

TALLER

Ciberseguridad para auditores internos: Fundamentos y controles

Horario:
18:30 a 20:30
(hora de Ecuador)

16, 17 18, 19 de noviembre (8 horas CPE)

Facilitador
Danny Bastidas, Gerente de Ciberdefensa - Banco Pichincha

El aumento de la frecuencia y gravedad de los ciberataques hace necesario que Auditoría Interna tenga mayor comprensión sobre ciberseguridad, conocer su rol que establecen las Normas Globales de Auditoría Interna frente a la prevención, gestión de los riesgos y los controles necesarios para mitigar las amenazas.

OBJETIVOS

- Definir la ciberseguridad desde una perspectiva de auditoría interna.
- Conocer la importancia de la gobernanza de seguridad de la información con el programa de ciberseguridad.
- Reconocer los controles preventivos, directivos, de detectivos, mitigación, redundantes, compensatorios y correctivos relacionados con la ciberseguridad típicos.
- Identificar actividades de auditoría interna simples para evaluar la resiliencia cibernética dentro de los programas de auditoría operativa existentes.

CONTENIDO TÉCNICO – 8 HORAS CPE

5. Descripción general de la ciberseguridad

- Visión general de la ciberseguridad
- El proceso de violación, y las motivaciones y tácticas de un mal actor.
- Tipos de controles para proteger o minimizar los ciberataques.
- Visión general de la defensa en profundidad, la seguridad en capas y el modelo de interconexión de sistema abierto (OSI).

5. Seguridad de la información - Gobernanza, riesgo y control

- Visión general de la gobernanza de la ciberseguridad y las Normas asociadas.
- Visión general de la gestión de riesgos de ciberseguridad y las Normas asociadas.
- Desarrollo de un programa de gestión de riesgos de ciberseguridad.
- Áreas de control de ciberseguridad y desarrollo de programas.
- Garantía de gobernanza, riesgo y controles de ciberseguridad, y auditoría de ciberseguridad.

5. Fundamentos de los controles

- Control interno
- Diseño y mantenimiento de controles.

- Tipos de controles.
- Niveles de controles.
- Clasificaciones de controles.
- Controles por función.
- Inventario de activos y controles.
- Auditoría de Controles según las NOGAI.

4. Controles por Función:

- Directivos
- Preventivos
- Detectivos
- Correctivos
- Mitigantes
- Compensatorios y redundantes

5. Evaluación de la ciberseguridad en programas de auditoría operativa

2. Visión general de las Normas Globales de Auditoría Interna relacionadas con los programas de trabajo que tienen en cuenta los riesgos relacionados con el ciberespacio.
2. Una descripción general de los GTAG y las guías prácticas relacionadas con los programas de trabajo que explican los riesgos relacionados con la ciberseguridad.
2. Una visión general de los marcos de ciberseguridad y control en la nube reconocidos por la industria.
2. Sugerencias para mejorar los programas de auditoría operativa con actividades de auditoría relacionadas con el ciber.

METODOLOGÍA

- Exposición teórica breve: Explicación de conceptos clave con apoyo visual.
- Estudio de casos reales: Resolución grupal de problemas.
- Debates y retroalimentación: Discusión de resultados y buenas prácticas.

FACILITADOR: Danny Bastidas, Gerente de Ciberdefensa en Banco Pichincha



Con más de 12 años de experiencia en Ciberseguridad, especializo en temas de Operación de Ciberseguridad, Gestión de proyectos, Seguridad de Información, administración de plataformas, arquitectura de seguridad, ISO 27001 - SGSI, CSIRT, PenTest, Hacking ético, procesos, Gestión de Incidentes, Gestión de Vulnerabilidades, Liderazgo de equipos..

Fue Director Nacional de Innovación Tecnológica en ECU 911, Gerente de Ciberseguridad en CNT, en Location World, especialista de seguridad de información en Telefónica.

Es Master en Ciberseguridad de la Universidad Católica de Murcia, tiene una Maestría en Gerencia Empresarial, administración y gestión de empresas. Cuenta con las licencias NSE de Network Security Associate, CCSE - Experto en Seguridad Certificado, CCSA – Administrador de Seguridad Certificado de Check Point, CCDA – Asociado de diseño Certificado de CISCO, Certified Ethical Hacker de EC- Council.

LOGÍSTICA

FECHAS: lunes 16, martes 17, miércoles 18, jueves 19 de noviembre

HORARIO: 18h30 a 20h30

PLATAFORMA: ZOOM

INVERSIÓN (adicionar IVA)

Socios individuales: \$270

Socios **corporativos** afiliados: \$250

Particulares: \$300

DESCUENTOS:

De 2 a 3 participantes el 5%

4 en adelante el 6%

INCLUYE: Certificado de participación, manual del participante (**digital**) del taller.

Tarjeta de crédito: Se puede diferir a 3 meses sin intereses



Información e inscripciones

IAI Ecuador

Teléf::0999729770,

0979268936, 2553957,

eventos@iaiecuador.org

www.iaiecuador.org



CIBERSEGURIDAD PARA AUDITORES INTERNOS – FUNDAMENTOS Y CONTROLES**1. Descripción general de la ciberseguridad**

- Visión general de la ciberseguridad
- El proceso de violación, y las motivaciones y tácticas de un mal actor.
- Tipos de controles para proteger o minimizar los ciberataques.
- Visión general de la defensa en profundidad, la seguridad en capas y el modelo de interconexión de sistema abierto (OSI).

2. Seguridad de la información - Gobernanza, riesgo y control

- Visión general de la gobernanza de la ciberseguridad y los estándares asociados.
- Visión general de la gestión de riesgos de ciberseguridad y los estándares asociados.
- Desarrollo de un programa de gestión de riesgos de ciberseguridad.
- Áreas de control de ciberseguridad y desarrollo de programas.
- Garantía de gobernanza, riesgo y controles de ciberseguridad, y auditoría de ciberseguridad.

3. Fundamentos de los controles

- Control Interno
- Diseño y mantenimiento de control.
- Tipos de controles.
- Niveles de control.
- Clasificaciones de control.
- Controles por función.
- Inventario de activos y control.
- Controles y los estándares.

1. Controles de Función:**Controles directivos**

- Visión general de los controles directivos y su importancia en la ciberseguridad.
- Exploración de las amenazas comunes a los controles directivos.
- Utilizando marcos, estándares y directrices de ciberseguridad para establecer controles directivos.
- Importancia de la capacitación en ciberseguridad como control directivo.
- Construir controles directivos para apoyar programas de incentivos.

Controles preventivos

- Visión general de los controles preventivos y su importancia en la ciberseguridad.
- Uso de controles preventivos con respecto a la anatomía de una violación:
 - Infiltración.
 - Propagación.
 - Agregación.
 - Exfiltración.
- Introducción a las técnicas de monitoreo e informes.

Controles detectivos

- Visión general de los controles detectivos y su importancia en la ciberseguridad.
- La tríada de ciberseguridad (CIA Triad).
- Controles para detectar incidentes cibernéticos.

- Centro de Operaciones de Seguridad (SOC) en respuesta a una violación de la ciberseguridad.
- Contener cualquier violación en la seguridad y determinar la exposición y exfiltración de datos resultantes.
- Registro de auditoría y gestión de eventos e información de seguridad (SIEM) para un seguimiento continuo.
- Consideraciones para la auditoría de los controles detectivos.
- Clasificación de datos, propiedad y controles detectivos.

Controles correctivos

- Visión general de los controles correctivos y su importancia en la ciberseguridad.
- Tipos comunes de controles correctivos:
 - Respaldo y restauración.
 - Continuidad del negocio.
 - Recuperación de desastres.
 - Respuesta a incidentes.
- Amenazas potenciales a la funcionalidad de los tipos comunes de controles correctivos.
- Conceptos de auditoría esenciales para evaluar los controles correctivos de ciberseguridad.

Controles mitigantes

- Visión general de los controles de mitigación y su importancia en la ciberseguridad.
- Amenazas potenciales a la funcionalidad de los tipos comunes de controles de mitigación.
- Proceso de gestión de riesgos de ciberseguridad y los controles de mitigación.
- Tipos comunes de controles de mitigación.
- Enfoques de auditoría esenciales para evaluar los controles de mitigación relacionados con la ciberseguridad.

Controles compensatorios y redundantes

- Visión general de los controles compensatorios y redundantes y su importancia en la ciberseguridad.
- Tipos comunes de controles compensatorios y redundantes.
- Amenazas potenciales a la funcionalidad de los tipos comunes de controles compensatorios y redundantes.
- Enfoques de auditoría para evaluar los controles compensatorios y redundantes relacionados con la ciberseguridad.

5. Evaluación de la ciberseguridad en programas de auditoría operativa

- Visión general de las Normas Globales de Auditoría Interna relacionadas con los programas de trabajo que tienen en cuenta los riesgos relacionados con el ciberespacio.
- Una descripción general de los GTAG y las guías prácticas relacionadas con los programas de trabajo que explican los riesgos relacionados con la ciberseguridad.
- Una visión general de los marcos de ciberseguridad y control en la nube reconocidos por la industria.
- Sugerencias para mejorar los programas de auditoría operativa con actividades de auditoría relacionadas con el ciber.