Programa de Sensibilización en Ciberseguridad

Conocimiento compartido de seguros en RED
Acelerando la transformación digital del seguro

Firewall Humano:
La importancia de una cultura de ciberseguridad

- Uno de los principales retos actuales que enfrentan las organizaciones a nivel mundial es el desarrollar y/o mejorar una **cultura de ciberseguridad** en sus managers, colaboradores, empleados y principales actores de su cadena de valor. Para lograrlo, es fundamental la concienciación de los empleados y colaboradores en este ámbito y que debe ser realizada a todos los niveles, desde los altos directivos, pasando por los managers y hasta cubrir a toda la organización.
- La construcción de una cultura de ciberseguridad empresarial que permita crear un «**firewall humano**» es fundamental para ganar la batalla a los ciberdelincuentes.
- Entre las acciones clave que se pueden mencionar para el desarrollo de una cultura de ciberseguridad podemos mencionar las siguientes: Liderazgo y estrategia desde la alta dirección, equipos de trabajo de concienciación, formación a todos los niveles, uso de diferentes metodologías de aprendizaje (casos, ejercicios de puesta en práctica, simulaciones de ataques, aprendizaje colaborativo), participación en grupos de interés entre empresas para intercambiar experiencias, y finalmente medición continua de los problemas y los avances.

Objetivos

- Desarrollar cultura y competencias claves para cumplir el modelo de seguridad en la empresa.
- Reforzar, complementar y poner en práctica los procesos y el modelo de ciberseguridad frente a las principales amenazas a las que están expuestas las personas en la empresa.
- Entregar contenido de temas claves relacionados con la seguridad de la información en línea: Dispositivos, Información Sensible, Ingeniería Social y Navegación Segura (correo electrónico)
- Proveer itinerarios de aprendizaje en el ámbito de sensibilización en Ciberseguridad para los participantes de la empresa, combinando formatos de autoaprendizaje con clases en vivo (con experto) y ejercicios de puesta en práctica (call-to-action y ataques simulados).
- Apoyar a la empresa en la ejecución de itinerarios de aprendizaje apoyados en profesores, expertos internacionales con sólida experiencia en Ciberseguridad, y en las últimas metodologías de aprendizaje y tecnologías educativas.
- Ofrecer una excelente experiencia de aprendizaje virtual para los participantes.
- Ser un socio estratégico para la empresa, apoyándole en la creación de cursos digitales de manera rápida y flexible, de tal forma que la empresa pueda centrarse en su negocio.

Community of Insurance

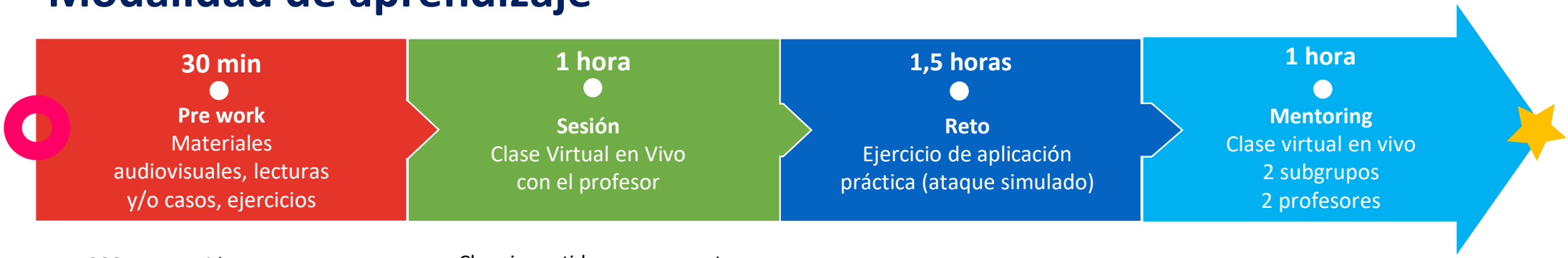
UniKemia
DRIVE FORWARD TRANSFORM

Contenidos

Temas: Cuatro (4) ámbitos

- **NAVEGACIÓN SEGURA** (Correo electrónico y navegación)
  - Compromiso del correo corporativo
  - Acceso a sitios en internet
- **DISPOSITIVOS**
  - Fuga de información
  - Pertenencia del equipo a una botnet
- **INGENIERÍA SOCIAL**
  - Vishing, Smishing, y técnicas de ingeniería social
- **INFORMACIÓN SENSIBLE**
  - Ramsonware
  - Incumplimiento normativo (GDPR)

Modalidad de aprendizaje



- SCORM con videos.
- Minicasos.
- Ejercicios.

Dedicación aprox: 20 minutos.

Preguntas de autoevaluación con el objetivo de asentar conocimientos.
Dedicación aprox.: 10 minutos.

Dedicación total aprox.: 30 min

- Clase impartida por un experto a través de videoconferencia
- Incluye tiempo para la presentación de ejemplos, y casos de los conocimientos adquiridos.
- Tiempo para preguntas de cierre del prework y/o revisión de los ejercicios prácticos.
- Presentación del reto a desarrollar.
- Interacción en vivo entre el profesor y los participantes.
- Uso de herramientas de encuestas y opinión registrada tales como Mentimeter.
- La clase será grabada para aquellos que no pudeda asistir o para consulta posterior.

Dedicación: 1 hora

- Ejercicio práctico: "Call to Action“
- El participante completa el ejercicio siguiendo 2 o 3 instrucciones del profesor.
- Se presentarán 4 escenarios de phishing (ataques simulados usando herramienta Sophos). Los 4 escenarios permitirán evitar o reducir la posibilidad de copiarse, y permitir abrir un aprendizaje más amplio y colaborativo en la sesión de mentoring grupal.
- El reto puede incluir una reflexión individual y una reflexión o actuación en parejas.
- Se incluirán 3 pistas que se "compran". Con gamificación.

Dedicación: 1,5 horas

- Clase virtual donde se pone en común los aprendizajes del grupo.
- Se ofrece las diferentes opciones de resolución del ejercicio.
- Reflexión y conclusiones.

Dedicación: 1 hora.

El grupo se divide en 2 subgrupos cada uno con un profesor

Muestra vídeos animados y SCORM con experto

Vídeos animados

Vídeos animados

SCORM con experto

Profesor: Javier Jarauta Sánchez

Mas de 35 años de experiencia en Ciberseguridad

Sistemas Informáticos Abiertos, S.A. (SIA)
Compañía especialista en Ciber del Grupo Indra
Head of Strategic Demand Generation

Profesor en la Universidad Pontificia Comillas ICAI-ICADE. Asignaturas de Ciberseguridad desde 2002 en Grado y Máster Informática y Telecomunicaciones

Director Máster en Ciberseguridad
En colaboración con Bankia, Iberdrola, Iberia, Santalucía y SIA.

Profesor en la Universidad Camilo José Cela (UCJC). Ciberdelincuencia en Grado de Criminología

Profesor en Ciberseguridad para Managers

Javier Jarauta Sánchez.
Profesor Unikemia,

Director Consultoría Grupo SIA Sistemas Informáticos Abiertos, S.A. Profesor de la Universidad Pontificia Comillas ICAI-ICADE. Director Máster en Ciberseguridad. Profesor de la Universidad Camilo José Cela (UCJC) Ciberdelincuencia en Grado de Criminología.

Universidad Pontificia Comillas Ingeniero del ICAI
- 1983. Instituto Investigación Tecnológica (IIT) de Comillas ICAI, siendo parte del equipo de fundadores.
- 1986. Técnicas de Cifra, S.A. joint venture con Datotek (Dallas-USA) pionera en Criptografía militar .
- 1992. Aeromar Telecomunicación, S.A. Proyectos de Seguridad Informática en Banca, Seguros, Sector Eléctrico, Transporte, Administración Pública y Defensa Nacional y NATO.
-2000. SIA. Sistemas Informáticos Abiertos S.A. actualmente Responsable de la Demanda Estratégica, la empresa especialista en Ciberseguridad del Grupo Indra, pionera en Firma Electrónica y Ciberseguridad, con más de 1.200 empleados.
La mayor empresa especialista Ciber en España y una de las mayores internacionalmente, abarcando todos los sectores públicos y privados: en TIC, Sistemas Industriales, Infraestructuras Críticas y Militares.
Director del Máster en Ciberseguridad de la Universidad Pontificia Comillas ICAI.

Profesor: José Antonio Cano

Senior Research Manager
IDC

Innovation & Entrepreneuship Advisor
Factoría Cultural Madrid

Deusto Business School
Tutor in Master in Business Innovation
Academic Director of EMBA Blended

Consultant Director (Technical & Economical) R&D&i
GAC Group (España)

Senior Manager
Deloitte

José Antonio Cano.
Profesor Unikemia,

Director de Análisis y Consultoría de IDC Research
Analyst research European DX and Cloud practice.

Doctor en Tecnologías de la Información y las Telecomunicaciones, por la Universidad de Valladolid.
Ingeniero de Telecomunicaciones. Universidad de Valladolid. PFC. Suma Cum Laude.
Máster en e-Business y Sistemas de Información por la Universidad de Alcalá de Henares
Máster en Relaciones Internacionales y Comercio Exterior por INFOREM
Especialista en Dirección de Proyectos por IESE

Profesor de Transformación Digital e Innovación en diferentes escuelas de Negocio (ESADE, DBS, CEU, etc.) y Universidades públicas y privadas.

Propuesta económica

Programa de Sensibilización en Ciberseguridad
Grupos de hasta 25 participantes

Se proveerá de un (1) curso de un total de 4 horas cada uno de acuerdo a la siguiente estructura:

A. Pre work - 30 minutos
B. Sesión interactiva – 1 hora
C. Reto – 1,5 horas
D. Mentoring en grupos – 1 hora. El grupo se divide en 2 subgrupos cada uno con un profesor.

Incluye: Contenido y materiales audiovisuales. Diseño de Reto. Campaña de phishing. Impartición de sesión interactiva. Impartición de Mentoring en grupos que se dividen en 2 subgrupos. Seguimiento de actividad y reportes del programa.

PRECIO POR GRUPO

Euros 2,750.00

El precio no incluye impuestos. En caso de aplicación de algún impuesto o retención, dicha cantidad deberá sumarse al precio final.

Programa de Sensibilización en Ciberseguridad

Conocimiento compartido de seguros en RED
Acelerando la transformación digital del seguro