativos e lexislacións que nos apliquen no eido industrial.

O Regulamento Xeral de Protección de Datos (RXPD) da Unión Europea constitúe un fito na normativa sobre a protección do dereito fundamentar á intimidade e, concretamente, sobre a protección das persoas físicas no tratamento e circulación dos seus datos persoais. O seu incumprimento pode chega a acarrear sancións de ata 20 millóns de euros ou un 4% da facturación global da organización afectada.

Ademais, existen outras regulacións (coma a LSSI) e que moitas veces se descoñecen a pesar de ser de obrigado cumprimento para aquelas empresas que realicen actividades económicas por Internet ou outros medios telemáticos.

Os contidos serán:

- Principios RXPD
- Medidas de seguridade: privacidade por deseño e por defecto
- Notificación de brechas de seguridade
- Avaliación de riscos
- Transferencias internacionais de datos

VII. A importancia da continuidade de negocio e a xestión das incidencias (4h)

A continuidade de negocio é unha temática que preocupa moito nunha rede industrial, pero que poucas veces se xestiona de xeito correcto.

É moi importante ter definido o nivel de risco onde nos queremos posicionar. A pesares de que en todo risco se agocha un nivel de incertidume , existen métodos que nos axudan a reducir o nivel de incógnita dos nosos escenarios.

Do mesmo xeito, debemos asegurarnos de que os nosos procesos de continxencia estean aliñados ás necesidades de negocio, xa que o máis común é que as copias de seguridade establecidas non cumpran cos parámetros necesarios.

Está claro que aplicar a continuidade de negocio é algo que ninguén quere que pase pero debemos estar preparados para a catástrofe.

Os contidos serán os seguintes:

- Análise de impacto
- Plan de continuidade de negocio
- Xestión de incidencias

VIII. Ferramentas para xestionar a seguridade (4h)

A seguridade ten diversas frontes que requiren dun grao de especialización alto. É por isto polo que existen diversas ferramentas que nos axudarán nesta tarefa se nos apoiamos nas mesmas.

Neste módulo faremos un repaso polas máis comúns, destacando exemplos da súa utilización.

Os contidos son:

- A importancia da automatización na seguridade da información
- Ferramentas para xestionar a seguridade
- Xeración de reports e cartas técnicas
- Caso práctico

IX. A seguridade nos programas de xestión e produción (ERP) (4h)

Son cada vez máis as empresas que buscan aplicación de xestión integrada que lles permitan realizar e controlar operación da organización de xeito centralizado e integrado.

O área de produción é unha das áreas con maior dependencia de sistemas de información e de xestión.

O termo ERP ven das palabras en inglés Enterprise Resource Planning e está fortemente ligado á planificación de recursos para levar a cabo a produción de produtos nas empresas.

A seguridade nos sistemas de información é un dos aspectos máis importantes en ciberseguridade, pero coa chegada da Industria 4.0, a conexión e integración de fábricas e incluso de elementos e produtos (Internet das Cousas, IoT) é maior que nunca. A falta de seguridade no deseño destes elementos está a provocar unha situación de grandes riscos que se ven reflectidos en incidentes reais ao noso redor.

Os contidos serán os seguintes:

- Introdución á seguridade nos ERP
- Acesos nun ERP, ¿como se xestionan?
- ¿Que é un risco? ¿Como o avaliamos? Tipos de riscos
- Principais problemas de seguridade nun ERP

A. [Workshop práctico] Seguridade nas redes inarámicas (5h)

Un dos principais puntos de aceso ás redes informáticas de empresas son as redes inarámicas. Coñecer as súas principais vulnerabilidades axúdanos a asegurar as nosas redes e evitar que podan penetrar nos nosos sistemas.

Neste workshop realizarase unha simulación dun test de intrusión dobre redes inarámicas, onde se explicarán os riscos que entrañan as vulnerabilidades técnicas e se explotará un escenario de demostración.

Para que o taller sexa o máis realista posible, proporcionarase un escenario máis similar a un entorno produtivo.

A pesar de que non é necesario ter coñecementos previos de Pentesting, os asistentes deberán ter un perfil técnico mínimo e entender conceptos coma DMZ, IP, vulnerabilidade. Tamén é recomendable contar con coñecementos co sistema operativo Linux a nivel usuario.

Os contidos serán:

- Atacando WEP
- Atacando WPA2
- Atacando portais cautivos
- Atacando RADIUS

B. [Workshop] Análise de vulnerabilidades (5h)

As vulnerabilidade técnicas son un dos principais problemas de seguridade da información nas organizacións.

Este workshop amosará como realizar unha análise automatizada para detectar as vulnerabilidades existentes de diferentes sistemas. Ademais, explotarase algunha das detectadas.

Para que o taller se poda aproveitar ao máximo, proporcionarase unha contorna virtual previamente configurada.

A pesar de non ser necesario ter coñecementos previos de Pentesting, os asistentes deben ter un perfil técnico mínimo, e entender conceptos coma exploi, IP ou vulnerabilidade.

Os contidos serán:

- Programas para analizar vulnerabilidades
- Instalando e configurando un escáner de vulnerabilidades
- Lanzamento do escáner
- Interpretación dos resultados de OpenVas
- Explotación de vulnerabilidades

C. Obradoiro de criptografía aplicada (10h)

O principal activo dunha empresa é a información. Sobre todo a información confidencial, que é a que máis valor ten. é importante saber protexer a información, tanto na súa integridade coma na súa visualización, porque non queremos que ninguén non autorizado a lea e faga cambios.

Estas sesións ensinarán aos alumnos a protexer tanto a integridade da información coma a súa visualización. Amosarase o valor da criptografía para entendela e saber que se debe aplicar en cada caso de uso e describiranse exemplos actuais que son posibles gracias á criptografía. No son necesarios coñecementos previos de ningún tipo, aínda que se verán algúns conceptos básicos de matemáticas que se repasarán nas sesións.

Dúas sesións prácticas de 5h de duración:

- Sesión 1:
  - Introdución á criptografía
  - Algoritmos de clave simétrica e funcións unidireccionais (DES, AES, Funcións Hash)
  - Algoritmos de clave asimétrica (Diffie-Hellman, RSA)
- Sesión 2:
  - Firma electrónica e certificados dixitais
  - Procesado de datos seguros (ElGamal, HSMs)
  - Criptografía en Blockchain

DATAS E LUGAR DE CELEBRACIÓN

O programa formativo **desenvolverase ao longo dos meses de setembro e outubro, os martes e xoves en horario de tarde**:

- 11 de setembro: módulos I e II
- 13 de setembro: módulo III
- 18 de setembro: módulo IV
- 20 de setembro: módulo V
- 25 de setembro: módulo VI
- 27 de setembro: módulo VII
- 2 de outubro: módulo VIII
- 4 de outubro: módulo IX
- Sesións prácticas:
    - 9 de outubro (A)
    - 11 de outubro (B)
    - 23 e 25 de outubro (C)

Os **módulos teóricos desenvolveranse en Santiago de Compostela**; os **módulos prácticos**, desenvolveranse nas instalacións do **Centro Tecnolóxico Gradiant en Vigo**. Para estas últimas sesións, pedirase ao alumnado contar co seu propio equipo informático para facer prácticas sobre o mesmo.

ALUMNADO

As prazas do programa formativo terán como destinatario principal ao **persoal técnico dedicado á seguridade da información nas entidades integradas no Clúster TIC Galicia en particular e outros sectores con interese nesta temática en xeral.** É imprescindible que os alumno sexan persoal dunha peme galega (traballador por conta allea, autónomo dependente, fundador...). Estes profesionais serán, principalmente, os encargados de crear a estratexia de seguridade da información nas súas entidades ou, no seu defecto, actual coma futuros expertos ante outras entidades.

Dado que as prazas son limitadas, realizarase un proceso de selección entre os alumnos inscritos, sempre que se superen as prazas dispoñibles, seguindo os seguintes criterios:

- Relación entre o posto de traballo e a temática do curso: peso máximo, 30%
    - Entidades TIC: 50 puntos
    - Entidades pertencentes a sectores industriais estratéxicos, segundo os definidos na Axenda de Competitividade do IGAPE: 35 puntos
    - Outras entidades e sectores: 20 puntos
- A igualdade de oportunidades entre homes e mulleres: peso máximo, 20%; o ratio calcularase segundo o ratio de inscritos
- Acceso preferente a discapacitados: peso máximo, 20%. Outorgarase 20 puntos en caso de acreditar algún tipo de discapacidade, e 0 en caso contrario.

O 30% restante calcularase mediante criterios coma a data e hora de inscrición, co gallo de evitar puntuacións duplicadas.

CUSTE

O presente programa formativo está co-financiado polo programa do Instituto Galego de Promoción Económica (IGAPE) IG229 - AXUDAS A PROXECTOS DE FORMACIÓN INDUSTRIA 4.0 (2017).

O **custe por alumno** será de **355€**.

PRAZOS

- **Pre-inscrición e reserva de praza:** ata o venres 3 de agosto
- **Matrícula*:** do 27 de agosto ao 7 de setembro
- **Comezo do curso:** martes 11 de setembro

** En caso de non cubrir o 100% das prazas no período de pre-inscrición ou reserva de praza, permitirase inscrición e matrícula ata esta data*

Nota: por criterios de selección, recoméndase a pre-inscrición e reserva de praza no menor tempo posible.

MÁIS INFORMACIÓN, PRE-INSCRICIÓN E CONTACTO

A pre-inscrición realízase on-line a través do seguinte formulario:

https://goo.gl/forms/f8KB7SHic0aVmJFp1

En caso de dúbida, contactar co CLUSTER TIC GALICIA

CENTRO DE EMPRENDEMENTO CREATIVO (CEM)
Cidade da Cultura, Monte Gaiás, s/n
15707 – Santiago de Compostela

info@clusterticgalicia.com – 881 939 651

SOBRE O PROVEDOR DE SERVIZO

Inprosec naceu coa meta de ofrecer unha solución de calidade nun novo mercado xurdido dunha necesidade incipiente: a seguridade de la información.

Os seus consultores e xestores de proxectos están certificados en fundamentos de Prince2 e ITIL, que son a base da súa metodoloxía de traballo.

Mediante a selección e formación dun equipo de consultores altamente cualificados e comprometidos, Inprosec ofrece un servizo de calidade de solucións de seguridade, traballando da man con grandes compañías tanto nacionais e internacionais.

Gradiant é un dos centros tecnolóxicos TIC de referencia en Galicia, que ten por obxectivo incorporar a súa visión e coñecemento en tecnoloxías de comunicación aos procesos e produtos que as empresas desenvolvan. Aportan o seu expertise dende o punto de vista da conectividade, a intelixencia e a seguridade para traballar man a man coa industria da súa contorna.

XUNTA DE GALICIA
UNIÓN EUROPEA
igape
galicia

Programas formativos para traballadores
Industria 4.0

Operación cofinanciada pola Unión Europea
Programa Operativo FSE Galicia 2014-2020

Conseguir formación e un emprego de calidade
O FSE inviste no teu futuro