PROGRAMA DEL CURSO

I. Identificación General

Nombre:	**Ciberseguridad en la Industria Aseguradora**
Horas:	35 horas
Destinatarios:	Este curso está dirigido a profesionales de distintas disciplinas que deseen tener una visión holística del problema de Ciberseguridad y entender las herramientas de gestión necesarias para poder hacer frente a la problemática. Desde este punto de vista este curso es aplicable para Abogados que desean tener mayor conocimiento en temas de Ciberseguridad, Chief Information Security Officer (CISO), personas de Recursos Humanos encargados de elaborar un programa de Cambio Cultural en Ciberseguridad y todo profesional que está o desee adquirir mayores conocimientos de Ciberseguridad.

II. Fundamentación Técnica

Este curso se realiza con la finalidad de entregar herramientas del Management que permitan gestionar de mejor forma los riesgos de ciberseguridad, dando una visión holística en temas de Gobiernos Corporativos, Gestión de Ciber Crisis, y los elementos del factor humano presente en los temas de Ciberseguridad. Considerando que en la actualidad todas las industrias, independientemente del tamaño de las organizaciones están afectas a esta problemática, la industria del seguro también debe mejorar sus capacidades y habilidades para enfrentar esta problemática.

III. Objetivo General

Los participantes en este curso tendrán una visión integral del problema de la ciberseguridad, como también una visión holística de los aspectos del managemnet que es necesario considerar para efectos de elaborar una estrategia en ciberseguridad de manera efectiva y la gestión los ciber riesgos.

IV. Desarrollo

Objetivos Específicos	Contenidos
Comprender la importancia de un buen Gobierno Corporativo en la gestión de la Ciberseguridad.	Unidad I: Gobiernos Corporativos y Ciberseguridad • Análisis de Caso – Data Breach at Equifax • Fundamentos de Gobiernos Corporativos • Mecanismos Internos y Externos • Elementos del Gobierno Corporativo relacionados a Ciberseguridad • Análisis de Caso – Cyber Breach at Target • Análisis del impacto en la gobernabilidad de las brechas de datos.
Distinguir la diversidad de amenazas y vulnerabilidades existentes en el Ciber espacio, y como una efectiva gestión de riesgo puede ayudar a mitigarlas	Unidad II: Ciber Ataques y Gestión de Riesgos • Principales amenazas y vulnerabilidades del ciberespacio • Cómo aplicar una metodología de riesgos para gestionar las amenazas • Enfoque Cualitativo vs Cuantitativo • Distintas técnicas de administración de riesgos
Identificar los diferentes marcos de control en ciberseguridad	Unidad III: La importancia de implementar un Marco de Control • Diferentes marcos de control en Ciberseguridad • ISO 27.002 e ISO 27032, Gestión de la Ciberseguridad • NIST Ciber Security Framework
Descubrir lo crítico que es mejorar la Cultura en Ciberseguridad de las organizaciones para mitigar este riesgo.	Unidad IV: El Factor Humano en Ciberseguridad • Diferencia entre educar, capacitar y sensibilizar • Distintos componentes asociados al Factor Humano en Ciberseguridad • Lo importante de medir el conocimiento, la actitud y comportamiento online para avanzar en un programa de Cambio Cultural en temas de Ciberseguridad • Estrategia de un programa de Cambio Cultural

Experimentar cómo funciona el negocio de las vulnerabilidades y las mejores prácticas de comunicación.	Unidad V: La Economía de las Vulnerabilidades • Ciclo de Gestión de Vulnerabilidad • Como funciona la economía de las vulnerabilidades • Distintos mecanismos de divulgación de vulnerabilidades • Análisis de Caso – La Economía de las Vulnerabilidades
Diferenciar entre las crisis de Emergencia, Crisis Estratégicas y Ciber crisis, y como las organizaciones deben estar preparadas para enfrentarlas	Unidad VI: Ciber Crisis – Cómo estar Preparados • Diferencia entre crisis de emergencia y crisis estratégica • Distintos factores que pueden llevar a una organización a una Crisis y Ciber crisis • Etapas de una Ciber Crisis • Simulación de Crisis y administración de escenarios • Análisis de Caso – EL Proyecto Phoenix
Relacionar los aspectos legales existentes en Ciberseguridad y los proyectos regulatorios en discusión.	Unidad VII – Aspectos Legales en Ciberseguridad • Nueva institucionalidad en materia de Ciberseguridad • Convenio de Budapest • Ley de Delitos Informáticos • Instructivos de Ciberseguridad • Protección de Infraestructura Crítica
Fomentar la importancia de la protección de datos, el ciclo de vida de estos y su relación con los temas de Ciberseguridad	Unidad VIII – Protección de Datos y Ciberseguridad • Fundamentos de Protección de Datos • Estrategia de Protección de Datos • Mapping de Datos • Privacy Impact Análisis (PIA) Gestión de Incidentes (Data Breach)
Relacionar los aspectos legales existentes en Protección de Datos y los proyectos regulatorios en discusión	Unidad IX – Aspectos Legales de Protección de Datos • Modelos Regulatorios por Industria (USA) • Modelos GDPR (General Data Protection Regulation) • Regulación y Proyecto de Ley en Chile. Reformas constitucionales.

Generar, a partir de los objetivos estratégicos de una organización, un marco de métricas en Ciberseguridad	Unidad X – Métricas en Ciberseguridad • Tipos de Métricas • Identificación de Audiencia (Estratégico vs Operacional) • Elaboración de Tendencias • Retorno de la Inversión

V. Orientaciones metodológicas

Se Aplicará Una Metodología Teórico-Práctica, donde los participantes aprenderán haciendo. En las exposiciones teóricas se usarán presentaciones Powerpoint y Estudios De Casos aplicables a las áreas de la seguridad.

En las horas prácticas se desarrollarán trabajos individuales y grupales, ejercicios de simulación, estudios de casos prácticos donde tendrán que aplicar la Materia revisada y las normas involucradas. Serán supervisados directamente por el profesor. Clase a clase se indicarán las referencias a los textos legales o normativa pertinentes a las materias que se discutan y a los diferentes tipos de riesgos cibernéticos.