CURSO ONLINE

elearning ALIDE

Gestión Integral

de la Ciberseguridad y Ciberresilencia en Bancos e Instituciones Financieras

11 DE JULIO AL 8 DE AGOSTO DE 2023

www.alide.org.pe

INFORMACIÓN GENERAL

PRESENTACIÓN

A diario conocemos noticias sobre incidentes de ciberseguridad en las cuales están involucrados tanto entidades públicas como privadas, ocasionando en muchos casos pérdida económica y reputacional. Es bien sabido que los ciber atacantes realizan sus ataques por medio de grupos organizados, con una metodología muy efectiva y con objetivos claramente identificados. Sin embargo, las organizaciones muchas veces son muy pasivas en sus acciones de protección y no trabajan bajo el supuesto de que se puede dar un ataque a su infraestructura o a su información.

Los ataques sobre todo para las instituciones financieras tienen objetivos económicos y de robo de información. Si partimos de esas premisas entonces no solo debemos pensar en la protección, si no en que hacemos durante el ataque y como lo hacemos. Por lo tanto, no solo es conocer los riesgos a los que las instituciones están expuestas y cómo se debe proteger la institución, así como también qué hacer para recuperarse luego de un ataque, o sea, aplicar los conceptos y procedimientos para garantizar una adecuada ciberresiliencia. El saber reconocer, evaluar y mitigar los incidentes de ciberseguridad se convierte en toda una necesidad, pero tanto la ciberseguridad como la ciberresiliencia deben estar enmarcadas dentro de una estrategia más amplia para de esa forma darle sentido en la institución que se pueda garantizar y cumplir los objetivos institucionales.

Estas acciones y estrategias deben enmarcarse dentro estándares internacionales que han sido probados y adoptados por las instituciones a nivel mundial, por lo que resulta necesario que se adopten estas prácticas toda vez que permiten -dentro de un marco de trabajo establecido- generar acciones y conductas que justamente evitan las iniciativas individuales o *sui generis* de las instituciones, las cuales en muchas ocasiones no dan los resultados adecuados.

Conscientes de la importancia para las instituciones financieras de la ciberseguridad y ciber-resiliencia que enfrentan, ALIDE presenta su Curso Online sobre Gestión Integral de la Ciberseguridad y Ciberresiliencia en Bancos e Instituciones Financieras, con la finalidad de cubrir de manera efectiva y metodológica todos los temas tratados y permita obtener una visión holística de la problemática y las maneras como pueden ser solucionadas.

DURACIÓN DEL CURSO

Se desarrollará en 5 sesiones teniendo un total de 15 horas lectivas, con la atención personalizada del expositor y el acceso al Campus Virtual de ALIDE, www.alidevirtual.org. Se utilizará la plataforma de videoconferencia "Zoom", por lo que podrán acceder a las sesiones desde una computadora personal o de escritorio, celulares y tabletas.

FECHAS

Se realizará de acuerdo con las fechas y horarios siguientes:

Sesión	Fechas	Horas	Horario *	Módulos
1	Martes, 11 de julio	3	3:00 a 6:00 pm	Módulo I: Ciberseguridad, Ciberriesgos y Ciberresiliencia, marcos normativos y definiciones
2	Martes, 18 de julio	3	3:00 a 6:00 pm	Módulo II: Gobierno de Ciberseguridad

Sesión	Fechas	Horas	Horario *	Módulos
3	Martes, 25 de julio	3	3:00 a 6:00 pm	Módulo III: Tecnologías de Ciberseguridad
4	Martes, 1 de agosto	3	3:00 a 6:00 pm	Módulo IV: Riesgos y Controles de ciberseguridad
5	Martes, 8 de agosto	3	3:00 a 6:00 pm	Módulo V: Ciberresiliencia

* Hora de Perú. Para visualizar tu hora local, hacer clic aquí y digita tu ciudad en el campo "Agregar otra ciudad"

OBJETIVOS

- Entender y conocer la dinámica de las diferentes tecnologías de ciberseguridad existentes en el mercado y cómo estas se integran para mejorar y optimizar la protección de una organización.
- Entender y conocer la dinámica de los riesgos tecnológicos, riesgos de seguridad de la información y riesgos de ciberseguridad en una institución
- Entender los requerimientos humanos y materiales dentro de una organización necesarios para la gestión de la ciberseguridad.
- Conocer las etapas y actividades para el desarrollo de una estrategia de ciberseguridad.
- Conocer la forma de generar planes de mitigación de riesgos.
- Explicar los niveles de ciberresiliencia organizacional y desarrollar una estrategia para tal efecto.
- Diagnosticar los niveles de ciberseguridad de la organización.
- Entender la estructura de un plan de ciberseguridad.

PROGRAMA TEMÁTICO

Módulo I: Ciberseguridad y Ciberresiliencia, Marcos Normativos y Definiciones
No. de horas: 3

- Ciberseguridad.
- Norma ISO 27032 / Marco NIST.
- Ciberseguridad y la seguridad de la información.
- Ciclo de vida de la ciberseguridad.
- Ciberseguridad y ciberresiliencia.
- Riesgos de ciberseguridad.
- Ciberseguridad; eventos principales.
- Implicancias en las organizaciones.

Módulo II: Gobierno de Ciberseguridad
No. de horas: 3

- Situación actual.
- Como funciona el gobierno de ciberseguridad.
- Roles y responsabilidades del gobierno de ciberseguridad.
- Factores críticos de éxito de un buen gobierno de ciberseguridad.
- Métricas para un gobierno de ciberseguridad.
- El rol del CISO.
- Ubicación del CISO en la estructura organizativa.
- CISO y ciberresiliencia.

Módulo III: Tecnologías de Ciberseguridad
No. de horas: 3

- Tecnologías de ciberseguridad:
    a. Protección del perímetro.
    b. Protección de la infraestructura.
    c. Protección de las aplicaciones.
        i. WAF
        ii. WAAF
        iii. RASP
    d. Ciclo de desarrollo de las aplicaciones.
        i. El Modelo DevSecOps
        ii. Pruebas SAST
        iii. Pruebas DAST
        iv. Pruebas SCA
    e. Protección del Endpoint
        i. EDR
    f. Tecnología de monitoreo
        i. SIEM
        ii. XDR
    g. El modelo ZERO TRUST

Módulo IV: Riesgos y Controles de ciberseguridad
No. de horas: 3

- Marco de gestión del ciber riesgo.
- Tareas de la gestión de ciber riesgos.
- Organización para la gestión de riesgos.
- Controles de ciberseguridad.
    a. Controles de nivel de aplicación.
    b. Controles de protección del servidor.
    c. Controles de usuario final.
    d. Controles contra ingeniería social.
- Controles CIS – 20 controles de ciberseguridad.
    a. Controles básicos.
    b. Controles fundamentales.
    c. Controles organizativos.

Módulo V: Ciberresiliencia
No. de horas: 3

- Modelo de desarrollo de un plan de ciberresiliencia.
- Gestión de incidentes.
- Planes de ciberseguridad.

ENFOQUE METODOLÓGICO

Nuestro modelo de formación se basa en una acción tutorial constante, en donde el participante estudiará de acuerdo con su tiempo y disponibilidad.

Cabe resaltar que en el Campus Virtual de ALIDE se colocará el enlace para las videoconferencias que se tendrán en cada una de las sesiones, a través de la plataforma “Zoom”, por lo que podrán acceder a las sesiones desde una computadora personal o de escritorio, celulares y tabletas. Cabe

mencionar que, si el participante no pudiese de participar en alguna sesión, le brindaremos la grabación de esta, la cual será publicada en el campus virtual de ALIDE.

Los participantes contarán con el acompañamiento permanente del expositor, a quien se le puede formular las preguntas y dudas que se tenga para recibir las orientaciones y respuestas a las consultas individual o grupalmente. Ello puede ser así en el desarrollo de las sesiones o a través de la opción de comunicación con el expositor que tiene el campus virtual de ALIDE.

PARTICIPANTES

Responsables de ingeniería o administración que están o estarán involucrados en el desarrollo y aplicación de riesgos de ciberseguridad en bancos comerciales, bancos de desarrollo, instituciones financieras no bancarias, organismos de supervisión bancaria y además de todos aquellos profesionales relacionados en el área de riesgos, auditoria de sistemas o auditores en general que requieran tener un conocimiento teórico y práctico sobre la gestión de riesgos.

EXPOSITOR

FRANO CAPETA MONDOÑEDO

Peruano. Ingeniero de Computación y Sistemas, estudios de Postgrado en Tecnologías de Información. Maestría en Administración de Empresas, Especializado en seguridad de la información y continuidad de negocios.
Auditor ISMS (Information Security Management Systems) acreditado por IRCA (International Register Certified Auditors), Auditor BCMS (Business Continuity Management Systems) acreditado por IRCA, posee las Certificaciones en gobierno empresarial de TI; Certificado CGEIT (Certified in the Governance of Enterprise IT) por ISACA, en riesgos;

Certificado CRISC (Certified in Risk and Information Systems Control) por ISACA, Certificado CISO (Chief Information Security Officer) por EC-Council, Certificado en ISO 27002 Information Security Foundations, Certificado en Ciberseguridad como Lead Cybersecurity manager, profesional certificado en Blockchain (CBP – Certified Blockchain Profesional) Certificado como ITIL Expert, con experiencia en implementación y administración de Proyectos de Tecnología de Información, seguridad de la información y continuidad del negocio. Miembro asociado del BCI (Business Continuity Institute), Miembro activo del Colegio de Ingenieros del Perú, miembro activo de ISACA (Information Systems audit and Control Association).

INVERSIÓN Y FORMA DE PAGO

- US$407 por participante (Institución miembro de ALIDE)
- US$581 por participante (Institución no miembro de ALIDE)

DESCUENTO CORPORATIVO POR GRUPOS

3% de la cuota correspondiente de 3 hasta 5 participantes
5% de la cuota correspondiente de 6 a más participantes

El importe de las inscripciones es neto sin afectar deducciones, impuestos y retenciones propios del país de procedencia del participante. Por lo tanto, si se va a aplicar deducciones o impuestos

al importe neto de la inscripción, debe comunicarse el porcentaje a aplicar, con el fin de emitir la factura por un monto tal que permita cobrar la cuota de inscripción estipulada. No se aplican los descuentos corporativos por grupos en caso se cargue algún impuesto local.

Para efectuar el pago, se debe realizar por intermedio de:

- Para instituciones en el Perú:
  Depósito bancario a Cta. Cte. N° 193-1132251188 del Banco de Crédito del Perú

- Para instituciones de otros países:
  Transferencia bancaria a la cuenta corriente de ALIDE N° 75022011-3 del Banco do Brasil S.A. (New York). Dirección: 535 Madison Avenue – 33th floor, New York NY 10022, U.S.A., Teléfono: (1-646) 845-3700 / 845-3752. ABA: 026003557. SWIFT: BRASUS33

Nota: Para todos los países, inclusive Perú, los pagos pueden realizarse mediante tarjeta de crédito (Visa/MC/AMEX/Diners), coordinando previamente con ALIDE.

CERTIFICACIÓN

Se otorgará Certificación Internacional a las personas que completen satisfactoriamente el curso, es decir, que cumplan con la evaluación encomendada por el expositor, de modo tal de obtener un puntaje superior a 7.4 sobre 10 puntos y la participación en cada una de las sesiones ya que también es calificada, por lo que se solicita la activa participación en cada una de ellas. En el certificado se indicará el desempeño obtenido por el participante. Éste será enviado por correo electrónico.

INSCRIPCIONES

El proceso de inscripción se realiza a través del Campus Virtual de ALIDE, www.alidevirtual.org, en el cual existe la opción correspondiente de REGISTRARSE, donde completará un formulario en línea, luego de lo cual se le facilita la confirmación y los pasos para el ingreso al Campus Virtual de ALIDE. El cierre de inscripción y matrícula del curso vence el martes, 4 de julio de 2023.

INFORMES Y CONSULTAS

Sr. Sandro Suito, Responsable de E-learning de ALIDE
Sra. Milagros Angulo, Asistente del Programa de Capacitación y Cooperación
E-mail: mangulo@alide.org