Diplomado en Gestión Estratégica de Ciberseguridad y Riesgos

Versión en Línea

Coordinadora académica: Dra. Laura Jácome

Nota: Este diplomado es en la modalidad en línea a través de la herramienta Zoom. Se requiere que el participante cuente con computadora, laptop, tablet, teléfono inteligente o cualquier otro dispositivo que permita reproducir audio y video y una buena conexión a internet.

Las clases serán en tiempo real en los días y horario publicados. Las sesiones no serán grabadas y el participante sólo tendrá acceso a las sesiones del diplomado en el grupo al cual se haya inscrito.

Objetivo general

Hoy en día, los negocios se desarrollan en ambientes cambiantes y complejos que requieren gran colaboración y procesamiento de información. Son ambientes con entornos regulatorios más estrictos, donde debe haber un fuerte grado de cumplimiento y con un incremento en los delitos cibernéticos detonando que sean relevantes los temas de gestión de riesgos y manejo de la seguridad de la información.

Dentro de este entorno empresarial, las tecnologías de información (TI) desempeñan un papel primordial como habilitadores de negocios. Por ello, las organizaciones demandan un enfoque tecnológico que sea, por un lado, altamente flexible y adaptable al entorno en constante evolución y, por otro lado, plataformas tecnológicas robustas que permitan la implementación de sus estrategias de negocios de forma segura. Para ello, los profesionales que participan en la creación, provisión, aseguramiento y uso de información deben ser capaces de abordar temas relacionados con buenas prácticas, metodologías y herramientas que les permitan, por un lado, convertirse en líderes de conocimiento e innovación y, por otro, ser capaces de soportar y transformar los negocios basándose en tecnologías de la información de manera eficiente y efectiva, en un ambiente altamente competitivo, regulado y cambiante. Este panorama, de dependencia tecnológica casa vez mayor y ciberataques más frecuentes, también ha dado lugar a que las personas del negocio, ejecutivos, consejeros, involucrados en la administración en general, conozcan ciertos aspectos de las TI, principalmente aquellos relacionados con riesgos y seguridad, que les permita tener un mejor entendimiento de los factores que inciden con el fin de tomar decisiones informadas y garantizar que la operación no se interrumpa y no se afecten los resultados esperados .

El diplomado "*Gobierno, Ciberseguridad y Estrategia*" está orientado a cubrir esas necesidades y se caracteriza por tener un enfoque corporativo que asegura a los participantes el desarrollo de una perspectiva holística de riesgos, gobierno y seguridad de la información como catalizador de valor para la empresa. El diplomado permite desarrollar una perspectiva del Gobierno Corporativo o Empresarial, Riesgos, Seguridad y su relación con las TI. Esta perspectiva incluye el establecimiento de los principios, las estructuras y las prácticas necesarias para establecer un buen Gobierno de TI y una buena gestión de Riesgos, desde el nivel estratégico hasta el nivel táctico y operativo para generar estrategias innovadoras basadas en TI y para incrementar el retorno de las inversiones asociadas, al tiempo que se optimizan los recursos, se mitigan los riesgos y se da cumplimiento efectivo a las regulaciones aplicables. Tiene un enfoque teórico pero basado en casos que permitan llevar a la práctica los conceptos aprendidos.

Módulo I
GOBIERNO, RIESGO Y CUMPLIMIENTO

Estableciendo las estructuras, procesos, políticas y normas para la correcta dirección de las compañías de tal forma que se asegure el valor, la rendición de cuentas, la equidad y la transparencia.

Objetivo
Entender cómo el gobierno corporativo proporciona una estructura para el establecimiento de objetivos por parte de la empresa, y determina los medios que pueden utilizarse para alcanzar dichos objetivos y para supervisar su cumplimiento, así como conocer como el corporativo abarca toda una serie de relaciones entre el cuerpo directivo de una empresa, su consejo, sus accionistas y otras partes interesadas. Comprender el valor de un buen gobierno corporativo y su relación con el Gobierno de TI para:

- Dimensionar los incentivos apropiados al Consejo y al cuerpo directivo, para que se persigan objetivos que sirvan a los intereses de la sociedad y de sus accionistas, además de facilitar una supervisión eficaz.
- Articular un elemento clave para aumentar la eficacia económica y potenciar el crecimiento, así como para fomentar la confianza de los inversores.
- Mejorar la comunicación y colaboración entre los diferentes líderes de la organización
- Asegurar la integración estratégica de TI con el negocio
- Establecer una administración eficiente de los recursos de TI en su ciclo de vida
- Establecer la administración efectiva de los riesgos de negocio asociados con TI
- Asegurar el cumplimiento de las normativas internas (políticas) y externas (regulaciones) soportadas por TI

Temario

1. Gobierno Corporativo
    a. Conceptos fundamentales
    b. Las Responsabilidades del Consejo
    c. Relaciones entre el cuerpo directivo de una empresa, su Consejo, sus accionistas y otras partes interesadas
    d. Normas y directrices en materia de gobierno corporativo,
    e. Principios de Gobierno corporativo
    f. El marco para el gobierno corporativo y su dependencia del entorno legal, reglamentario e institucional
    g. Gobierno corporativo y su relación con el establecimiento de objetivos por parte de la empresa, la determinación delos medios que pueden utilizarse para alcanzar dichos objetivos y la supervisión de su cumplimiento.
2. Gobierno de TI
    a. Enfoque en COBIT
    b. Conceptos generales de Gobierno Empresarial de TI
    c. Descripción general de algunos estándares, prácticas y marcos de trabajo relevantes (ej. COSO, ISO 31000, COBIT, ITIL, BASILEA II)

Módulo 2
ESTRATEGIA Y ARQUITECTURA DE NEGOCIO

Estableciendo objetivos de negocio y alineando las decisiones tecnológicas para alcanzarlas dentro de un marco que garantice la correcta operación.

Objetivo

Proporcionar los métodos necesarios para la definición estratégica de la empresa que determinen sus capacidades futuras de tal forma que se garantice la operación y de la empresa bajo un nivel de riesgo controlado así como Proporcionar una visión integral de la Arquitectura Empresarial como marco de trabajo integral que proporcione el contexto empresarial necesario para la gestión de los objetivos establecidos, dentro de un riesgo controlado y bajo actividades de cumplimiento de tal forma que:

- Se consideren los diferentes aspectos involucrados en la planeación estratégica: tecnología, procesos, recursos humanos y finanzas
- Establezcan objetivos de corto y largo plazo tanto de negocio como de TI
- Establezcan las iniciativas, programas y proyectos requeridos para crear, mejorar o transformar las capacidades actuales
- Se utilicen marcos de AE y GRC para abordar las estrategias planteadas.

Temario

1. Conceptos generales de estrategia
2. Fundamentos de la metodología Balanced Scorecard (de Kaplan y Norton)
3. El Balanced Scorecard (BSC) corporativo y el de TI

4. Fundamentos de Arquitectura Empresarial y su relación con la gestión estratégica corporativa y de TI
5. Teoría en Arquitectura Empresarial: Conceptos Generales y Fundamentos
6. Conceptos del marco de arquitectura empresarial del Open Group: TOGAF
7. Conceptos del marco de la OCEG para GRC
8. Modelo de Capacidad GRC de la OCEG
    a. Estructura del Modelo
    b. Componentes de una solución GRC
    c. Factores Críticos de Éxito
9. TOGAF y OCEG operando de forma armónica para lograr capacidades tradicionalmente desarrolladas por departamentos como: auditoría interna, cumplimiento, riesgos, legal, TI así como las líneas de negocio y los comités establecidos

Módulo 3
RIESGOS OPERATIVOS Y RIESGOS DE TI

Promoviendo un ambiente confiable de negocios.

Objetivo
El objetivo de este curso es mostrar un panorama del Riesgo Operativo y Riesgo de TI, conocer las mejores prácticas para la implementación y desarrollo de las funciones relativas a su gestión para lograr cumplir los objetivos empresariales y poder:

- Garantizar la identificación y administración eficiente de los riesgos operacionales de forma rentable,
- Garantizar la identificación de controles clave para mitigar los riesgos.
- Establecer un monitoreo constante y congruente con el apetito de riesgo de la entidad

Temario
1. Tipos y conceptos de riesgos
    a. Tipos de Riesgos
    b. Factores de riesgo operacional
    c. Análisis de causa raíz
    d. Estableciendo el apetito al riesgo
    e. Ciclo de la administración de riesgo operacional
2. Roles y responsabilidades (Papel del Comité de Riesgos)
    a. ¿Qué valor agrega el administrador de riesgos a la organización?
3. Mejores prácticas y marcos regulatorios
    a. Basilea II
    b. ERM-COSO
    c. Ley SOX
    d. Mejores Prácticas Corporativas

4. Auto evaluación de riesgos y controles (RCSA**)**
    a. Metodologías para la elaboración de la matriz
    b. Valoración de riesgos y controles clave
    c. Elaboración de mapas de riesgo
    d. Presentación de informes
    e. Desarrollo, seguimiento y evaluación de planes de mitigación
    f. Presentación de informes
5. Indicadores Claves de Riesgos (KRI**)**
    a. Identificando y definiendo los indicadores clave de riesgo (KRI)
    b. Unidades de cuantificación y su normalización
    c. Establecimiento de límites de tolerancia, umbrales y objetivos
    d. Análisis de escenarios
6. Eventos de pérdidas - incidencias**.**
    a. Taxonomía de riesgos operacionales y de eventos de pérdida
    b. Registro de incidencias
    c. Uso de información interna y externa
    d. Conciliación de la base de datos vs la información contable
    e. Informes, seguimiento y tratamiento de los resultados
    f. Control de daños y pérdidas
7. Modelo de cuantificación del riesgo operacional
    a. La causalidad como base del modelo
    b. Valoración del riesgo y de las pérdidas potenciales
    c. Validación del modelo
    d. Capital económico y capital regulatorio
8. Riesgos de TI
    a. Definición e identificación del riesgo tecnológico
    b. Clasificación y jerarquización de las aplicaciones por su nivel de riesgo
    c. Evaluación de los controles generales y de las aplicaciones
    d. Implicaciones de la función de seguridad de la información

Módulo 4
GOBIERNO Y GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Garantizando la confiabilidad operativa de las organizaciones mediante la disminución de los riesgos tecnológicos.

Objetivo
Crear e implementar una estrategia de gobierno y gestión de la seguridad de la información que permita garantizar a las organizaciones operar en un ambiente de mínimo riesgo para sus activos tecnológicos críticos de tal forma que:

- Se garantice la continuidad operativa a pesar de las amenazas informáticas
- Se minimice el riesgo tecnológico optimizando el uso de los recursos
- Se logre el cumplimiento de disposiciones legales en términos de seguridad de la información

Temario

1. Fundamentos de seguridad de la información
    a. Contexto externo e interno de la organización desde un enfoque de seguridad de la información
    b. Propiedades de la seguridad: confidencialidad, integridad y disponibilidad
    c. Arquitectura de seguridad
    d. Componentes del riesgo: amenaza, vulnerabilidad, vector de ataque y nivel de riesgo
2. Gobierno de seguridad de la información
    a. Estructura organizacional
    b. Roles y responsabilidades
    c. Comités y grupos de trabajo
3. Sistema de Gestión de Seguridad de la Información (SGSI)
    a. Mejores prácticas (ISO 27000, NIST, COBIT)
    b. Planeación de un SGSI: objetivos y alcance
    c. Administración de riesgo: análisis de vulnerabilidades, pruebas de penetración y evaluación del riesgo
    d. Implementación de controles: preventivos, de detección y de recuperación
    e. Evaluación de desempeño y mejora continua: medición, monitoreo y análisis

Módulo 5

ADMINISTRACIÓN DE CRISIS EN SEGURIDAD DE LA INFORMACIÓN

Objetivo

Crear e implementar una estrategia administración de crisis, respuesta a incidentes en cómputo y su investigación por medio para poder:

- Entender que un plan de respuesta a incidentes requiere de personal clave dentro de la organización
- Identificar cómo se puede reaccionar correctamente un incidente, regresar a la operación y aprender de los mismos.
- Obtener las pruebas necesarias para su posible presentación ante una autoridad logrando un cumplimiento en caso de existir.
- Hacer uso de ciberinteligencia por medio de OSINT y otras herramientas que permitan contrarrestar al incidente.

Temario

1. Respuesta a Incidentes
    a. La estructura y participantes de un equipo de respuesta
    b. Objetivos del Equipo de Respuesta a Incidentes
    c. Capacidades requeridas para un Equipo de Respuesta a Incidentes
    d. Metodología, Procesos y Procedimientos
    e. Tipos de Incidentes y cómo reaccionar a ellos.
    f. Herramientas
    g. El valor de la Concientización

2. Investigaciones Digitales: Cómputo Forense
    a. Cómputo Forense
    b. Pasos del Cómputo Forense
    c. Cadena de Custodia y Valores de Integridad
    d. Metodologías
    e. Análisis General
    f. Marco Jurídico
    g. Delitos Informáticos
    h. Futuro del Cómputo Forense
3. Ciber-Inteligencia
    a. El proceso de Inteligencia
    b. Tipos de Inteligencia
    c. Recolección
    d. Análisis
    e. Procesamiento

Coordinadora académica

Dra. Laura Jácome

Doctora en Ingénierie des Connaissances et des Systèmes d'Information por el Institut National des Télécommunications de Evry, Francia. Obtuvo la mención *Très Honorable* en la realización de su tesis que versó sobre la flexibilidad en los sistemas de información de operadores de telecomunicaciones. Maestra en Mastère Spécialisé Manager Télécom por el Institut National des Télécommunications y Maestra en Tecnologías de Información y Administración por el ITAM. Conferencista en diversos foros académicos y empresariales. Cuenta con amplia experiencia profesional en el desarrollo e implantación de sistemas, así como en implantación de mejores prácticas para la prestación de servicios de TI y de arquitectura empresarial. Dentro del área académica, ha sido profesora de los cursos de Ingeniería de *software*, procesos de negocios y auditoría de procesos de negocios. Es Testigo Social de Transparencia Mexicana en diversos proyectos.