CURSO A DISTANCIA

Riesgos Tecnológicos y de Ciberseguridad

11 DE NOVIEMBRE AL 22 DE DICIEMBRE

www.alidevirtual.org

elearning ALIDE

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, muchos de estos incidentes son motivados por riesgos tecnológicos que no han sido identificados ni mitigados, convirtiéndose estos luego en una pesadilla empresarial.

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 aun, 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 deben estar enmarcados 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, para que de esta formar se puedan 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 estos.

Conscientes de la importancia para las instituciones financieras de los riesgos tecnológicos y de ciberseguridad que enfrentan, ALIDE presenta su Curso a Distancia sobre **RIESGOS TECNOLOGICOS Y CIBERSEGURIDAD,** con la finalidad de que cubra 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

El curso tiene una duración de seis (6) semanas consecutivas, con la atención personalizada del tutor y el acceso al Campus Virtual de ALIDE, www.alidevirtual.org. Se recomienda como mínimo una dedicación de 8 horas semanales estableciendo su propio ritmo y horario de aprendizaje.

FECHAS

El curso se inicia el **11 de noviembre** y culmina el **22 de diciembre de 2019.**
El cierre de inscripción y matrícula del curso vence el miércoles 6 de noviembre de 2019.

OBJETIVOS

- Entender y conocer la dinámica de los riesgos tecnológicos, riesgos de seguridad de la información y riesgos de ciberseguridad en una institución, proponiendo una metodología para tal efecto.

- Conocer las etapas y actividades para el desarrollo de una correcta identificación de riesgos tecnológicos, y riesgos de ciberseguridad.

- Conocer la forma de generar planes de mitigación de riesgos.

TEMARIO Y PROGRAMACIÓN DE ACTIVIDADES

El curso se desarrollará en tres partes diferenciadas: la primera destinada a la inducción de 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; la segunda dedicada a la intervención en un foro de discusión para el intercambio de experiencias entre los participantes; y la tercera, al desarrollo de un conjunto de ejercicios relacionados con la metodología propuesta de identificación de riesgos tecnológicos y de ciberseguridad

PRIMERA PARTE: ASPECTOS BÁSICOS DE LOS RIESGOS TECNOLÓGICOS Y DE CIBERSEGURIDAD

Temas	Duración	Fechas
Módulo I: Ciberseguridad y Riesgos: Definiciones y Conceptos ➢ Ciberseguridad. ➢ Norma ISO 27032. ➢ Seguridad de la información. ➢ Norma ISO 27001/ ISO 27002. ➢ Ciberseguridad vs seguridad de la información vs seguridad informática. ➢ Implicancias en las organizaciones. Foro 1: Grandes robos de información.	1 semana	11 – 17 de noviembre
Módulo II: Riesgos, Normas y Estándares ➢ Marco de gestión de riesgo. ➢ Norma ISO 31000. ➢ Norma ISO 27005. ➢ Normas NIST. Módulo III: Gobierno de Ciberseguridad ➢ Estructura de gestión para la ciberseguridad y los riesgos. ➢ El rol del CISO. ➢ Ubicación del CISO en la estructura organizativa. ➢ Nivel de preparación del CISO. ➢ Funciones del día a día. ➢ El rol de CRO. ➢ El rol de comité de gestión de seguridad. Foro 2: ¿Qué tanto nos ayudan las normas estándares?	1 semana	18-24 de noviembre

Temas	Duración	Fechas
Módulo IV: Ciberseguridad ➢ Política de ciberseguridad. ➢ Tipo de políticas de ciberseguridad. ➢ Desarrollo y despliegue de políticas. ➢ Controles de ciberseguridad. ➢ Controles de nivel de aplicación. ➢ Controles de usuario final. ➢ Controles contra ataques de ingeniería social. Foro 3: ¿Cómo controlamos los ataques de ingeniería social?	1 semana	25 de noviembre – 1 de diciembre
Módulo V: El Proceso de Riesgo (Parte I) ➢ Identificación de controles existentes. ➢ Identificación del nivel de madurez. ➢ Identificación de vulnerabilidades. ➢ Vulnerabilidades. ➢ Identificación de consecuencias. ➢ Amenazas, vulnerabilidad y consecuencias. Foro 4: ¿Cuál es mi nivel de riesgo?	1 semana	2-8 de diciembre
Módulo VI: El Proceso de Riesgo (Parte II) ➢ Análisis de riesgo. ➢ Evaluación de las consecuencias. ➢ Evaluación de las consecuencias – Factores a ser considerados. ➢ Probabilidad del riesgo. ➢ Evaluación del riesgo. ➢ Nivel de riesgo. ➢ Guía para la evaluación del riesgo. ➢ Priorización del riesgo. Foro 5: Riesgos	1 semana	9-15 de diciembre
Módulo VII: Gestión de Riesgos y Controles ➢ Tratamiento del riesgo. ➢ Selección de las opciones de tratamiento. ➢ Controles ISO 27002. ➢ Retención del riesgo. ➢ Evitar el riesgo. ➢ Aceptación del plan de tratamiento. ➢ Implementación del plan de tratamiento. Foro 6: El plan de tratamiento del riesgo, su aprobación e implementación.	1 semana	16-22 de diciembre

SEGUNDA PARTE: FORO DE INTERCAMBIO DE EXPERIENCIAS SOBRE GESTIÓN DE RIESGOS TECNOLÓGICOS Y DE CIBERSEGURIDAD

En esta parte del curso, los participantes podrán intercambiar opiniones sobre un tema planteado por el instructor-tutor del curso, de tal manera de generar una retroalimentación que incluye puntos de vista, observaciones y cuestionamientos relacionados con el objetivo del curso y de los módulos en cuestión. Se busca promover un espacio de debate dinámico donde el objetivo sea incentivar la participación para la discusión del o de los temas buscando que se

reflejen opiniones sólidas relacionadas con el tópico propuesto. Esto será realizado de manera semanal, pues todas las semanas se propondrá un tema para el foro, el cual será en principio desarrollado por el instructor-tutor y luego los participantes tendrán que intervenir y comentar.

Para ello será indispensable la reflexión crítica de los participantes sobre el o los temas de debate y la aportación de nuevas ideas, lo cual es lo estrictamente evaluado, soportada - sólo cuando corresponda - con referencias complementarias.

TERCERA PARTE: TRABAJO FINAL

Para finalizar el curso, se trabaja con los participantes la aplicación de conocimientos en un trabajo práctico final que integra lo aprendido en los diferentes módulos. La supervisión del trabajo práctico implica la acción interactiva participante – tutor.

ENFOQUE METODOLÓGICO

Nuestro modelo de formación a distancia se basa en una acción tutorial constante, en donde el participante estudiará de acuerdo a un plan de trabajo donde se definirán tareas semanales. El éxito del curso a distancia se sustenta en la actuación conjunta del instructor – tutor y de los participantes, a quienes se les requiere el compromiso de estudios de un tiempo mínimo de ocho (8) horas semanales. Esta dotación de tiempo se aprovechará al máximo, si se sigue de manera cuidadosa la distribución del tiempo y las tareas asignadas.

Las tareas programadas son de dos tipos: auto-evaluaciones y trabajo final:

- Foros de debate que serán convocados y calificados por el instructor – tutor por cada módulo, con los temas específicos de análisis, fechas y duración los cuáles permitirán el fructífero intercambio de experiencias entre participantes de diferentes instituciones y países.

- 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 tutor 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.

Los participantes contarán con el acompañamiento permanente del instructor - tutor, a quien se le puede formular las preguntas y dudas que se tenga, para recibir las orientaciones y respuestas a las consultas individualmente o grupalmente. Asimismo, se podrán compartir documentos, trabajos destacados, enlaces Web de interés y glosario de términos, promoviendo de este modo el intercambio de experiencias entre el tutor y los participantes. Los participantes de los cursos a distancia de ALIDE, accederán libremente al DATA BANK ALIDE, http://alidedatabank.org/index.php, que es una plataforma de servicios del Centro de Documentación de ALIDE (Cedom), especializado en Banca de Desarrollo.

Para un buen aprovechamiento del curso, aconsejamos conectarse a diario o días alternos. No obstante, en el Campus Virtual se colocarán avisos y anuncios sobre las actividades a realizar, que serán informados a los participantes mediante mensajes de alerta a sus respectivos correos electrónicos.

PARTICIPANTES

Responsables de ingeniería o administración que están o estarán involucrados en el desarrollo y aplicación de riesgos 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.

INSTRUCTOR – TUTOR

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$400 por participante (Institución miembro de ALIDE)
- US$550 por participante (Institución no miembro de ALIDE)

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

Una vez realizado el pago, las instituciones deberán enviar copia del documento de depósito al Programa de Capacitación y Cooperación de ALIDE, E-mail: ssuito@alide.org.

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 tutor 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. Cierre de inscripciones: miércoles 6 de noviembre de 2019, informes y consultas dirigirse a:

Sandro Suito Larrea
Responsable del E-Learning ALIDE
Programa de Capacitación y Cooperación
Teléfono: +511 203-5520 Ext. 223
Correo: ssuito@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