PROGRAMA DEL CURSO

I. Identificación General

Nombre:	**Ciber Seguridad**
Horas:	2 horas
Destinatarios:	Directores, gerentes generales, gerentes de área, fiscales y toda persona que tenga un cargo de responsabilidad en una compañía.

II. Fundamentación Técnica

El tema de la ciber seguridad es un tema complejo y que toma cada día mayor relevancia, el ciber crimen seguirá creciendo y se cree que para el año 2019 el ciber crimen recolectará más de 3 trillones de dólares. Recientes estudios en Europa hablan de que el GDP de los países europeos se está viendo erosionado en mas de un 2% producto del ciber crimen. Por lo tanto, lo que tenemos que hacer, y la clave, es gestionar el riesgo y entender también, que la ciberseguridad no es un tema tecnológico, es un tema estratégico, de negocios, y que probablemente la mejor manera para enfrentar este riesgo es el management, teniendo un buen liderazgo de las personas dentro de las organizaciones, las cuales tendrán que liderar este nuevo escenario al cual nos vemos enfrentados.
En este curso entenderemos que la ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada. Es por esto, que se hace relevante que toda la organización, en especial sus líderes, comprendan la importancia de cuidar este importante activo.

III. Objetivo General

El participante identificará amenazas en las compañías para evitar ataques cibernéticos a partir de estrategias de ciberseguridad junto con la adopción de medidas de protección.

IV. Desarrollo

Objetivos Específicos	Contenidos
Reconocer la realidad nacional e internacional respecto a la ciberseguridad y la normativa de la protección de datos.	Unidad I: Panorama Internacional y Local - Política Internacional de ciber seguridad (GDPR) - Regulación europea de protección de datos - Política Nacional de Ciber Seguridad - Creación de agencia de protección de datos - Regulación de estructuras críticas - Multas al no cumplimiento - Figura del DPO
Relacionar la seguridad de la información con el concepto ciberseguridad.	Unidad II: Seguridad de la Información v/s Ciberseguridad - Seguridad de la información - Protección del activo digital - Concepto de Ciberseguridad - Seguridad de la información - Protección de confidencialidad - Integridad - Disponibilidad de los datos
Identificar la evolución y cambios de las amenazas en el ciber espacio.	Unidad III: Evolución de las Amenazas en el mundo actual - Ataques no sofisticados (scrip kiddies) - APT (advanced persistent treet) - Vectores de ataques en la actualidad: Fishing, cibercriminales, espionaje entre países, hacktivismo
Comprender las estrategias de ciberseguridad de acuerdo a la realidad de la compañía.	Unidad IV: Estrategia de Ciberseguridad y Gestión de Riesgos - Estrategia de ciberseguridad: - A qué se refiere defender o controlar - Activos digitales de la organización - Presupuesto necesario - Qué Frame work utilizar - Apetito al riesgo en ciberseguridad - Cultura de ciberseguridad - Plan de gestión de incidentes - Plan de ciber crisis - Por qué implementar un frame work de seguridad: - ISO 27001 / 27002 Versión 2013 - NIST cibersecurity frame work 2014 - Qué estrategias implementar en la organización - Diseñar defensas para detectar y retrasar ataques. - Servidores Honeypot - Seguridad en profundidad - Programa de Gestión de Riesgos

Analizar las medidas de protección que tiene la compañía ante un ciber ataque	Unidad V: Cerrando el GAP: Sofisticaciones y Medidas de Protección. - GAP: Ciber ataques mejoran rápidamente/ ciberdefensas mejoran gradualmente. - Disminución del GAP: 1.- Awarness, cambio de comportamiento y cambio cultural - Caso Enron en EEUU 2.- Gobernabilidad - Administración de riesgos 3.- Ciber Crisis - Administración de la crisis: - Liderazgo en crisis - Toma de decisiones - Comunicaciones / redes sociales - Grupos de interés afectados 4.- Ciber Forensic 5.- Monitoreo del servidor y las redes 6.- Protección Legal - Impacto de las regulaciones en las organizaciones: - Gobernabilidad - Operacional - Tecnológico - Legal 7.- Ciber Insurance