| 1.- Identificación de la Unidad de Aprendizaje | | | | | |
|---|---|---|---|---|---|
| **Nombre de la Unidad de Aprendizaje** | | | | | |
| Ciberseguridad | | | | | |
| **Clave de la UA** | **Modalidad de la UA** | **Tipo de UA** | | **Valor de créditos** | **Área de formación** |
| IF433 | Presencial | Curso-Taller | | 6 | CISA |
| **Hora semana** | | **Horas teoría/semestre** | **Horas práctica/ semestre** | **Total, de horas:** | **Seriación** |
| 3 | | 32 | 30 | 62 | |
| **Departamento** | | | **Academia** | | |
| Justicia Alternativa, Ciencias Forenses y Disciplinas Afines al Derecho | | | | | |

**Presentación**

La Ciberseguridad es uno de los temas de mayor relevancia para gobiernos y organizaciones privadas en todo el mundo. Por consiguiente, en los últimos años se ha incrementado significativamente la demanda de talento en Ciberseguridad a nivel mundial no satisfecho con la oferta actual de profesionales. Dicha brecha se acentuó a raíz de los cambios suscitados en las formas de trabajo luego de la pandemia y la aceleración de los procesos de transformación digital y agilidad en las organizaciones. Asimismo, se han incrementado y complejizado las amenazas a las que están expuestas las infraestructuras.

El cumplimiento con las normativas y regulaciones en materia de privacidad exige niveles de conocimiento técnico y de gestión para impulsar y adoptar medidas técnicas y organizativas a fin de dar cumplimiento a lo requerido por las mismas.

| Tipos de saberes | | |
|---|---|---|
| Saber<br>(Conocimientos) | Saber hacer<br>(Habilidades) | Saber ser<br>(Actitudes y valores) |
| Estándares básicos de seguridad y el correcto seguimiento del protocolo.<br><br>Aplicación de auditorías de seguridad y de las herramientas de análisis forense.<br><br>Legislación y regulación de la seguridad en entornos tecnológicos y de información.<br><br>Técnicas de análisis de sistemas de información, redes de comunicación, aplicaciones web y dispositivos móviles.<br><br>Desarrollo y utilización de código para la detección y arreglo de vulnerabilidades en sistemas de seguridad. | Detección de amenazas a los sistemas de información y la subsecuente gestión de operaciones para proteger los datos.<br>Creación de planes de prevención y contingencia ante amenazas de seguridad.<br>Hacer uso ético de las herramientas y protocolos necesarios con el fin de mantener una actitud de servicio, integridad y confidencialidad.<br>Aplicación de pensamiento sistémico en la resolución de problemas.<br>Uso de herramientas de cómputo para el desarrollo de estrategias de ciberseguridad.<br>Comunicación asertiva en ámbito organizacional.<br>Adaptación en contextos internacionales de tecnología y negocios.<br>Autogestión del aprendizaje. | Pensamiento emprendedor y crítico.<br>Capacidad de solución de problemas y manejo de recursos.<br>Gusto por mantenerse a la vanguardia de las tecnologías de seguridad.<br>Liderazgo en equipos de trabajo multidisciplinarios.<br>Interés de mantenerse actualizado en herramientas y tecnologías de software.<br>Ética profesional y responsabilidad social. |

| Competencia genérica | Competencia profesional |
|---|---|
| Análisis y seguimiento de pistas | Evalúa la información documental y digital en entornos reales o virtuales, con herramientas tecnológicas y de comunicación, mediante técnicas de investigación para la reconstrucción de hechos o estimación de amenazas. |
| **Saberes previos del alumno** | |
| Respuesta ágil a situaciones imprevistas de trabajo y la vida cotidiana<br>Autogestión del aprendizaje.<br>Entender lenguajes en código.<br>Pensamiento lógico y crítico | |

| Perfil deseable del docente |
| --- |
| Conocimientos:<br>- Tratamiento de evidencias digitales<br>- Conocimiento en los roles y áreas de especialización del investigador de evidencia digital |
| Organización y capacidad de trabajar bajo presión.<br>Afinidad por el manejo de herramientas tecnológicas. |

| **Perfil de egreso al que se abona** |
| --- |
| Realiza trabajo en equipo de manera interdisciplinaria y multidisciplinaria y cuenta con las herramientas de liderazgo para la coordinación de equipos de investigación.<br><br>Emite reportes de auditorías con base en el análisis, interpretación y síntesis de información documental y digital, mediante uso de tecnologías de la información y comunicación. |

| **Contenido** |
| --- |
| Unidad 1. Introducción<br>1.1 Antecedentes<br>1.2 Ciberdelincuencia:<br>1.2.1 Hacktivismo<br>1.2.2 Hackers<br>1.2.3 Crackers<br>1.2.4 Phreakers<br>1.2.5 Ciberdelincuente<br><br>Unidad 2. Servicios y mecanismos de seguridad<br>2.1 Servicios de seguridad<br>2.1.1 Autenticación<br>2.1.2 Control de acceso<br>2.1.3 Confidencialidad<br>2.1.4 Integridad de datos<br>2.1.5 No repudio<br>2.1.6 Disponibilidad<br>2.2 Mecanismos de seguridad<br>2.2.1 Cifrado<br>2.2.2 Firma digital<br>2.2.3 Integridad de datos<br>2.2.4 Relleno de tráfico<br>2.2.5 Funciones hash<br>2.2.6 Códigos de autenticación<br>2.2.7 Certificados digitales<br><br>Unidad 3. Análisis de vulnerabilidades<br><br>3.1 Code execution<br>3.2 DoS<br>3.3 Overflow |

3.4 Sql injection
3.5 XSS
3.6 Directory trnasversal
3.7 CSRF
3.8 Bypass something

Unidad 4.Métricas y estándares de ciberseguridad
4.1 CVSS
4.2 CVE
4.3 BishopFox
4.4 ISO27001 Sistema de Gestión de Seguridad de la Información
4.5 PCI-DSS
4.6 ISO 31000

**Estrategias generales para impartir la unidad de aprendizaje**

Diapositivas de PowerPoint, figuras, gráficos, esquemas, imágenes o videos..

**Módulo I. Introducción**

Unidad 1. Introducción
1.1 Antecedentes
1.2 Ciberdelincuencia:
- 1.2.1 Hacktivismo
- 1.2.2 Hackers
- 1.2.3 Crackers
- 1.2.4 Phreakers
- 1.2.5 Ciberdelincuente

**Competencia Específica**

Pensamiento crítico

**Tipos de saberes**

| Saber (Conocimientos) | Saber hacer (Habilidades) | Saber ser (Actitudes y valores) |
|---|---|---|
| Identificar los diferentes perfiles de Ciberdelincuencia | Autogestión del aprendizaje. | Pensamiento crítico |

| Módulo II. Servicios y mecanismos de seguridad | | |
|---|---|---|
| Unidad 2. Servicios y mecanismos de seguridad<br>2.1 Servicios de seguridad<br>2.1.1 Autenticación<br>2.1.2 Control de acceso<br>2.1.3 Confidencialidad<br>2.1.4 Integridad de datos<br>2.1.5 No repudio<br>2.1.6 Disponibilidad<br>2.2 Mecanismos de seguridad<br>2.2.1 Cifrado<br>2.2.2 Firma digital<br>2.2.3 Integridad de datos<br>2.2.4 Relleno de tráfico<br>2.2.5 Funciones hash<br>2.2.6 Códigos de autenticación<br>2.2.7 Certificados digitales | | |
| **Competencia Específica** | | |
| Capacidad de solución de problemas y manejo de recursos. | | |
| **Tipos de saberes** | | |
| Saber<br>(Conocimientos) | Saber hacer<br>(Habilidades) | Saber ser<br>(Actitudes y valores) |
| Definir y describir las propiedades de la información y sus métodos para asegurar su autenticidad. | Creación de planes de prevención y contingencia ante amenazas de seguridad. | Capacidad de solución de problemas y manejo de recursos. |

| Módulo III Análisis de vulnerabilidades |
|---|
| Unidad 3. Análisis de vulnerabilidades<br><br>3.1 Code execution<br>3.2 DoS<br>3.3 Overflow<br>3.4 Sql injection<br>3.5 XSS<br>3.6 Directory trnasversal<br>3.7 CSRF<br>3.8 Bypass something |
| **Competencia Específica** |

| |
|---|
| Interés de mantenerse actualizado en herramientas, tecnologías y técnicas para detección de ataques informáticos. |

| **Tipos de saberes** | | |
|---|---|---|
| Saber<br>(Conocimientos) | Saber hacer<br>(Habilidades) | Saber ser<br>(Actitudes y valores) |
| Desarrollo y utilización de código para la detección y arreglo de vulnerabilidades en sistemas de seguridad. | Detección de amenazas a los sistemas de información y la subsecuente gestión de operaciones para proteger los datos. | Interés de mantenerse actualizado en herramientas, tecnologías y técnicas para detección de ataques informáticos. |

| **Módulo IV Métricas y estándares de ciberseguridad** |
|---|
| Unidad 4.Métricas y estándares de ciberseguridad<br>4.1 CVSS<br>4.2 CVE<br>4.3 BishopFox<br>4.4 ISO27001 Sistema de Gestión de Seguridad de la Información<br>4.5 PCI-DSS<br>4.6 ISO 31000 |
| **Competencia Específica** |
| Hacer uso ético de las herramientas y protocolos necesarios con el fin de mantener una actitud de servicio, integridad y confidencialidad. |

| **Tipos de saberes** | | |
|---|---|---|
| Saber<br>(Conocimientos) | Saber hacer<br>(Habilidades) | Saber ser<br>(Actitudes y valores) |
| Estándares básicos de seguridad y el correcto seguimiento del protocolo. | Hacer uso ético de las herramientas y protocolos necesarios con el fin de mantener una actitud de servicio, integridad y confidencialidad. | Gusto por mantenerse a la vanguardia de las tecnologías de seguridad. |

| **Bibliografía básica** |
|---|
| NAVA, Alberto (2019). Ciberdelitos. Tirant Lo Blanch.<br>Stewart , J. Michael (2020) Network Security, Firewalls, and VPNs.<br>Mukherjee, Aditya (2020) Network Security Strategies.<br>Select Proceedings of the International Conference (2023). Information Security, Privacy and Digital Forensics.<br>Cisco Certified CyberOps Associate 200-201 Certification Guide: Learn blue teaming strategies and incident response techniques to mitigate cybersecurity incidents. (2021). |

How to Measure Anything in Cybersecurity Risk (2023).

**Bibliografía complementaria**


Gilman, Evan (2017) Zero Trust Networks.
McClure, Stuart (2010). “Hackers 6: secretos y soluciones de seguridad en redes”.
Cheswick, W. R. (2003). A Security Review of Protocols: Lower Layers.Firewalls and Internet Security: Repelling the Wily Hacker(19-40).
Clancy, Thomas (2018). Cyber Crime and Digital Evidence: Materials and Cases.
NIST Cybersecurity Framework: A pocket guide. (2018).
MITNICK, Kevin (2005). The art of intrusion. John Wiley & Sons
MITNICK, Kevin (2001). The art of deception. John Wiley & Sons


## 3.-Evaluación

**Criterios de Evaluación (% por criterio)**

1. EVALUACIÓN DIAGNÓSTICA
Sin valor acreditable. Aplicada al inicio de cada etapa con la finalidad de identificar los conocimientos previos que posee el estudiante sobre el tema respectivo de etapa.

2. EVALUACIÓN FORMATIVA
Comprende todas las actividades relacionadas con el programa y realizadas por el estudiante, mismas que dan cuenta de su proceso de aprendizaje a lo largo del semestre. Las actividades se evalúan cuantitativamente.

3. EVALUACIÓN SUMATIVA
Para su determinación se toman en cuenta los criterios de desempeño reflejados en las evidencias individuales: Exámenes departamentales, exámenes parciales, actividades de clase, tareas y un proyecto de investigación.

4. EVALUACIÓN CONTINUA
Obtener una calificación suficiente aplicando los criterios que se especifican a continuación:

| Criterio | Porcentaje |
|---|---|
| Tareas | 40 % |
| Reporte de prácticas | 50 % |
| Participación en clase | 10 % |
| | |
| **TOTAL** | **100%** |
| | |

## 4.-Acreditación

En concordancia con la normativa universitaria, la asistencia a las actividades presenciales es obligatoria y la participación del alumno en todas las actividades docentes se valorará positivamente en la calificación final. Por ello, será necesario: 1. Haber asistido al menos al 80% de clases magistrales y tutorías 2. Haber realizado su proyecto de investigación y entregado dicho documento.

Lo anterior de acuerdo al REGLAMENTO GENERAL DE EVALUACIÓN Y PROMOCIÓN DE ALUMNOS DE LA UNIVERSIDAD DE GUADALAJARA que señala: Artículo 5. El resultado final de las evaluaciones será expresado conforme a la escala de calificaciones centesimal de 0 a 100, en números enteros, considerando como mínima aprobatoria la calificación de 60. Las materias que no son sujetas a medición cuantitativa, se certificarán como acreditadas (A) o no acreditadas (NA).

Artículo 20. Para que el alumno tenga derecho al registro del resultado final de la evaluación en el periodo ordinario, establecido en el calendario escolar aprobado por el H. Consejo General Universitario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente, y II. Tener un mínimo de asistencia del 80% a clases y actividades registradas durante el curso.
Artículo 27. Para que el alumno tenga derecho al registro de la calificación en el periodo extraordinario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente. II. Haber pagado el arancel y presentar el comprobante correspondiente. III. Tener un mínimo de asistencia del 65% a clases y actividades registradas durante el curso.

## 5.- Participantes en la elaboración

| Código | Nombre |
|---|---|
| 2966256 | Luis Pedro García Yáñez |
| 2700735 | Laura López López |
| | |

## 6.- Fecha de adaptación

Agosto 2023