PATROCINA

Aiuken Solutions

unir ESTUDIOS AVANZADOS

Riesgos de ciberseguridad y su impacto en negocio

La digitalización y multicanalidad aumentan el riesgo de amenazas y filtraciones poniendo en peligro uno de los mayores activos de las empresas: los datos

IMPARTIDO POR EXPERTOS DE:

- BANKIA
- CARREFOUR
- CCN- CNI
- AIUKEN
- RAZONA LEGAL TECH
- GAS NATURAL FENOSA
- MAPFRE
- AENOR
- UNIVERSIDAD REY JUAN CARLOS
- UNIVERSIDAD POLITÉCNICA DE MADRID
- FERROVIAL
- RENFE
- INNOVATION4SECURITY – GRUPO BBVA
- REALE SEGUROS
- BANCO SANTANDER
- TELEFONICA
- BANKITER
- CNPIC (CENTRO NACIONAL DE INFRAESTRUCTURAS CRÍTICAS)
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
- CUERPO NACIONAL DE POLICÍA
- MINISTERIO DE JUSTICIA

Índice

Presentación

Vivimos inmersos en proceso de transformación digital. Las empresas están realizando grandes inversiones en tecnología para digitalizar sus negocios. Los ordenadores y dispositivos inteligentes se han convertido hoy en día en los mejores aliados del entorno profesional y en ellos se procesa y almacena gran cantidad de información. Si alguno de nuestros dispositivos sufre cualquier clase de ataque, la **confidencialidad, integridad y disponibilidad** de esta información podrían comprometerse ante terceros, lo cual podría llegar a traer **consecuencias desastrosas** e incluso podría impedir la **Continuidad del Negocio**.

Conscientes de esta situación, las amenazas inteligentes APT´s, empiezan a acaparar protagonismo y a instalarse como una preocupación cuya responsabilidad y reto va más allá del CISO **haciéndose extensivo a toda la dirección, CXO´s**, estando implicado en esta responsabilidad el propio CEO. Tener una adecuada política de Ciberseguridad, permitirá proteger a nuestra organización partiendo de la concienciación y la formación a los empleados de las posibles amenazas y riegos.

Sin embargo, garantizar la seguridad de los procesos y operaciones en un entorno de negocio digitalizado exige soluciones avanzadas y contrastadas, que se traduzcan en rápidas repuestas ante cualquier ataque y permitan afrontar las amenazas de manera clara y contundente. Esto será posible **sólo si adoptamos una estrategia de Ciberseguridad dentro de la estrategia corporativa y operacional, incorporando, además de procesos y procedimientos, prácticas de Business Intelligence aplicadas al campo de la Seguridad.**

Por otra parte, una adecuada política de Ciberseguridad nos permitirá estar al día en "***compliance***". Este cumplimiento normativo abarca entre otros, aspectos regulatorios en materia de Privacidad, uso de Información Confidencial, Secreto de las Telecomunicaciones, Sociedad de la Información… incluyendo las responsabilidades penales, tanto sobre las personas jurídicas como personas físicas, que son recogidas en nuestro Código Penal y Estatuto de los Trabajadores.

Durante **6 semanas de formación** profundizaremos en todas las problemáticas a las que se enfrentan los Directivos y las empresas con los ciberataques y conocerá cómo solucionarlas de la mano de los mejores expertos.

En espera de que este programa sea de su total interés, reciba un cordial saludo.

España es el tercer país del mundo que más ciberataques recibe

Nuestros datos están expuestos a ataques para luego monetizarlos

La interconectividad, que tiene evidentes ventajas, ayuda a incrementar la ciberdelincuencia

Por qué UNIR recomienda este programa

Porque la transformación digital ha convertido a los Datos y la Información en el mayor activo de cualquier compañía. La pérdida o vulnerabilidad de dicho activo puede tener consecuencias desastrosas para el negocio. Solo aquellas empresas que impliquen a todo su equipo directivo en la estrategia de ciberseguridad, verán reducido su riesgo de sufrir un ciberataque.

BENEFICIOS

Realizando este programa aprenderá a identificar y mitigar los riesgos, cómo preparar a su compañía para actuar ante un ciberataque y cómo sobreponerse con éxito minimizando el impacto en el negocio.

DIRIGIDO A

- Directores Generales de Negocio
- Directores de Finanzas CFO
- Directores de las Unidades de Riesgo CRO
- Director Desarrollo Digital CDO
- Directores de Marketing CMO
- Director Responsabilidad Corporativa CRO
- Directores de Social Media SMM
- Directores de Tecnologías de Información CIO
- Directores de Seguridad CSO
- Directores de Seguridad de la Información CISO
- Directores de Privacidad DPO

Datos clave

Sólo 6 semanas
Del 20 de septiembre al 27 de octubre

20 conferencias online
Adaptándose al escaso tiempo de los profesionales participantes

Sesión Presencial de Networking

Ponentes profesionales de empresas líderes

Consulta a tu asesor el precio y los descuentos por inscripción anticipada
Tlf.: 941 209 743
Mail: info@unir.net

Por qué elegirnos

Nuestro modelo pedagógico pionero en el mercado y basado en **clases online en directo**, permite al profesional seguir el curso **en cualquier momento y desde cualquier lugar**, para adaptarse a la exigente agenda de nuestros participantes. Para fomentar el **NETWORKING** clave en su desarrollo profesional, nuestros programas terminan con una sesión presencial en la que podrán conocer personalmente al resto de participantes con los que han compartido experiencias a través de nuestra plataforma. En dicha sesión, expondrán la **resolución del Caso Práctico** sobre el que habrán trabajado a lo largo del curso en equipos multidisciplinares junto al instructor.

FLEXTIME

Nos adaptamos a tu disponibilidad horaria permitiéndote acceder y participar en directo a las sesiones online, a los foros de discusión, así como a los materiales complementarios. Sin barreras geográficas, en cualquier momento y en cualquier lugar.

PROFESSIONAL SPEAKERS

Todos nuestros ponentes son profesionales de empresas líderes, que imparten sus sesiones en base a su propia experiencia, lo que aporta una visión real del mercado

NETWORKING INTERNACIONAL

Podrás conocer al resto de participantes de España y Lationoamerica con los que te pondremos en contacto de forma presencial y/o virtual a lo largo del curso.

LEARNING BY DOING

La aplicación de conocimientos a través de la resolución de un caso práctico aporta al participante una experiencia formativa única. Se resolverá en grupos de trabajo multidisciplinares para fomentar el Networking y estará dirigido por un especialista en la materia. Sus conclusiones serán la excusa perfecta para intercambiar experiencias con el resto de participantes.

SESIONES ONLINE EN DIRECTO

Gracias a nuestra tecnología podrás seguir e intervenir en las sesiones estés donde estés y sin necesidad de desplazamientos. Y si por algún motivo no pudieras asistir, no te preocupes ya que todo el material queda grabado para que lo puedas volver a ver siempre que quieras.

MENTORING CONSTANTE Y PERSONALIZADO

Desde el primer día se te asignará un tutor que te acompañará y apoyará en todo momento, resolviendo todas las dudas que te puedan surgir y tratando de potenciar tus habilidades para tu desarrollo profesional.

Ponentes

D. Ángel Campillo Viejo
CISO
CARREFOUR

D. Vicente Moscardó Gil
Director Área Planificación, Riesgos y Control IT
BANKIA

D. Juan Antonio Gómez Bule
Consejero del Centro Nacional para Excelencia para las Fuerzas y Cuerpos de Seguridad del Estado
MINISTERIO DEL INTERIOR

D. Javier Candau
Jefe del Área de Ciberseguridad
CCN - CNI

D. Juan Miguel Velasco
Director General
AIUKEN SOLUTIONS

Dña. Paloma Llaneza
Socia Directora
RAZONA LEGAL TECH

D. José Luis Bolaños
Director de Security
GAS NATURAL FENOSA

Dª. Elena Mora
Subdirectora del Área Regulatorio de Seguridad
MAPFRE

Dña. Paloma Garcia
Business Standards Development Manager
AENOR

D. José Antonio Rubio
CISO
UNIVERSIDAD REY JUAN CARLOS

D. José Antonio Mañas
Catedrático
UNIVERSIDAD POLITÉCNICA DE MADRID

D. Juan Cobo
CISO
FERROVIAL

D. Francisco Lázaro
CISO
RENFE

D. Rafael Ortega
Director General
INNOVATION4SECURITY – GRUPO BBVA

D. Jesús Marcos de la Fuente
Director del Área Técnica de Seguros Patrimoniales
REALE SEGUROS

D. José Carlos Moreno Durán
Director Inteligencia & Análisis. Área Corporativa de Seguridad
BANCO SANTANDER

D. Manuel Carpio Cámara
CISO
TELEFÓNICA

D. Fernando Vega
CISO
BANKITER

D. Fernando J. Sánchez
Director del Centro Nacional de Protección de Infraestructuras Críticas
CNPIC

Dª. Elvira Tejada de la Fuente
Fiscal de la Sala del TS. Delegada Nacional de la Unidad de Criminalidad Informática.
MINISTERIO DE JUSTICIA

D. Jesús Rubí Navarrete
Subdirector
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

D. Esteban Gándara Trueba
Comisario de la Unidad Central de Seguridad Privada
CUERPO NACIONAL DE POLICÍA

DIRECTOR DEL PROGRAMA

D. JAVIER GARCÍA CARMONA

FORMER CISO - IBERDROLA

Ingeniero de Telecomunicaciones y Máster en Administración y Dirección de Empresas. Ha desarrollado su carrera profesional en distintas posiciones en el sector de las telecomunicaciones y al ámbito de la seguridad, habiendo ejercido los últimos como Responsable Seguridad de la Información y de las Comunicaciones del Grupo Iberdrola (CISO) y Responsable de la adaptación y cumplimiento del marco normativo en Privacidad (DPO).

Es Profesor en el Máster de Seguridad de la Información en la Universidad Politécnica de Madrid.

Miembro AENOR en el Subcomité de Normalización SC-27 Seguridad Tecnologías de la Información. Miembro de grupo de trabajo TNCEIP, de la Comisión Europea de Seguridad, en el sector de la energía. Miembro de grupo de trabajo Servicio de la Ciencia del JRC (Joint Research Center) de la Comisión Europea. Miembro de la Plataforma Europea de Seguridad de Redes e Información (Nis Platform).

Programa

MÓDULO 1

La nueva Era Digital y el directivo 4.0

La nueva Era Digital: Nuevas oportunidades y nuevos retos

El proceso de transformación digital de la sociedad y las empresas es uno de los mayores retos a los que nos vamos a enfrentar a lo largo de la historia. Entender este cambio de paradigma como una oportunidad para impulsar nuestra organización en este nuevo escenario, es una necesidad incuestionable. Sin embargo, lo que por un lado se plantea como un síntoma de evolución facilitando multitud de procesos dentro de las organizaciones, lleva asociados una serie de riesgos propios de este nuevo contexto digital.

- Un nuevo contexto: nuevas formas de vender, comprar e interactuar
- Internet y las Redes Sociales
- Un nuevo concepto: El "internet de las cosas, IOT"
- La tecnología como elemento facilitador
- La información en la Era Digital
- Internet y Redes Sociales
- Smart Cities
- La compartición de la información y su tratamiento
- La información en movimiento
- La Nube

D. Ángel Campillo Viejo
CISO
CARREFOUR

El directivo 4.0: Profesionales y directivos ante el Ciber-Reto

Una estrategia de ciberseguridad será eficaz sólo si en ella está implicado el equipo directivo de la Compañía, permitiendo así, a la organización estar preparada para hacer frente a los ciberataques. Los altos directivos del sector bancario tienen muy presentes los riesgos que conlleva el desarrollo del negocio digital que los sitúa como una diana para los piratas informáticos. Conscientes de esta situación Bankia ha creado un comité de Ciberseguridad en el participa su Consejero Delegado y equipo directivo.

- La Ciberseguridad como prioridad estratégica corporativa en las empresas, organismos e instituciones.
- Quiénes son los stakeholders de la ciberseguridad en la empresa
- Buenas prácticas
- El nuevo Rol del CIO, el CISO y el CTO
- El caso Práctico de Bankia

Vicente Moscardó Gil
Director Área Planificación, Riesgos y Control IT
BANKIA

MÓDULO 2

Ciber-riesgos: riesgos propios de la Era Digital

La organización como función social: las amenazas, los riesgos y sus posibles impactos según la naturaleza de actividades las empresas y la procedencia de su capital

Hay una serie de servicios que las empresas prestan a la sociedad, de carácter esencial y/o crítico para los ciudadanos y una posible interrupción alteración de éstos, como consecuencia de una ciberataque, pueden causar un importante trastorno en la sociedad.

Es por ello que sus empresas proveedoras deben tomar consciencia de su responsabilidad y dotarse de los recursos y medios necesarios para prevenir y superar dichos ciberamenaza y ciberriesgos.

Por otra parte, El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) define como "operador crítico" aquella infraestructura que forma parte de uno de los 12 sectores que prestan servicios esenciales (Administración, Agua, Alimentación, Energía, Espacio, Industria Química, Industria Nuclear, Instalaciones de Investigación, Salud, Sistema Financiero y Tributario, Tecnologías de la Información y las Comunicaciones, y Transporte).

Dada su implicación en la sociedad, este tipo de infraestructuras se rigen por una normativa específica denominada como Ley de Infraestruturas Críticas. Sin embargo hay otra serie de servicios que no siendo esenciales pueden causar un importante trastorno en la sociedad si ven interrumpido su servicio como consecuencia de una ciberataque.

Es por ello que sus empresas proveedores deben tomar consciencia de su responsabilidad y dotarse de los recursos y medios necesarios para prevenir y superar un ciberataque.

- Las amenazas, los riesgos y sus posibles impactos según naturaleza de actividades las empresas y la procedencia de su capital
- Responsabilidad de la organización en la prestación de servicios
- Requisitos y responsabilidad de los operadores no críticos pero esenciales

D. Juan Antonio Gómez Bule
Consejero del Centro Nacional para Excelencia para las Fuerzas y Cuerpos de Seguridad del Estado
MINISTERIO DEL INTERIOR

Ciberseguridad y Cibervigilancia: nuevas amenazas y tácticas de defensa para garantizar la estrategia empresarial de los directivos

El uso de las nuevas tecnologías y de Internet comportan muchos riesgos en términos de seguridad. No sólo se puede poner en peligro la privacidad personal, sino también a empresas y por consiguiente a su estabilidad generando grandes prejuicios económicos. Hasta ahora se temían los ciberataques empresariales puesto que se realizaban por hackers o grupos organizados para comprometer a una entidad, infraestructura o a un gobierno. Actualmente con el auge de la transformación digital y el uso de los multidispositivos ha proliferado también la cibervigilancia, es decir, el acceso masivo a datos personales y comunicaciones de ciudadanos.

- Quién es y donde está nuestro enemigo
- Cuáles son los colectivos interesados en acceder a nuestra info mación.
- Grupos de interés (Individuos, grupos activistas, competencia, crimen organizado, países…)
- Objetivos: robo, alteración y deterioro
- Legislación nacional vs. Legislación Internacional
- Cuáles son las mejores herramientas de defensa para prevenir la cibervigilancia
- Tendencias futuras en ciberataques y cómo adelantarnos

D. Javier Candau
Jefe del Área de Ciberseguridad
CCN - CNI

El nuevo escenario de la digitalización y los riesgos asociados: Cloud y Social Business

La utilización masiva de dispositivos conectados puede ser una puerta de entrada para los piratas informáticos enfrentando a las corporaciones a nuevos desafíos en materia de seguridad a los que no se sabe cómo dar respuesta. A medida que empresas y trabajadores se lanzan a conectar masivamente todos sus dispositivos, el riesgo de que la información generada pueda sufrir algún tipo de vulnerabilidad aumenta.

Cuatro son las grandes tendencias tecnológicas que están marcando la digitalización de las empresas: **el cloud computing, la movilidad, el big data** y, de forma transversal, la **seguridad de los datos**. El cloud computing y, con él, el big data y la movilidad, plantean inevitables dudas en torno a la seguridad de los datos. Por otra parte, los expertos alertan de los riesgos del crecimiento desmesurado de la tecnología IoT (Internet of Things), especialmente entre las empresas, que son las que, a priori, albergan información más comprometida y apetitosa para los hackers. Es por ello que los hackers se aprovechan de las vulnerabilidades de los dispositivos conectados para acceder a las redes corporativas y al hardware al que se conectan.

- Evolución de la tecnología en la sociedad
- Retos de la seguridad en **entornos cloud**: público, privado e híbrido
  - Delegación de autentificación a terceros
  - Comunicaciones cifradas para garantizar la seguridad
- Social Business: gestionando procesos a través de redes sociales
- Estrategia de ciberseguridad en entornos de movilidad
- Modus operandi e impactos

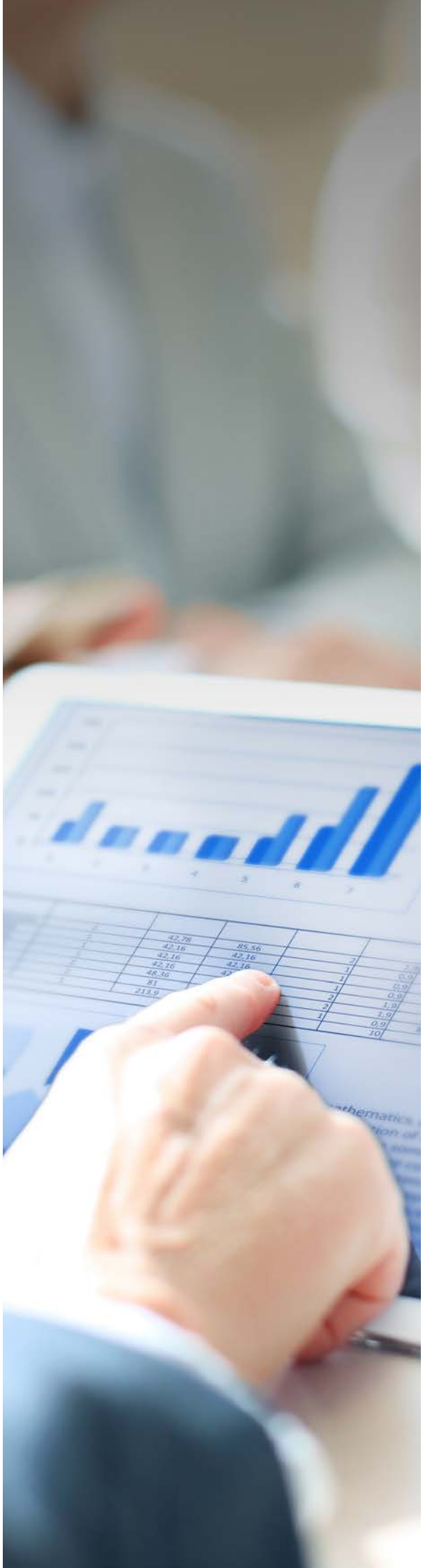
D. Juan Miguel Velasco
Director General
AIUKEN SOLUTIONS

La importancia del Compliance en los nuevos modelos digitales. Gobierno corporativo y cumplimiento. Reglamento de protección de datos y directiva NIS

Los miembros de la alta dirección deben comprender el ámbito y alcance de las normas que afectan a su sector productivo y a las transversales ya que su incumplimiento puede tener un coste penal, sancionatorio y reputacional. Desde una fuga de datos hasta un ataque desde sus sistemas, las políticas y procesos de ciberseguridad son un requerimiento legal cuyo incumplimiento recae en la organización y en quien la dirige.

- Cumplimiento legal y responsabilidad civil
- Reglamento de protección de datos y directiva NIS
- Compliance Penal y programas de prevención de la responsabilidad penal de altos cargos y directivos
- Gestión integrada de los programas de cumplimiento ¿es posible?
- Cultura, procesos y personas implicadas en el cumplimiento empresarial
- Procedimientos y medidas de control para supervisar, gestionar y monitorizar el cumplimiento normativo

Dña. Paloma Llaneza
Socia Directora
RAZONA LEGAL TECH



MÓDULO 3

El análisis y la gestión de riesgos en la estrategia de ciberseguridad

La Ciberseguridad no es un problema tecnológico sino un problema estratégico y de gestión de riesgos. Es por ello que **el comité de dirección debe exigir un control y evaluación del riesgo constante, permanente y actualizado**. En este sentido la Gestión de Riesgos debe ir orientada a proteger la información y la reputación de la organización. Por ello se hace imprescindible:

- Implementar y administrar controles que tengan como foco principal los objetivos del Negocio
- Promover acciones correctivas y preventivas de forma eficaz y eficiente
- Garantizar el cumplimiento de reglamentaciones
- Definir los procesos de gestión de la seguridad de la información

Conocer los requisitos, elementos y acciones necesarios para implementar una adecuada gestión del riesgo es clave para garantizar su éxito. Para ello, deberemos llevar a cabo la aplicación sistemática de políticas, prácticas y procedimientos de gestión destinados a identificar, analizar, evaluar, tratar y monitorear el riesgo. En la implantación de un modelo de gestión de ciberseguridad bajo el prisma de la inteligencia estratégica, todo pasa por una mayor comprensión del entorno digital corporativo. La gestión del riesgo operacional y organizacional implicará una evaluación continua del riesgo en cada uno de los puntos clave y críticos.

Problemática de riesgo de información en la organización

D. José Luis Bolaños
Director de Security
GAS NATURAL FENOSA

Política y objetivos de la seguridad de la información: Definición de roles y responsabilidades

- Política de Seguridad de la Información
- Relación con los Objetivos de Seguridad de la Información
- Importancia de la Política
- Elaboración de la Política
- Identificación y Definición de Roles y Responsabilidades

Dª. Elena Mora
Subdirectora del Área Regulatorio de Seguridad
MAPFRE

Nuevos escenarios de normalización de la seguridad

- Normativa TI actual
- Novedades en materia de normalización y su impacto en el negocio
- Sistemas de Gestión de Seguridad de la Información

Dña. Paloma Garcia
Business Standards Development Manager
AENOR

Resiliencia en procesos críticos y de negocio

- Resiliencia de procesos críticos
- Amenazas
- Requerimientos de la seguridad
- Vulnerabilidades
- Activos
- Valor de los activos

D. José Antonio Rubio
CISO
UNIVERSIDAD REY JUAN CARLOS

Análisis y valoración de los riesgos, amenazas y vulnerabilidades

D. José Antonio Mañas
Catedrático
UNIVERSIDAD POLITÉCNICA DE MADRID

Elaboración del plan de tratamiento de los riesgos: programas y presupuestos

Cómo elaborar un plan de tratamiento de riesgos en ciber-seguridad

D. Juan Cobo
CISO
FERROVIAL

Concienciación y formación en seguridad

En materia de Seguridad de la información: Concienciada, Sensibilizada, Formada y Capacitada son estadios diferentes del camino que toda empresa debe completar para minimizar los riesgos asociados a la información y en consecuencia mantener las operaciones y respaldar el crecimiento del Negocio .

Para ello deberemos Concienciar con información inteligible, Sensibilizar mediante casos prácticos , Involucrando al trabajador, Formar según roles y perfiles adecuados, y finalmente Capacitar con formación en sus herramientas, simulación y procedimientos (contemplando el ciclo PDCA).

- ¿De qué manera se involucra al personal interno y externo clave en las cuestiones de seguridad?
- Cuáles deben ser nuestros objetivos
- Cómo generar, en la Alta Dirección, interés en esta materia
- Cómo generar, en los trabajadores, interés en esta materia
- Qué necesidades son típicamente necesarias. Roles
- Qué tipos de contenidos debemos generar
- Cuáles son las mejores modalidades y técnicas de formación

D. Francisco Lázaro
CISO
RENFE

Procesos y procedimientos de seguridad para la gestión del riesgo. Servicios avanzados de seguridad

- Qué procesos utiliza para gestionar la respuesta ante incidencias y la recuperación tras desastres
- Qué procedimientos permiten detectar posibles amenazas

D. Rafael Ortega
Director General
INNOVATION4SECURITY – GRUPO BBVA

Ciberseguros para garantizar la continuidad del negocio: programas de pólizas de seguros

La ciberseguridad 100% no existe, por eso hay que medir los riesgos expuestos y establecer programas aseguradores que los cubran.

- Calidad del riesgo y riesgo medible.
- Coberturas ofertadas por el mercado.
- Privacy y Agencia de protección de datos.
- Reclamaciones de terceros
- Futuro asegurador

D. Jesús Marcos de la Fuente
Director del Área Técnica de Seguros Patrimoniales
REALE SEGUROS

Proyectiva en seguridad: Security Business Intelligence

Los modelos de seguridad tradicionales centraban sus esfuerzos en mantener las amenazas externas alejadas de la compañía, sin embargo esto ya no es suficiente. **Los nuevos modelos de ciberseguridad son predictivos y han de aplicarse de manera trasversal a toda la organización** por lo que proporcionar estrategias adecuadas a la anticipación debe ser uno de los ejes vehiculares de las definiciones de los programas de seguridad.

Es fundamental dotarse de soluciones integrales y Análisis de Riesgos Dinámicos a la hora de diseñar la capa de protección, para ello debemos poner nuestro foco en el desarrollo e implementación de estrategias que complementen las medidas de seguridad actualmente definidas, con la aplicación de tendencias innovadoras que permitan la mitigación y anticipación de riesgos operacionales, sin perder de vista la importancia de la gestión adecuada de la respuesta.

Líneas de actuación, de máximo nivel, que no solo nos aseguren una protección frente a las amenazas tradicionales físicas sino que también de aquellas que afectan a la seguridad lógica y que ante una eventualidad, permitan y garanticen una adecuada gestión de los incidentes, reduciendo los tiempos de exposición. Diseño que pretende fortalecer un entorno colaborativo entre las diferentes áreas que participan en la toma de decisiones, con un fin evidente, garantizar los procesos de negocio. Bajo la premisa de que la amenaza tarde o temprano se va a materializar.

- Panorama actual y tendencias Ciberseguridad
- Trazabilidad: la huella digital
- Big Data: All word is watching
- Vigilancia digital (estrategia de monitorización)
- Capacidades de protección (herramientas y soluciones)
- Escenarios de Riesgo y amenazas. Especial seguimiento hacktivismo y cyberterrorismo
- Gestión del riesgo operacional en las entidades financieras

D. José Carlos Moreno Durán
Director Inteligencia & Análisis. Área Corporativa de Seguridad
BANCO SANTANDER

MÓDULO 4

La respuesta ante incidentes: estrategia ante el ciberataque

La gestión eficaz de un incidente de ciberseguridad es clave para poder mantener la actividad de la empresa. En la Política de Gestión de Incidentes, deberán participar todas aquellas personas que tengan acceso tanto a la información como a las tecnologías que lo soportan, incluso a aquellos gestionados por terceros. La rapidez con que se pueda reconocer, analizar y responder amenazas minimizará el daño y disminuirá los costes de recuperación. Por ello, la respuesta de incidentes, debe estar en el ADN de la Organización.

Preparación: cómo actuar ante el ciberataque y definición de las estructuras organizativas

- Definición de las estructuras organizativas
  - Comité de Crisis
  - Comité de Evaluación
  - Comité Jurídico
  - Comité de Comunicación
- Definición de estructuras tecnológicas de atención a incidentes
- Recursos humanos y técnicos de identificación de incidentes: La importancia del **simulacro y el "red team".**
- Plan de contingencias y plan de continuidad

D. Manuel Carpio Cámara
CISO
TELEFÓNICA

Análisis y detección: nuevas herramientas para detectarlo. El papel de Big Data y del Business Intelligence

- Confección e implantación de procedimientos operativos de Seguridad (POS)
- Implantación de infraestructuras técnicas para la detección de ataques
- Dotación de recursos de análisis de información de Seguridad
- Sistemas de monitorización de la información de seguridad
- Modelización de actuaciones ante incidentes
- Análisis de información: el papel del Big Data y del Business Inteligence

D. Manuel Carpio Cámara
CISO
TELEFÓNICA

Contención, erradicación y recuperación (DR, BCP)

- Confección de planes de actuación ante crisis y sus seguimientos por los Comités
- Confección de los modelos de gobierno, gestión y operación de recuperación ante desastres (DR)
- Confección de los modelos de gobierno, gestión y operación de continuidad de Negocio (BCP)

D. Fernando Vega
CISO
BANKITER

Lecciones aprendidas en el establecimiento de equipos especializados y del modelo de mejora continua

- Establecimientos de equipos especializados en el análisis de datos de evolución de incidentes y crisis para modelización de actuaciones futuras
- Establecimiento de modelo de mejora continua

D. Fernando Vega
CISO
BANKITER

EMPRESAS COLABORADORAS

FTI Fundación Tecnologías de la Información

AMETIC

NETWORKING SESSION

Sesión presencial de clausura

Mesa redonda: La información en la era digital y sus responsabilidades

D. Fernando J. Sánchez
Director del Centro Nacional de Protección de Infraestructuras Críticas
CNPIC

Dª. Elvira Tejada de la Fuente
Fiscal de la Sala del Tribunal Supremo
Delegada Nacional de la Unidad de Criminalidad Informática. Fiscalía General del Estado
MINISTERIO DE JUSTICIA

D. Jesús Rubí Navarrete
Subdirector
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

D. Esteban Gándara Trueba
Comisario de la Unidad Central de Seguridad Privada
CUERPO NACIONAL DE POLICÍA

Café Networking

LEARNING BY DOING. Resolución caso práctico junto al instructor

Fin de la Jornada Presencial de Clausura

INSTRUCTOR DEL CASO PRÁCTICO

JOSÉ ANTONIO RUBIO
CISO - UNIVERSIDAD REY JUAN CARLOS

Doctor Ingeniero en Ciberseguridad y Confianza Digital.

Director del IDG Digital Trust Think Tank.

Colaborador Honorífico de la Universidad Complutense de Madrid.

Coordinador Nacional en AENOR del CTN 71/SC 27/GT 4 y GT 5.

Miembro del CTN 307/SC 1 sobre Sistemas de Gestión del Cumplimiento y Sistemas de Gestión Anticorrupción.

Director de Relaciones Académicas de ISACA Madrid.

Miembro del Network and Information Security Platform de la Comisión Europea. Miembro del Foro Nacional de Confianza Digital de la Secretaría de Estado de Telecomunicaciones y Sociedad de la Información. Miembro de las Comisiones de Calidad y Seguridad, y de Gestión del Compliance de la Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información.

MÓDULO PRÁCTICO (2H)

El instructor entregará un caso práctico a los participantes al inicio del curso. Para trabajar en su resolución el instructor creará equipos multidisciplinares y a ser posible multisectoriales. Dichos grupos trabajarán el caso y entregarán sus conclusiones al instructor una semana antes de la sesión presencial. Deberán nombrar un portavoz que en un tiempo limitado exponga y defienda la resolución del caso. Tanto el instructor como el resto de participantes pondrán en cuestión dichas conclusiones. Esta sesión, tendrá lugar en el auditorio de Proeduca en Madrid. Quienes no puedan asistir de manera presencial, podrán hacerlo por streaming.

En el caso práctico se perseguirán los siguientes objetivos:

- Enlazar los objetivos de negocio con los objetivos en materia de Ciberseguridad y Compliance.
- Identificar aquellos procesos de negocio que deben recibir una especial atención.
- Entender los riesgos digitales derivados de las nuevas oportunidades de negocio que se generan en la organización.
- Entender las cadenas de valor de la actividad organizativa y su sinergia con el área de Ciberseguridad
- Identificar acciones en Ciberseguridad y Compliance y su empleo como elementos de ventaja competitiva, liderazgo en mercado y barrera frente a competidores
- Entender la Responsabilidad Penal de la Persona Jurídica y cómo cumplir con la debida diligencia en materia de Gobierno Corporativo del Riesgo.
- Promover un cambio en el pensamiento y actitud de la organización ante la Ciberseguridad.

Otros Programas Avanzados que pueden ser de tu interés:

- Big Data for Business
- Corporate Compliance
- Inteligencia Artificial el nuevo motor para la transformación empresarial
- Finanzas para no financieros

Otros programas de interés de la Escuela de Ingeniería:

- Máster universitario en Análisis y Visualización de Datos Masivos / Visual Analytics & Big Data
- Máster Universitario en Seguridad Informática
- Máster en DevOps, Cloud Computing y Automatización de Producción de Software
- Máster en Project Management (PMP®)
- Curso de Preparación para la Certificación PMP ®

CONSULTA CON TU ASESOR LOS DESCUENTOS POR INSCRIPCIÓN A VARIOS PROGRAMAS

Tlf.: 941 209 743
Mail: info@unir.net

unir
ESTUDIOS
AVANZADOS

Delegación Madrid
C/ Almansa, 101
28040 Madrid
España
+34 915 674 391

Delegación México
Av. Extremadura, 8.
Col Insurgentes Mix-
coac. Del.Benito Juárez
03920, México D.F.
+52 55 63951017

Delegación Colombia
Carrera 21 # 102-46
Bogotá, Bogotá, D.C.
Colombia
+317 574 2631
+310 666 5574