Maestría en Ciberseguridad

Estrategia Aplicada a la Ciberseguridad

Gobierno de la Ciberseguridad
La finalidad de este curso es que los participantes desarrollen competencias para implementar y gestionar un gobierno efectivo de la ciberseguridad en sus organizaciones. Se explorarán los fundamentos del gobierno corporativo y su aplicación en la seguridad de la información, así como la importancia de la alineación con los objetivos estratégicos.
Los temas a desarrollar incluyen: Principios de Gobierno Corporativo, Marcos de Referencia en Ciberseguridad (COBIT, ISO 27001), Políticas, Normas y Procedimientos. Roles y Responsabilidades en el Gobierno de la Ciberseguridad, Monitoreo y Evaluación del Desempeño.

Presupuesto y Financiamiento de Ciberseguridad
La finalidad de este curso es que los participantes desarrollen las competencias necesarias para planificar y gestionar presupuestos en ciberseguridad. Se estudiarán los principios de análisis de costos, priorización de inversiones, y justificación financiera en proyectos de ciberseguridad.
Los temas a desarrollar incluyen: Introducción al Presupuesto en Ciberseguridad, Modelos de Costos Directos e Indirectos, Priorización de Inversiones en Ciberseguridad, Herramientas de Análisis de Retorno de Inversión (ROI), Estrategias de Financiamiento para Proyectos de Seguridad.

Planeamiento Estratégico y Manejo de KPI´s
La finalidad de este curso es introducir, analizar y aplicar aspectos claves relativos a la planificación estratégica de los negocios alineados a soluciones de Ciberseguridad y específicamente al proceso de formulación y toma de decisiones estratégicas con un seguimiento de indicadores. Estructurar una forma de pensar estratégica a través de un modelo secuencial de pasos a seguir para de una situación presente lograr una situación futura deseada.

Gestión de Servicios de TI y la Ciberseguridad
La finalidad de este curso es, ahondar en la comprensión de la identificación de nuevas amenazas basados en la gestión de recursos y servicios que se brindan dentro del crecimiento de las tendencias digitales basado en estándares. El participante desarrolla competencias para asumir roles de liderazgo para las propuestas de iniciativas, programas y planes que respondan a las necesidades de Ciberseguridad con capacidad de resiliencia y habilidad.

Cultura de Ciberseguridad y Gestión del Cambio
La finalidad de este curso es que los participantes comprendan la importancia de fomentar una cultura organizacional orientada a la ciberseguridad. Se abordarán temas relacionados con los factores humanos en la seguridad, la resistencia al cambio y las estrategias para gestionar la adopción de prácticas seguras en las organizaciones. Los temas a desarrollar incluyen: Introducción a la Cultura Organizacional en Ciberseguridad, Factores Humanos y la Psicología del Cambio, Planificación y Gestión del Cambio Organizacional, Estrategias para el Desarrollo de una Cultura de Ciberseguridad, Indicadores para Medir el Impacto Cultural.

Gestión Estratégica para el Desarrollo Seguro
La finalidad de este curso es identificar y mitigar los riesgos desde la concepción del diseño hasta la implementación y el mantenimiento con un análisis y pensamiento lógico, así como creativo, siendo de alto impacto para garantizar que el software sea resistente a ataques y vulnerabilidades.

Gestión de la Ciberseguridad

Estándares de Seguridad de Información
La finalidad del curso es conocer los estándares de ciberseguridad a gobierno, gestión, control y estándares técnicos de ciberseguridad

Data Security: Protección de Información
La finalidad del curso es conocer los conceptos, métodos, técnicas y herramientas relacionadas con la Seguridad de los datos

Control de Accesos y Gestión de Identidades
La finalidad es proporcionar una formación completa y cualificada en sistemas de control de accesos, desde el punto de vista del diseño, instalación, puesta en marcha y mantenimiento de los mismos.

Seguridad Defensiva de la Información
La finalidad del curso es conocer los conceptos, métodos, técnicas y herramientas relacionadas con la Seguridad Defensiva de la Información

Arquitectura de Ciberseguridad
La finalidad del curso es conocer los conceptos, métodos, técnicas y herramientas relacionadas con la Arquitectura de Ciberseguridad

Tendencias Emergentes en Ciberseguridad
La finalidad del curso es que el participante conozca las tendencias emergentes en ciberseguridad, tanto del punto de vista de amenazas como de las medidas de protección

Seguridad Ofensiva de la Información
La finalidad del curso es conocer los conceptos, métodos, técnicas y herramientas relacionadas con la Seguridad Ofensiva de la Información

INTEGRACIÓN CON EL NEGOCIO

Gestión de Crisis y Respuesta ante Incidentes
La finalidad es aprender a desarrollar y ejecutar una real capacidad de gestión de crisis para la organización utilizando un marco de mejores prácticas establecido a través del desarrollo y compresión de los principios, estrategias y técnicas de respuesta a incidentes y gestión de crisis

Risk Management: Gestión de Riesgos
La finalidad de este curso es que los participantes comprendan los principios y procesos esenciales para la gestión de riesgos en ciberseguridad. El curso aborda temas clave como la identificación y análisis de vulnerabilidades, la evaluación de riesgos, y el diseño de planes de mitigación en un contexto organizacional. Los temas a desarrollar incluyen: Introducción a la Gestión de Riesgos, Métodos de Identificación y Evaluación de Riesgos (ISO 31000, NIST), Planificación de Respuesta a Incidentes, Herramientas de Monitoreo y Control de Riesgos.

Ciberseguridad en la Nube
La finalidad del curso es conocer los conceptos, métodos, técnicas y herramientas relacionadas con la Seguridad de las plataformas de Nube

Ciberseguridad en Entornos Industriales
La finalidad del curso es identificar los conceptos sistemas y procesos industriales, la importancia de la ciberseguridad identificando vulnerabilidades aplicando herramientas, normas y estándares globales de Ciberseguridad Industrial

Aspectos Legales y Regulatorios
La finalidad del curso es conocer y comprender los instrumentos jurídicos y legislación vigente del ecosistema TIC y economía digital. El participante desarrolla sus conocimientos del marco jurídico, normativo y regulatorios, en el contexto de la regulación en materia de cibercrimen y esto le permitirá de base en la estrategia de soluciones de seguridad basado en sus deberes y derechos en temas vinculados al conocimiento e implementación de actividades de ciberseguridad.

Plan de Continuidad de negocio
La finalidad de este curso es analizar y comprender en forma profunda los procesos y prácticas esenciales para la gestión efectiva de incidentes de ciberseguridad. aprendiendo a identificar, analizar, responder y recuperarse de incidentes de seguridad, minimizando el impacto en las organizaciones y asegurando la continuidad del negocio

Ciberinteligencia y Gestión de Amenazas
La finalidad del curso es conocer los conceptos, métodos, técnicas y herramientas relacionadas con la Ciberinteligencia y gestión de amenazas

Compliance: Cumplimiento Normativo
La finalidad de este curso es que los participantes comprendan el marco normativo y regulatorio que rige la ciberseguridad, con un enfoque práctico en la evaluación de casos reales y en el diseño de políticas de cumplimiento. Los temas a desarrollar incluyen: Introducción al Compliance en Ciberseguridad, Normativas Internacionales y Locales (GDPR, PCI DSS, ISO 27001), Marco Legal Peruano en Ciberseguridad, Auditoría y Evaluación de Cumplimiento, Ética y Responsabilidad en Ciberseguridad.

Liderazgo e Innovación

Innovación y Design Thinking
La innovación se ha convertido en una incipiente necesidad en la gestión digital para evolucionar en entornos cada vez más dinámicos. Las estrategias y métodos tradicionales para la gestión, están dando paso a metodologías conocidas como “lean” en las que, la creatividad y el pensamiento de diseño se convierten en los motores y dónde el centro de todo desarrollo se enfoca en las personas (A Human centered design).

Mindset para el Liderazgo

En este curso se busca que los participantes desarrollen su capacidad para ejercer cambios en su entorno como líderes en Ciberseguridad. En ese sentido, a partir de la identificación de los aspectos claves para propiciar transformación, autoconocimiento, ejercicio del diálogo y desarrollo de técnicas de influencia, los participantes incrementarán sus habilidades para constituirse en agentes de cambio en la gestión digital

Presentaciones de Alto Impacto

La comunicación es una herramienta estratégica para la gestión y dirección de empresas. La transmisión clara de idea, asertividad, y las estrategias de comunicación son vitales para el logro de los objetivos empresariales.

Lego Serious Play

La gestión de ciberseguridad se realiza en un entorno de constante cambio, lo cual requiere el desarrollo de habilidades blandas (Soft Skills) para afrontar esta realidad. Por ello, es importante identificar herramientas que permitan innovar y transformar la visión de los profesionales del sector de ciberseguridad.

Investigación

Proyecto de Investigación I

La finalidad de este curso es introducir y guiar a los estudiantes en el desarrollo de trabajos de investigación aplicados a ciberseguridad. Se enfoca en la identificación de problemas relevantes, la formulación de preguntas de investigación, la definición de objetivos y la delimitación del alcance del trabajo.

Proyecto de Investigación II

La finalidad de este curso es permitir a los estudiantes construir el marco teórico y diseñar el marco metodológico de su trabajo de investigación. También incluye la recolección inicial de datos con el uso de herramientas tecnológicas especializadas.

Proyecto de Investigación III

La final de este curso es completar el proceso de investigación, enfocándose en el análisis de resultados, la aplicación práctica del proyecto y la preparación para la defensa oral. También abarca la redacción del informe final.