CURSO ON-LINE

RIESGOS TECNOLÓGICOS Y DE CIBERSEGURIDAD

8 ABRIL AL 6 DE MAYO DE 2021

www.alide.org

elearning ALIDE

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. Muchos de estos incidentes son motivados por riesgos tecnológicos que no han sido identificados ni mitigados, convirtiéndose estos luego en una pesadilla empresarial. Si a esto le sumamos el periodo especial que estamos viviendo en todos los países desde el mes de marzo-abril 2020 hasta nuestros días, los riesgos ahora se han incrementado apareciendo nuevas categorías de riesgos.

Las instituciones deben tener una clara identificación de sus riesgos tecnológicos, dado que la tecnología de información hace parte fundamental de cualquier estrategia de negocios, y en estas épocas de transformación digital más aún. Por lo tanto, el saber reconocer, evaluar y mitigar los riesgos tecnológicos se convierte en toda una necesidad; sin embargo, la identificación de los riesgos tecnológicos debe estar enmarcada dentro de una estrategia de seguridad y de ciberseguridad para de esa forma darle sentido en la institución y que obedezca a una estrategia amplia, de forma 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.

El hecho de que una institución tenga la iniciativa de generar un apetito de riesgos requiere una participación a todo nivel de la institución y se desliga de la clásica concepción en la cual se piensa que tanto la seguridad como la ciberseguridad es un tema meramente tecnológico. El conocimiento y la aplicación de una metodología va a permitir a una institución garantizar la identificación de los riesgos, pero por, sobre todo, debe garantizar la mitigación de éstos.

Conscientes de la importancia para las instituciones financieras de los riesgos tecnológicos y de ciberseguridad que enfrentan, ALIDE presenta su Curso Online sobre RIESGOS TECNOLOGICOS Y DE CIBERSEGURIDAD, 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 Y HORARIOS

Se realizará de acuerdo con las fechas y horarios siguientes:

Sesión	Fechas	Horas	Horario *	Módulos
1	Jueves, 8 de abril	3	3:00 a 6:00 pm	Módulo I: Ciberseguridad y Riesgos: Definiciones y Conceptos
2	Jueves, 15 de abril	3	3:00 a 6:00 pm	Módulo II: Gobierno de Ciberseguridad
3	Jueves, 22 de abril	3	3:00 a 6:00 pm	Módulo III: Ciberseguridad
4	Jueves, 29 de abril	3	3:00 a 6:00 pm	Módulo IV: El Proceso de Riesgo

Sesión	Fechas	Horas	Horario *	Módulos
5	Jueves, 6 de mayo	3	3:00 a 6:00 pm	Módulo V: Controles y Tecnología de Ciberseguridad

* Estos horarios son válidos para 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 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 los riesgos de ciberseguridad.
- Conocer las etapas y actividades para el desarrollo de una correcta identificación de riesgos tecnológicos, y riesgos de ciberseguridad.
- Identificar tecnologías de ciberseguridad requeridas para mejorar los niveles 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

Durante el curso se dará una inducción a los conocimientos y métodos de cómo enfrentar los riesgos tecnológicos y de ciberseguridad en una institución financiera y el uso de las nuevas tendencias tecnológicas. Asimismo, el desarrollo de un conjunto de ejercicios relacionados con la metodología propuesta de identificación de riesgos tecnológicos y de ciberseguridad

Módulo I: Ciberseguridad y Riesgos: Definiciones y Conceptos
No. de horas: 3

- Ciberseguridad.
- Norma ISO 27032.
- Seguridad de la información.
- Norma ISO 27001/ ISO 27002.
- Ciberseguridad vs seguridad de la información vs seguridad informática.
- Ciclo de vida de la ciberseguridad.
- Partes interesadas.
- Ciberseguridad; eventos principales.
- Implicancias en las organizaciones.

  Caso de aplicación 1: "Estamos bien seguros!!"

  Discusión del caso de aplicación 1

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.
- Gestión de riesgos de seguridad, dentro del gobierno corporativo.
- Métricas para un gobierno de Ciberseguridad.

- El rol del CISO.
- Ubicación del CISO en la estructura organizativa.
- Funciones del día a día.

  Caso de aplicación 2: "…Pero ¿Estás seguro que necesitamos personal para la ciberseguridad?
  Discusión del caso de aplicación 2

Módulo III: Ciberseguridad
No. de horas: 3

- Ciberseguridad y ciberataques.
- Ciberseguridad y sus interfases con otros departamentos.
- Política de ciberseguridad.
- Tipo de políticas de ciberseguridad.
- Mecanismos de ataque.
- Principales amenazas cibernéticas y vectores de mitigación.
- Ciberresiliencia.
- Autoevaluación de nuestro nivel de ciberseguridad
- ¿Que nos enseñan los ataques?

  Caso de aplicación 3: "Los ataques son cada vez más complejos"
  Discusión del caso de aplicación 3

Módulo IV: El Proceso de Riesgo
No. de horas: 3

- Marco de gestión de riesgo.
- Tareas de la gestión de ciber-riesgos.
- Organización para la gestión de riesgos.
- Conceptos básicos; vulnerabilidad, amenaza y riesgo.
- Actividades a seguir para gestionar los riesgos.
  a. Identificación de activos.
  b. Propietario del activo.
  c. Clasificación del activo
  d. Valoración del activo.
- Evaluación de las consecuencias – Factores a ser considerados.
- Probabilidad del riesgo.
- Matriz del riesgo.
- Nivel de riesgo.
- Tratamiento del riesgo.
- Riesgos tecnológicos y su identificación;
  a. Test de intrusión y sus metodologías.
  b. Etapas de una prueba de intrusión.
  c. Las 7 fases de un ciberataque.
  d. Pruebas SAST
  e. Pruebas DAST
- Identificación de consecuencias.
- Amenazas, vulnerabilidad y consecuencias.

  Caso de aplicación 4: "Aplicación del proceso de riesgos"
  Discusión del caso de aplicación 4

Módulo V: Controles y Tecnología de Ciberseguridad
No. de horas: 3

- Controles de ciberseguridad – los 10 pasos hacia la ciberseguridad.
- 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.
- Tecnologías de ciberseguridad
- Planes de Cibersegurdad

Caso de aplicación 5: "¿Qué control es el adecuado?
Discusión del caso de aplicación 5

ENFOQUE METODOLÓGICO

Nuestro modelo de formación se basa en una acción tutorial constante, en donde el participante estudiará de acuerdo con un plan de trabajo que se definirá en cada una de las sesiones. Habrá sesiones prácticas a través talleres de trabajo individual/grupal, para lo cual deberán tomar nota de los requerimientos de participación, por cada sesión de clase se propondrá un caso de estudio, el cual debe ser analizado y comentado por el participante y luego será comentado y discutido por el docente.

Las tareas programadas son de tres tipos: desarrollo de casos prácticos, auto-evaluaciones y trabajo final:

- El desarrollo de casos que serán propuestos por el docente y que estarán directamente vinculados al tema de la semana de clase y tendrán por objetivo promover la discusión y escuchar diversos puntos de vista sobre el tema en base a las experiencias de los participantes.

- La auto evaluación comprende un cuestionario con preguntas relacionadas con el módulo que fortalecerán los conocimientos del participante y constituirán una medida de cómo va progresando el participante en el curso.

- El trabajo final, que será encomendado por el expositor con el fin que se apliquen todos los conocimientos, experiencias y aspectos prácticos revisados durante el curso, para que los participantes muestren su suficiencia a la culminación del mismo.

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 la misma 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 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$350 por participante (Institución miembro de ALIDE)
- US$500 por participante (Institución no miembro de ALIDE)

DESCUENTO CORPORATIVO POR GRUPOS

3% del pago total, de 3 hasta 5 participantes
5% del pago total, de 6 a más participantes

El importe de las inscripciones es neto sin afectar deducciones o impuestos. 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.

Para efectuar el pago, se debe realizar una transferencia o depósito bancario a:

- Para instituciones en el Perú: 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 – 34th floor, New York NY 10022, U.S.A., Teléfono: (1-646) 845-3700 / 845-3752. ABA: 026003557. SWIFT: BRASUS33

CERTIFICACIÓN

Se otorgará certificación Internacional a las personas que completen satisfactoriamente el curso, es decir, que cumplan con las tareas y trabajos encomendados por el expositor y obtengan un puntaje superior a 7.4 sobre 10 puntos. Cabe indicar que la participación en el curso es calificada, por lo que en el certificado se indicará el desempeño obtenido por el participante. El certificado 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 jueves, 1 de abril de 2021.

INFORMES Y CONSULTAS

Sr. Sandro Suito, Responsable de E-learning de ALIDE
Sr. Benjamin Carbajal, Especialista del Programa de Capacitación y Cooperación,
E-mail: bcarbajal@alide.org

ASOCIACIÓN LATINOAMERICANA DE INSTITUCIONES FINANCIERAS PARA EL DESARROLLO (ALIDE)
Paseo de la República 3211. San Isidro. Lima 27
Apartado postal 3988, Lima 100 – Perú
Web: www.alide.org