Seguridad de la Información, Ciberseguridad y Protección de Datos

FUNDAMENTACIÓN TÉCNICA DEL PROGRAMA

Actualmente existe una gran cantidad de incidentes relacionados con la fuga de información, robo de datos bancarios, extracción de bases de datos privadas o daños a los sistemas informáticos de diferentes organizaciones, por esta razón, se deben adoptar medidas orientadas a educar y capacitar al personal que trabaja en áreas técnicas en materias de ciberseguridad.

El curso de Introducción a la Ciberseguridad y Protección de Datos Personales es la base para entender sobre las nuevas amenazas que afectan a los sistemas de información, materializando diversas estrategias y políticas que permitan prevenir daños en cualquier organización.

DESCRIPCIÓN DEL PROGRAMA

El programa contempla un nivel de profundidad, para personas con básico conocimiento hasta un conocimiento medio en el área de la seguridad de la información, ciberseguridad y protección de datos personales. El nivel contempla cinco unidades de aprendizaje en modalidad e-learning, que abordan desde lo conceptual, hasta lo práctico, permitiendo al estudiante avanzar por cada fase para la creación de una estrategia de Ciberseguridad, entendiendo los riesgos y medidas necesarias para el control de estas medidas, cómo se gestionan y norman de acuerdo con lo estipulado en el Instructivo presidencial nº08, el Decreto 83 y la ISO27001.

OBJETIVO GENERAL

Dotar de nuevas competencias, dependiendo del nivel de conocimiento de cada participante, en el ámbito de la ciberseguridad, seguridad de la información y protección de datos personales; fundamentando conceptos y aplicando técnicas para la implementación de un modelo de Gestión de Seguridad de la Información en diversos ambientes.

DIRIGIDO A

Funcionarios y empleados del sector público y privado en un nivel: básico - intermedio; que deseen implementar tanto una estrategia, como políticas de Ciberseguridad, considerando como base el Instructivo presidencial nº08, el Decreto 83 y la ISO27001.

REQUISITOS DE INGRESO

Manejo en el área de Informática, o bien, tener conocimientos básicos previos de seguridad de la información a nivel teórico y práctico, de acuerdo con los resultados del test diagnóstico.

CARACTERÍSTICAS DEL PROGRAMA

Lugar de Ejecución:	**Plataforma Blackboard Collaborate Ultra,** Campus Virtual de Universidad Mayor, plataforma por excelencia en e-Learning, con la cual tendrán acceso al material, sesiones, comunidades y evaluaciones; además de estar en contacto permanente con la Universidad, docentes y compañeros de curso.
Modalidad:	En línea por sesiones virtuales sincrónicas en Campus Virtual, con interacción permanente.
Duración:	16 horas cronológicas – 21 horas pedagógicas
ID Convenio Marco:	1637440

CONTENIDOS DEL PROGRAMA

Unidad de Aprendizaje 1: Principios de la Ciberseguridad

Objetivo Específico: Los estudiantes comprenderán los diferentes principios en torno a la Ciberseguridad, junto a una propuesta de implementación para sus distintas funciones.

Total de Horas:
Nº de Horas Teóricas: 01 hra.

Contenidos:
- Conceptos Ciber
- Propuesta de funciones
- Conceptos claves de la seguridad de la información.

Unidad de Aprendizaje 2: Aspectos legales de la Ciberseguridad

Objetivo Específico: Los estudiantes comprenderán sobre aspectos legales referentes a la Ciberseguridad en base a la política nacional vigente y las consideraciones necesarias para abordar, controlar e implementar estrategias de Ciberseguridad en una organización.

Total de Horas:
Nº de Horas Teóricas: 02 hra.
Nº de Horas Practicas: 01 hra.

Contenidos:
- Protección de datos personales.
- Seguridad en sistemas operativos y aplicaciones.
- Desarrollo organizacional.
- Política Nacional de Ciberseguridad y su convivencia con la norma ISO27001, Instructivo Presidencial Nº 8 y decreto 83.
- Elaboración legal de una estrategia de Ciberseguridad

Unidad de Aprendizaje 3: Análisis de Ciberseguridad

Objetivo Específico: Los estudiantes podrán comprender cómo se realiza un análisis de incidentes, asociado a los boletines informativos de registro de incidentes.

Total de Horas:
Nº de Horas Teóricas: 01 hrs.
Nº de Horas Práctica: 01 hrs.

Contenidos:
- Introducción y conceptos asociados a el análisis de incidentes.
- Herramientas asociados a la seguridad.
- Práctica en plataforma para hacer análisis de archivos maliciosos.

Unidad de Aprendizaje 4: Análisis de riesgos y servicios WEB

Objetivo Específico: Los estudiantes entenderán algunas herramientas de análisis de aplicaciones web para poder determinar sus vulnerabilidades.

Total de Horas:
Nº de Horas Teóricas: 04 hrs.
Nº de Horas Prácticas: 02 hrs.

Contenidos:
- Funcionamiento de las aplicaciones web y su relación con la seguridad de la información.
- Vulnerabilidades que puedan afectar a las aplicaciones web.
- Análisis de vulnerabilidades en aplicaciones web.

Unidad de Aprendizaje 5: Ciberseguridad en ambientes reales

Objetivo Específico: Los estudiantes aplicaran medidas de seguridad en diferentes ambientes de trabajo tanto internos, como externos de la organización.

Total de Horas:
Nº de Horas Teóricas: 02 hrs.
Nº de Horas Prácticas: 02 hra.

Contenidos:
- Aplicación de la seguridad en entornos controlados y no controlados en la organización.
- Ciberseguridad personal para integrantes de la organización.
- Ejercicio aplicado de ciberseguridad.

METODOLOGÍA

Durante el tratamiento teórico del programa, los docentes se valdrán de recursos didácticos como presentaciones de diapositivas, información con material de apoyo visual en formato de texto, imágenes y videos explicativos, con el fin de que los estudiantes puedan integrar los conocimientos adquiridos en casos prácticos y, fomentando además la adquisición de los conocimientos teóricos mediante la implementación de una secuencia de enseñanza. Se realizarán actividades de aprendizaje prácticas. La actividad se iniciará con una acción guía por parte del docente a través de ejemplos, que deberá ser analizada por los participantes para promover el desarrollo colaborativo de soluciones y/o conclusiones, así como la preparación para las evaluaciones prácticas.

El docente supervisará cada actividad, donde los estudiantes desarrollarán trabajos utilizando diversas herramientas de software, con ejercicios de distintas dificultades y tipos de escenarios, donde aplicarán los conocimientos aprendidos, sistematizando sus conclusiones para aplicar a posibles casos de su entorno. Todas las actividades prácticas serán ejecutadas con el equipamiento del laboratorio de computación, dispuesto para los estudiantes de este curso.

EVALUACIÓN

- Al inicio del curso se realizará una evaluación por medio de una prueba diagnóstica; para determinar el nivel de los estudiantes, la cual será ajustada y evaluada nuevamente al término del curso, de tal forma de obtener la brecha.
- Al término del quinto módulo será realizado un trabajo aplicado final, el cual determinará la nota final correspondiente al curso.
- Se aprueba con un 75% de asistencia online.

MATERIAL DE APOYO ACADÉMICO

El material instruccional, basado en la literatura relacionada con cada unidad de aprendizaje, estará a disposición de los estudiantes en la plataforma virtual.

EQUIPO ACADÉMICO

CRISTIAN BARRÍA HUIDOBRO

Postdoctorado (e) en Alta Investigación en Educación Multicultural de la Universidad de San Buena Ventura de Cali (Colombia); Doctor en Ingeniería Informática de la Pontificia Universidad Católica de Valparaíso; Magíster en Ciencias de la Ingeniería Informática de Pontificia Universidad Católica de Valparaíso; Magíster en Gestión y Planificación Educacional de la Universidad Diego Portales.

PEDRO HUICHILAF ROA

Magíster Derecho Informático y de las Telecomunicaciones (E). Licenciado en Ciencias Jurídicas y Sociales. Ex Subsecretario de Telecomunicaciones de Chile.

LORENA GALEAZZI AVALOS

Magíster en Seguridad de la Información. Ingeniero en Conectividad y Redes. Técnico en Administración de Redes. Técnico en Electrónica en Telecomunicaciones.

SAUL ORTEGA ALVARADO (MÉXICO)

Ingeniero en Telemática, Técnico en Sistemas Digitales por el Instituto Politécnico Nacional en México, Investigador del Centro de Investigación en Ciberseguridad, Especialista en Google Cloud y seguridad en la nube. CIO en NetMex Compañía de innovación en TI México.

JOSÉ CARDONA CAICEDO (COLOMBIA)

Máster en Seguridad Informática, Universidad de la Rioja - España, Ingeniero en Electrónica y Comunicaciones Universidad del Cauca – Colombia.

CERTIFICACIÓN

Al finalizar el programa, cada alumno que cumpla con el porcentaje mínimo de asistencia establecido y las evaluaciones que contempla el programa, recibirá un Certificado, detallando el programa realizado y el número de horas completados.