

## PROGRAMA CURSO FUNDAMENTOS DE CIBERSEGURIDAD

<b>Relator</b>	Mario Augusto Villanueva Alveal		
<b>Modalidad</b>	Online	<b>Horas</b>	18 horas sincrónicas
<b>Fecha de inicio</b>	22/04/2024	<b>Fecha de termino</b>	16/06/2024

Sesión	Contenido	Actividad
<p><b>Sesión 01: "Las redes están bajo ataque"</b> (Módulos N°1 y 2) <b>Lunes 22 de abril</b> <b>15:00 a 17:00</b></p>	<ul style="list-style-type: none"> <li>Amenazas Comunes.</li> <li>Ataques, Conceptos y Técnicas</li> <li>Las redes como Objetivo.</li> </ul>	<ul style="list-style-type: none"> <li>Conceptos básicos y la importancia de la ciberseguridad en el mundo actual.</li> <li>Revisiones técnicas comunes de ataque, como phishing, malware, y ataques de denegación de servicio.</li> <li>Revisión conceptual de las diferentes áreas de la ciberseguridad, como la seguridad de redes, la criptografía, la seguridad de aplicaciones.</li> <li>Revisión de diferentes métodos de infiltración.</li> </ul>
<p><b>Sesión 02: Sistemas Operativos.</b> (Módulos N.º 7 y 8) <b>Miércoles 24 de abril</b> <b>15:00 a 17:00</b></p>	<ul style="list-style-type: none"> <li>Sistema Operativo Windows</li> <li>Sistema Operativo GNU/Linux.</li> </ul>	<ul style="list-style-type: none"> <li>Revisión de Historia.</li> <li>Revisión de recomendaciones de Seguridad para Windows.</li> <li>Revisión Arquitectura, Sistemas de archivos e inicio de Windows.</li> <li>Revisión de uso de recursos.</li> <li>Nociones básicas de GNU/Linux.</li> <li>Administración básica de GNU/Linux</li> <li>Sistemas de Archivos.</li> <li>Revisión de GUI.</li> </ul>
<p><b>Sesión 03: Principios, prácticas y procesos de ciberseguridad.</b> (Módulos N.º 10) <b>Lunes 29 de abril</b> <b>15:00 a 17:00</b></p>	<ul style="list-style-type: none"> <li>Triada de la ciberseguridad.</li> <li>Estados de los Datos.</li> <li>Prácticas de Seguridad.</li> </ul>	<ul style="list-style-type: none"> <li>Revisión de CID y sus fundamentos.</li> <li>Revisión del ciclo de vida de la información y sus mecanismos de protección.</li> <li>Revisión de buenas prácticas y normas</li> </ul>

<p><b>Sesión 04:</b> Principios, prácticas y procesos de defensas en redes. (Módulos N.º: 11, 12 y 13) <b>Miércoles 8 de mayo</b> <b>15:00 a 17:00</b></p>	<ul style="list-style-type: none"> <li>Defensa en profundidad.</li> <li>Gestión de Operaciones de Ciberseguridad.</li> <li>Políticas, Regulaciones y Estándares de Seguridad.</li> <li>Gestión de operaciones en ciberseguridad.</li> <li>Mecanismos de gestión de acceso.</li> </ul>	<ul style="list-style-type: none"> <li>Definición de activos, vulnerabilidades y amenazas.</li> <li>Clasificación de activos.</li> <li>Identificación de amenazas.</li> <li>Revisión de la gestión en niveles: Físicos y de aplicación,</li> <li>Revisión de los modelos de resiliencia en ciberseguridad.</li> <li>Revisión de mecanismos para la prevención y control de acceso.</li> </ul>
<p><b>Sesión 05:</b> MasterClass Cisco.</p>	<ul style="list-style-type: none"> <li>.</li> </ul>	<ul style="list-style-type: none"> <li>.</li> </ul>
<p><b>Sesión 06:</b> Seguridad en la Nube. (Modulo N.º 17) <b>Miércoles 22 de mayo</b> <b>15:00 a 17:00</b></p>	<ul style="list-style-type: none"> <li>Virtualización y computación en la nube.</li> <li>Seguridad de la infraestructura en la nube.</li> <li>Seguridad de aplicaciones en la nube.</li> <li>Seguridad de los datos en la nube.</li> </ul>	<ul style="list-style-type: none"> <li>Conocer distintos entornos de virtualización.</li> <li>Conocer los fundamentos de la computación en la nube.</li> <li>Conocer las responsabilidades sobre la seguridad de la infraestructura en la nube.</li> <li>Revisión de la importancia en la validación, control, y integridad en APPs.</li> </ul>
<p><b>Sesión 07:</b> Criptografía. (Módulo N.º: 18) <b>Lunes 27 de mayo</b> <b>15:00 a 17:00</b></p>	<ul style="list-style-type: none"> <li>Criptografía y su relación con la confidencialidad.</li> <li>Técnicas de enmascaramiento de datos.</li> <li>Uso de hashes</li> <li>Criptografía de clave pública.</li> <li>Autoridades del sistema de confianza de PKI</li> </ul>	<ul style="list-style-type: none"> <li>Conocer los tipos de cifrados de datos.</li> <li>Revisión de que es la Esteganografía.</li> <li>Revisión del uso de hashes en el día a día.</li> <li>Revisión de los usos de la criptografía de clave pública.</li> </ul>
<p><b>Sesión 08:</b> Evaluación de alertas. (Módulos N.º: 19, 20 y 21) <b>Miércoles 29 de junio</b> <b>15:00 a 17:00</b></p>	<ul style="list-style-type: none"> <li>Protocolos de monitoreo.</li> <li>Tipos de datos.</li> <li>Fuentes de alertas.</li> </ul>	<ul style="list-style-type: none"> <li>Revisión de los protocolos más comunes usados para el monitoreo de red.</li> <li>Revisión de los tipos de datos asociados a monitoreo, alertas y registros.</li> </ul>

		<ul style="list-style-type: none"><li>• Revisión de herramientas de recopilación, análisis de alertas.</li></ul>
<p><b>Sesión 09: Respuesta a un incidente.</b> (Módulos N.º: 24, 26, 27) <b>Lunes 3 de junio</b> <b>15:00 a 17:00</b></p>	<ul style="list-style-type: none"><li>• Inteligencia sobre amenazas.</li><li>• Tipos de riesgos.</li><li>• Manejos de Evidencia.</li><li>• Respuesta a incidentes.</li></ul>	<ul style="list-style-type: none"><li>• Revisión de fuentes de información y servicios sobre inteligencia de amenazas.</li><li>• Conocer como establecer los niveles de riesgos en activos de valor.</li><li>• Conocer labores y procesos asociados a la informática forense.</li><li>• Conocer mecanismos para establecer una capacidad de respuesta a incidentes.</li></ul>