Formación y Competencias en Ciberseguridad

Dr. Víctor A. Villagrá

Director Máster Ciberseguridad UPM

Dpto. Ingeniería Telemática – ETSIT- UPM

victor.villagra@upm.es

POLITÉCNICA

ETSIT UPM

Who am I

- Docencia e Investigación en el área de ciberseguridad desde 1998.
- Diseño, coordinación e impartición de las asignaturas de ciberseguridad en:
  - Grado de Ingeniería de Tecnologías y Servicios de Telecomunicación
  - Máster Universitario en Ingeniería de Telecomunicación
  - Máster Universitario en Ingeniería de Redes y Servicios Telemáticos
  - Másteres Propios de la Universidad Politécnica de Madrid
- Diseño y Coordinación de Másteres de Ciberseguridad:
  - Máster UPM / ISMS-Forum en Dirección y Gestión de la Seguridad en la Información (2007-2016)
  - Máster Universitario en Ciberseguridad (2017 - ….)
- Más de 100 árticulos y ponencias en congresos:
  - https://scholar.google.com/citations?hl=es&user=kjqhtEsAAAAJ
- Investigador principal en proyectos de ciberseguridad:
  - Públicos: Plan Nacional I+D / Unión Europea
  - Privados: MCCE / EDA / ENISA / Empresas (INDRA/Telefónica/….)

El talento en Ciberseguridad

La falta de talento de ciberseguridad afecta a tres de cada cuatro empre

Actualidad 16 MAY 2019

Las empresas luchan contra la falta de talento en ciberseguridad

Por **redaccion_cuadernosdeseguridad** - 27 marzo, 2019

La continua y la perjudicial escasez de talento en ciberseguridad ha llevado a la mayoría de las

El experto en ciberseguridad, Adolfo Hernández, explica el panorama actual del sector

Inicio » Comunicación » Comunicados CCN-CERT

Conseguir talento en ciberseg

Detalles
Publicado: 07 Marzo 2019

- Ciberseguridad
- mujer

- La participación de la mujer es clave pa
- El sector laboral de la ciberseguridad e conseguir profesionales cualificados e
- Solo el 11% de los profesionales en cib

El déficit de talento en ciberseguridad incrementa los riesgos digitales de las empresas

Redacción Interempresas 06/03/2019 762

Contar con capital humano cualificado es imprescindible para potenciar el sector de la ciberseguridad. Se prevé que para el 2022 serán necesarios en Europa 350.000 perfiles de experto en ciberseguridad. Asimismo, el especialista en ciberseguridad puede venir de diferentes disciplinas académicas; no necesariamente son ingenieros o expertos en sistemas. Cuidar de la ciberseguridad se ha convertido en un factor clave que dota de confianza y buena reputación a las empresas.

El talento en Ciberseguridad

- ¿De verdad no hay talento? ¿O hay otros factores?

El salario medio bruto de estos profesionales alcanzó en 2017 los 32.640 euros, mientras que la media de las

DIFICULTAD PARA CUBRIR VACANTES

Guerra en el Ibex por el talento 'millennial': 100.000€ al año por los perfiles tecnológicos

Bancos

EL CHIVATO

Éstos son los “mimados” de Deloitte

Pues bien. El Chivato ha escuchado que existe una excepción, al menos en una de las ‘Big Four’. Se trata de **Deloitte**, de cuya sede salen puntualmente cada día, a las siete de la tarde, los consultores del **departamento de Ciberseguridad.**

Al parecer, los directivos de la empresa **cuidan especialmente de estos empleados**, a quienes no les exigen que permanezcan más horas en la oficina de las estipuladas por contrato.

Formación en Ciberseguridad

- Dónde se genera el talento en ciberseguridad:
  - Formación Reglada Oficial
  - Formación no reglada
  - Auto-formación
  - Una mezcla de las anteriores
- Formación Reglada:
  - Universidad
  - Formación Profesional
- Formación no reglada:
  - Certificaciones
  - Academias / Otros centros de formación
  - Cursos on-line, MOOCs, etc.
- Auto-formación:
  - Gran cantidad de información y recursos en Internet

Formación Universitaria en Ciberseguridad

- Que ofrece la universidad?
  - Grados generalistas en TIC
  - Másteres generalistas en TIC
  - Másteres especializados
- Grados/Máster Generalistas: Informática/Telecomunicación
  - Suficientemente formados y con capacidad de adaptación
  - Tienen la base necesaria en todos los aspectos de Ciberseguridad:
    - Informática, arquitecturas hardware y software.
    - Sistemas Operativos
    - Programación, Análisis y Diseño Software.
    - Redes de Comunicación. Internet. Aplicaciones y Servicios.
  - **Generan talento**: adaptación muy pequeña

Formación Universitaria en Ciberseguridad

- Máster Especializado:
  - Específico de Ciberseguridad
  - Habilidades y capacidades básicas adquiridas en Grado
  - Máster: conceptos y tecnologías utilizadas en la actualidad.
  - Formación absolutamente práctica.
- **Generan talento** de aplicación inmediata

Certificaciones en Ciberseguridad

- Orientadas a profesionales
  - Demostrar una especificación en determinados campos de las TIC
  - Usado por la industria para establecer un estándar de formación y habilidades requeridas en seguridad
- Organismos principales
  - (ISC)$^{2:}$ CISSP, etc.
  - ISACA: CISA, CISM, ec.
  - GIAC (SANS Institute)
  - EC Council: CEH, ENSA, etc.
  - CompTIA
  - ISMS Forum: CDDP, CSSK, etc.
  - ISECOM: OPST, etc.
  - MILE2: CCISO, etc.
  - Otras: Microsoft, Cisco, etc.

Competencias en Ciberseguridad

- ¿Y qué tiene que saber un profesional de la Ciberseguridad?

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

2019

LÍNEA DE ACCIÓN 5

Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.

5. Actualizar, o en su caso desarrollar marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral.

6. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.

7. Impulsar la inclusión de perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público.

8. Detectar, fomentar y retener el talento en ciberseguridad, con especial atención al campo de la investigación.

Competencias en Ciberseguridad

- Aspectos claves para la formación en Ciberseguridad:

AMENAZAS: KNOW YOUR ENEMY

Motivación: conocer las amenazas y los atacantes

Objetivos de ataque

Mecanismos tecnológicos/humanos

Consecuencias

PLANIFICACIÓN Y GOBIERNO

Diseño de una Política de Ciberseguridad.

Análisis y Gestión de Riesgos

Cumplimiento Legislativo/Normativo

Buenas Prácticas y Estándares SGSI

Certificación y Auditoría de Políticas

TECNOLOGÍAS DE CIBERSEGURIDAD

Entender fundamentos, objetivo y funcionamiento

Elegir tecnología para tu política, no al revés

Tecnologías para todas las áreas:

- Entornos IT: sistemas, redes, datos
- Cloud, IoT, Industria 4.0, Radio, etc.

OPERACIÓN DE CIBERSEGURIDAD

Despliegue de Procesos y Procedimientos: SOC

Monitorización, Reacción

Planes de Contingencia

Formación, Ejercicios

Hacking ético

Análisis Forense

Ingeniería Inversa

Inteligencia de Amenazas

Habilidades horizontales:
Dirección y liderazgo, Fundamentos y Conceptos Empresariales, etc.

KNOW YOUR ENEMY

- Entender los actores, motivos y técnicas y herramientas usadas por los atacantes
- Dos principales tipos de amenazas:
  - Amenazas Humanas: la persona es el eslabón más débil
    - Técnicas de Ingeniería Social
  - Amenazas Tecnológicas
    - Aprovechando fallos del software o de su configuraciones
- Mejor estrategia: evitarlas
  - Formación de usuarios
  - Seguridad en el ciclo de vida del software

- Diseño de una completa Política de Ciberseguridad para la organización
  - Análisis y Gestión de Riesgos
  - Cumplimiento Legal: GDPR, etc.
  - Organización, procesos y procedimientos
    - Estándares de SGSI
  - Continuidad de Negocio
  - Formación, etc.
- Plan Director de Ciberseguridad

PLANIFICACIÓN Y GOBIERNO

SERVICIOS DE CIBERSEGURIDAD

- Objetivo: entender la tecnología actual de servicios de Ciberseguridad
  - Que se adapte a tu política y necesidades (y no al revés)
- Cómo proteger tus activos:
  - Infraestructura IT, pero también…
    - Comunicaciones
    - Recursos en la Nube
    - Dispositivos Industriales
    - Dispositivos IoT

OPERACIÓN DE CIBERSEGURIDAD

- Despliegue de los procesos de ciberseguridad
  - Monitorización completa de eventos e incidentes
  - Inteligencia de Amenazas: Compartición de conocimiento
  - Análisis de situación (awareness)
  - Planes de Respuesta a Incidentes
  - Planes de Recuperación (resiliencia)

Formación y Competencias en Ciberseguridad

Dr. Víctor A. Villagrá

Director Máster Ciberseguridad UPM

Dpto. Ingeniería Telemática – ETSIT- UPM

victor.villagra@upm.es

POLITÉCNICA

ETSIT UPM