Catálogo de Servicios y Soluciones de Ciberseguridad onTech 2023

onTech INNOVATION

EL CLÚSTER TECNOLÓGICO Y BIOTECNOLÓGICO DEL SUR DE EUROPA

ÍNDICE

SERVICIOS 03

SOLUCIONES 08

SERVICIOS

• Ciberseguridad Estratégica

- Plan Director de Seguridad
  Virtual CISO
- Consultoría Especializada
  Diseño de Arquitecturas
  Seguras Seguridad en Cloud
- Análisis de riesgos y vulnerabilidades.
  Gestión de riesgos y bastionado de
  sistemas.
- Implementación de Sistema de Gestión de Seguridad de la Información (SGSI), adecuación a la normativa ISO 27001.
- Esquema Nacional de Seguridad (ENS).
- Creación de un Sistemas de Gestión de la Continuidad del Negocio (SGCN) bajo la norma ISO 22301.

• Legal

- Auditoría de cumplimiento de la normativa aplicable y detección y valoración de riesgos legales
- Privacidad desde el
  diseño. Cumplimiento
  normativo
  - LSSI
  - ENS
  - SGSI
  - Otra normativa aplicable.
- Protección de datos
  - RGPD

• Ciberseguridad Preventiva

(Diagnóstico de Seguridad Interno / Externo Legal y Técnico / Emisión de Informe)

- Informes de Exposición Corporativa & Directivos (¿Reputación Digital?) Auditorías de Seguridad Informática.
- Análisis de
  Aplicaciones. Análisis
  de Dispositivos.
- Análisis de riesgos legales / cumplimiento
  normativo. Auditoría Página Web.
- Simulación de ataques.

• Ciberseguridad Reactiva

(Análisis del incidente de seguridad / Emisión de Informe)

- **Respuesta a incidentes Análisis Forense Informático.**
- **Análisis de Vectores de Intrusión.**
- **Análisis cumplimiento obligaciones legales relativas a los incidentes y brechas de seguridad.**

• Ciberseguridad gestionada

(Soporte y Mantenimiento)

- **Monitorización activa de Infraestructura con sistemas SIEM (Security Incidents and Events Manager).**
- **Investigación y tratamiento de incidentes de seguridad tecnológica. Servicios Gestionados de Ciberseguridad**
  - **Servicio Correctivos / Evolutivos / Preventivos**
- **Servicio de SOC**

• Formación y concienciación

(Formación y Concienciación en Ciberseguridad y Protección de datos)

1. **Productos bajo licencias (distribución en formato Scorm 1.2 o 2004, Aplicación móvil (SaaS) o LMS PC (SaaS)**
   a. Programa de Ciberseguridad y protección de datos **que integra la concienciación y formación en los procedimientos y tratamiento de datos, de acuerdo al Reglamento Europeo y la generación de hábitos para evitar las brechas de seguridad, espionaje, suplantación de identidad, robo de credenciales, etc.**

Audiencia

- Empresas de Telecomunicaciones.
- Entidades de Crédito.
- Aseguradoras y Reaseguradoras.
- Centros Sanitarios y Docentes.
- Empresas con infraestructuras críticas.
- Administraciones Públicas
- Cualquier empresa que quiera proteger sus datos.

Temáticas**

- ¿A quién le importan tus datos?
- ¡Protección contra el Phishing!
- ¡Protección contra la Ingeniería Social!
- ¡Protección de Equipos!
- ¡Protección del Software!
- ¡Protección de las Comunicaciones, Redes Sociales y Dispositivos Móviles!

b. Programa de concienciación en Neurociberseguridad **que facilitan un diálogo entre la neurociencia a través de los procesos cognitivos (neurociencia cognitiva) y la seguridad en el ámbito digital para empoderar a los usuarios desde el autoconocimiento (rasgos de personalidad y sesgos cognitivos) que les permita conocer sus debilidades y fortalezas ante posibles amenazas.**

Audiencia

- Empresas de Telecomunicaciones.
- Entidades de Crédito.
- Aseguradoras y Reaseguradoras.
- Centros Sanitarios y Docentes.
- Empresas con infraestructuras críticas.
- Administraciones Públicas
- Cualquier empresa que quiera proteger sus datos.

Temáticas**

- Test Autodiagnóstico - Dime cómo es tu lunes y te diré cómo serás* hackeado.
- ¡Protección contra el Phishing!
- ¡Protección contra la Ingeniería Social!
- ¡Protección de Equipos!
- ¡Protección del Software!
- ¡Protección de las Comunicaciones, Redes Sociales y Dispositivos Móviles!

2. **Diseño y gestión de Webinars formativos o conferencias para los profesionales de las organizaciones para la concienciación en ciberseguridad.**

   Temáticas
   - Hacking Psicológico
   - Guerras híbridas: cuando el cerebro es el blanco
     Fraude del CEO
   - Neuroderechos digitales
   - Hábitos en ciberseguridad
   - Otros

3. **Formación técnica para diferentes colectivos técnicos en las organizaciones:** Desarrolladores de Software, Administradores de sistemas, Unidades de Control: mediante webinars o encuentros presenciales.

4. **Formación para los Comités Directivos/Consejos de administración:** mediante webinars o encuentros presenciales.

5. **Diseño y puesta en marcha de programas de concienciación ad hoc** para las organizaciones con contenidos síncronos y asíncronos, adaptados a las necesidades y duración. Por ejemplo: "La Semana de la Ciberseguridad de la empresa".

6. **Diseño y puesta en marcha de campañas de comunicación de los programas formativos,** que incluye los materiales ON y OFF del pre-lanzamiento, lanzamiento y dinamización del programa (recordatorios y motivación)

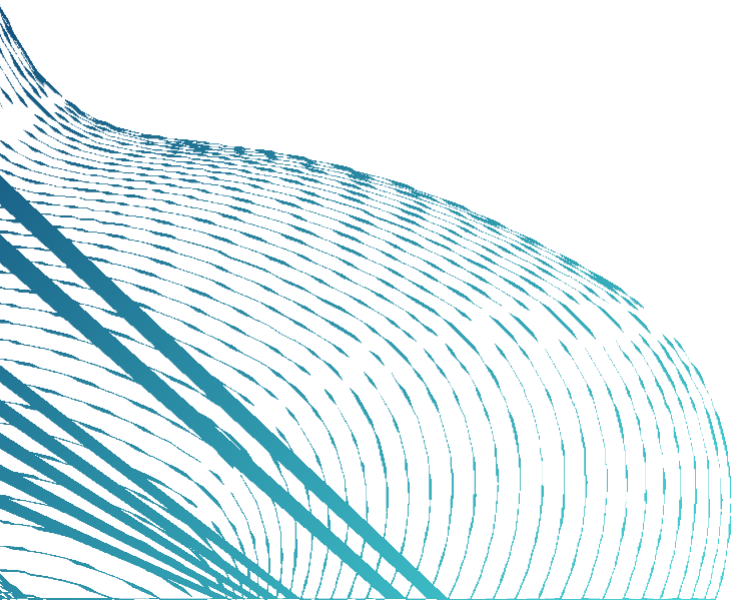
7. **Diseño de campañas de simulaciones de ciberataques** para medir los resultados de los programas formativos, incluye auditoría previa, el diseño, la estrategia, contenido de la simulación y entregable técnico con el resultado de la simulación:

   - Spear Phishing
   - Rogue AP / Evil Twin
   - Smishing
   - QRishing

*El test de autodiagnóstico se realiza en colaboración con la Unidad de Análisis de Inteligencia (UNINT). La UNINT depende de la Escuela de Inteligencia Económica (La_SEI) de la Universidad Autónoma de Madrid (UAM).
**Propuesta creativa y narrativa distinta a lo habitual en cada temática. El contenido formativo para que sea efectivo debe parecerse al tipo de contenido que le gusta a la gente, por eso, en lugar de píldoras, realizamos episodios, como en las series

• Certificaciones de ciberseguridad para productos

- Laboratorio acreditado para LINCE. Metodología ligera de evaluación y certificación para productos de seguridad TIC desarrollada por el Centro Criptológico Nacional que permite incluir productos en el catálogo CPSTIC
- / STIC 105 que es el catálogo de referencia para productos TIC ciberseguros en la Administración Pública española. Ofrece un listado de productos con unas garantías de seguridad contrastadas por el Centro Criptológico Nacional.
- Laboratorio acreditado para evaluaciones Common Criteria. Common Criteria es una norma internacional (ISO/IEC 15408) y la certificación más aceptada y utilizada para evaluar la seguridad de los productos de TIC. Reconocida en más de 30 países.
- Laboratorio acreditado para evaluaciones IoT de Consumo – ETSI EN 303 645. Norma de referencia internacional que reúne los requisitos básicos relativos a la ciberseguridad para el IoT de consumo (electrodomésticos, relojes inteligentes, dispositivos de automatización…)
- Laboratorio acreditado para evaluaciones de ciberseguridad Industrial IoT – IEC 62443.
- Seguros Cobertura sobre Riesgos Cibernéticos:
    - Gastos para recuperar actividad – Respuestas a incidentes, violación de privacidad, gestión de crisis, protección de marca, gerencia de riesgos y gastos de rectificación.
    - Perdida de beneficios por ciberataques. Reparación de sistemas.
    - Extorsión cibernética (importe del pago del rescate). Robo de identidad.
    - Daño reputacional.
    - Violación en la Protección de Datos. SANCIONES Y MULTAS del organismo regulador y cobertura de gastos de notificación por violación de privacidad.
    - Daños a terceros – RESPONSABILIDAD CIVIL por violación de privacidad, fallo de seguridad y contenidos digitales.

SOLUCIONES

- **Redes**
  - NGFirewall ; DDoS; Microsegmentación ; SD-WAN; NDR ; ZTNA; SWG
- **Identidad**
  - IAM ; PAM; MFA
- **Endpoints / Devices**
  - EPP; NGAV; EDR; XDR; UEM; MDM; MTD
  - Visibilidad Activos
- **Datos**
  - DLP ; Cifrado
- **Seguridad Cloud**
  - SASE ; SSE; CASB; SWG ; ZTNA;
  - Email & Collaboration Security Solutions [O365; Google]
  - CNAPP (Plataforma de protección de aplicaciones nativas en la nube).
- **Seguridad Aplicaciones Web / Desarrollo**
  - WAF ; API Protection;
  - Application Security Testing (SAST;DAST;IAST;RASP)
- **Monitorización Avanzada de Cibeseguridad**
  - SIEM ; SOAR
- **Auditoría Seguridad**
  - Análisis Vulnerabilidades;
  - PenTesting Simulación Phishing