ASIGNATURA DE INTEGRADORA

1. Competencias	Diseñar y optimizar soluciones de redes digitales, a través de la administración y dirección de proyectos tecnológicos, alineados a normas y estándares vigentes, para contribuir a la continuidad del negocio.
2. Cuatrimestre	Décimo
3. Horas Teóricas	4
4. Horas Prácticas	26
5. Horas Totales	30
6. Horas Totales por Semana Cuatrimestre	2
7. Objetivo de aprendizaje	El alumno integrará un portafolio de evidencias que le permitan establecer un plan maestro de ciberseguridad para atender las necesidades de una organización.

Unidades de Aprendizaje	Horas		
	Teóricas	**Prácticas**	**Totales**
I. Análisis del problema y contexto de la organización	2	13	15
II. Integración y presentación del proyecto	2	13	15
Totales	**4**	**26**	**30**

INTEGRADORA

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**I. Análisis del problema y contexto de la organización**
2. Horas Teóricas	2
3. Horas Prácticas	13
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno determinará el contexto empresarial y tecnológico de la organización para la elaboración de un plan maestro de ciberseguridad.

Temas	Saber	Saber hacer	Ser
Planteamiento del problema.	Identificar los elementos clave de un caso de estudio en ciberseguridad. Definir el concepto de Plan maestro de ciberseguridad. Enlistar las etapas del proceso de diseño e implementación de un plan maestro de ciberseguridad. Identificar las expectativas organizacionales en términos de ciberseguridad.	Determinar el alcance de un riesgo de ciberseguridad. Diagramar las etapas de implementación de un plan maestro de ciberseguridad.	Analítico Autodidacta Capacidad para investigar Capacidad de Síntesis Pensamiento estructurado Proactivo Responsable

Temas	Saber	Saber hacer	Ser
Análisis del contexto de la organización.	Identificar el marco normativo y regulatorio aplicable a la organización. Identificar las características del sector al que pertenece la organización. Enlistar las áreas de la organización que intervienen de forma directa e indirecta en la estrategia de ciberseguridad. Identificar los riesgos no tecnológicos asociados al contexto de la organización. Identificar estándares internacionales para la valoración inicial de la organización en términos no tecnológicos.	Esquematizar la documentación regulatoria interna y externa de la organización. Documentar el contexto interno y externo de la organización en términos empresariales (no tecnológicos). Esquematizar la estructura orgánica de la organización.	Analítico Autodidacta Capacidad para investigar Capacidad de Síntesis Pensamiento estructurado Proactivo Responsable

Temas	Saber	Saber hacer	Ser
Análisis tecnológico de la organización.	Identificar los riesgos tecnológicos asociados al contexto de la organización. Identificar estándares internacionales para la valoración inicial de la organización en términos tecnológicos. Identificar el grado de aplicación de controles de seguridad. Identificar riesgos y eventos que hayan vulnerado la ciberseguridad de la organización. Identificar estándares internacionales para la valoración de la madurez de procesos orientados a la ciberseguridad de la organización. Identificar escalas de evaluación de madurez de capacidades (CMM).	Evaluar las capacidades de los responsables de la gestión de activos tecnológicos de la organización. Evaluar el grado de madurez de las estrategias de ciberseguridad existentes en la organización. Verificar la efectividad de las estrategias de ciberseguridad implementadas en la organización.	Analítico Autodidacta Capacidad para investigar Capacidad de Síntesis Pensamiento estructurado Proactivo Responsable

INTEGRADORA

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
Elabora y presenta un reporte de análisis del contexto de una organización que integre lo siguiente: -Introducción -Justificación -Diagrama que muestra las etapas y descripción del proceso de implementación de un plan maestro de ciberseguridad. -Descripción de los antecedentes de la organización (historia, productos y servicios que ofrece) -Objetivos organizacionales relacionados con la protección de sus servicios informáticos. -Identificación del sector al que pertenece la organización. -Identificación de los riesgos más comunes en términos de ciberseguridad del sector al que pertenece la organización (basado en datos estadísticos de fuentes externas). -Esquema del marco regulatorio aplicable a la organización (interno y externo). -Estructura orgánica de la organización. -Diagnóstico de capacidades de los responsables de la	1. Comprender el concepto y relevancia del plan maestro de ciberseguridad. 2. Identificar las etapas del proceso de implementación del plan maestro de ciberseguridad. 3. Analizar las características del contexto empresarial de una organización. 4. Analizar las características del contexto tecnológico de una organización.	1. Proyecto 2. Rúbrica

gestión de los activos informáticos de la organización. -Anexo de carta de autorización de la organización para el desarrollo del proyecto. -Anexo de acuerdo de confidencialidad en el manejo de información de la organización. -Referencias bibliográficas.		

INTEGRADORA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Aprendizaje situado -Análisis de casos -Equipos colaborativos	-Paquetería de ofimática -Software especializado -Equipo de cómputo -Internet

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X		**X**

INTEGRADORA

UNIDADES DE APRENDIZAJE

1. Unidad de aprendizaje	**II. Integración y presentación del proyecto**
2. Horas Teóricas	2
3. Horas Prácticas	13
4. Horas Totales	15
5. Objetivo de la Unidad de Aprendizaje	El alumno diseñará un plan maestro de ciberseguridad que atienda las necesidades de protección física y lógica de la organización.

Temas	Saber	Saber hacer	Ser
Establecimiento de estrategias e iniciativas	Identificar estrategias orientadas al mejoramiento de los métodos de trabajo vigentes en la organización. Identificar estrategias orientadas al mejoramiento de la infraestructura tecnológica física y lógica de la organización. Identificar proyectos viables que permitan la mitigación de riesgos tecnológicos y de ciberseguridad.	Enlistar el plan de implementación de estrategias orientadas al mejoramiento de los métodos de trabajo en la organización. Enlistar el plan de implementación de estrategias orientadas al mejoramiento de la infraestructura tecnológica física y lógica de la organización. Proponer proyectos orientados a la mitigación de riesgos tecnológicos y de ciberseguridad. Determinar las capacidades requeridas por los responsables de la gestión de activos tecnológicos de la organización. Elaborar presupuestos de recursos materiales y humanos para el desarrollo de un plan maestro de ciberseguridad.	Analítico Autodidacta Capacidad para investigar Capacidad de Síntesis Colaborativo Pensamiento estructurado Proactivo Ordenado Responsable

Temas	Saber	Saber hacer	Ser
Presentación del plan maestro de ciberseguridad	Identificar áreas de oportunidad en la elaboración del plan maestro de ciberseguridad. Identificar estrategias de persuasión para la autorización de proyectos. Identificar estrategias para la sensibilización en temas de riesgos asociados a la ciberseguridad.	Justificar el desarrollo de un plan maestro de ciberseguridad en el contexto empresarial y tecnológico. Elaborar resúmenes ejecutivos para la valoración de proyectos. Integrar informes técnicos para la validación de proyectos.	Analítico Autodidacta Capacidad para investigar Capacidad de Síntesis Colaborativo Pensamiento estructurado Proactivo Ordenado Responsable

INTEGRADORA

PROCESO DE EVALUACIÓN

Resultado de aprendizaje	Secuencia de aprendizaje	Instrumentos y tipos de reactivos
1. Elabora y presenta un plan maestro de ciberseguridad que integra lo siguiente: - Introducción - Justificación - Reporte de análisis del contexto - Resultados de la valoración inicial de la organización. - Evaluación de la efectividad y madurez de las estrategias implementadas por la organización en términos de ciberseguridad. - Resultados de las pruebas tecnológicas simuladas aplicadas a las estrategias de ciberseguridad de la organización en un ambiente controlado (pruebas de penetración y análisis de vulnerabilidades) - Tabla de integración de estrategias, iniciativas y proyectos orientados a la mejora de la ciberseguridad, con descripción detallada, justificación y presupuesto de recursos materiales y humanos. - Análisis detallado de capacidades requeridas por el personal responsable de la gestión de los activos informáticos de la organización. - Priorización de la	1. Identifica la estrategia que la organización implementa en temas de ciberseguridad. 2. Analiza la eficiencia y grado de madurez de las estrategias de ciberseguridad de la organización. 3. Analiza las capacidades del personal responsable de la gestión de los activos informáticos de la organización. 4. Explica el proceso de implementación de un plan maestro de ciberseguridad.	1. Proyecto 2. Rúbrica

implementación de estrategias, iniciativas y proyectos. - Cronograma de implementación. 2. Elabora una presentación ejecutiva que integra lo siguiente: - Marco teórico - Justificación - Resultados de pruebas realizadas - Alcances - Tabla de iniciativas, estrategias y proyectos - Cronograma de trabajo - Conclusiones.		

INTEGRADORA

PROCESO ENSEÑANZA APRENDIZAJE

Métodos y técnicas de enseñanza	Medios y materiales didácticos
-Aprendizaje situado -Análisis de casos -Equipos colaborativos	-Paquetería de ofimática -Software especializado -Equipo de cómputo -Internet

ESPACIO FORMATIVO

Aula	Laboratorio / Taller	Empresa
X		**X**

INTEGRADORA

CAPACIDADES DERIVADAS DE LAS COMPETENCIAS PROFESIONALES A LAS QUE CONTRIBUYE LA ASIGNATURA

Capacidad	Criterios de Desempeño
Implementar servicios lógicos de red a través de la aplicación de métricas, normas y estándares vigentes, para ofrecer soluciones en la comunicación y colaboración digital de las organizaciones.	Entrega una memoria técnica que integre lo siguiente: - Planeación para la implementación. - Línea base del servicio. - Bitácora de implementación. - Pruebas de la implementación. - Hojas de estándares vigentes
Evaluar soluciones y servicios lógicos de red mediante la aplicación e interpretación de métricas, para determinar áreas de oportunidad en plataformas digitales de tecnologías de la información.	Entrega un reporte técnico que incluye lo siguiente: - Análisis de información de monitoreo e incidentes. - Nivel de cumplimiento de Indicadores Clave de Desempeño.
Implementar las soluciones de seguridad de información a partir de los lineamientos organizacionales y en apego a los procedimientos y estándares aplicables a las tecnologías seleccionadas, para salvaguardar los activos de las organizaciones.	Entrega una memoria técnica que integre lo siguiente: - Línea base del servicio. - Bitácora de implementación. - Pruebas de la implementación.
Monitorear la implementación de soluciones y políticas de seguridad de información a través del análisis de los resultados de auditorías, para optimizar los procesos de continuidad del negocio.	Entrega un reporte técnico que incluye lo siguiente: - Bitácora de eventos. - Lista de verificación de las políticas de seguridad de la organización. - Reportes de rendimiento y eficiencia de la solución.
Implementar procesos y servicios tecnológicos a través de la aplicación de métricas, normas y estándares vigentes, para ofrecer soluciones de infraestructura de red en las organizaciones.	Entrega una memoria técnica que integre lo siguiente: - Planeación para la implementación. - Línea base del servicio. - Bitácora de implementación. - Pruebas de la implementación. - Hojas de estándares vigentes
Evaluar procesos y servicios tecnológicos mediante la aplicación e interpretación de métricas, en apego a normas y estándares vigentes, para determinar áreas de oportunidad en la infraestructura de red de las organizaciones.	Entrega un reporte técnico que incluye lo siguiente: - Análisis de información de monitoreo e incidentes. - Nivel de cumplimiento de Indicadores Clave de Desempeño.

INTEGRADORA

FUENTES BIBLIOGRÁFICAS

Autor	Año	Título del Documento	Ciudad	País	Editorial
Francisco Lázaro Domínguez	2014	*Introducción a la Informática Forense*	España	España	Ra-Ma S.A. ISBN : ISBN:978-84-9964-209-3
Antonio Postigo Palacios	2020	*Seguridad Informática*	Madrid	España	Parainfo ISBN: 9788428344555
Baca Urbina Gabriel	2016	*Introducción a la Seguridad Informática*	México	México	Grupo Editorial Patria ISBN: 978-607-744-344-5
Sánchez Cano Gabriel	2018	*Seguridad cibernética. Hackeo ético y programación defensiva*	México	México	Alfaomega ISBN: 978-607-538-294-4
Santos Omar	2021	*Cisco CyberOps Associate*	Hoboken	Estados Unidos	Cisco Press ISBN-13:978-0-13-680783-4
David Arroyo Guardeño; Víctor Gayoso Martínez; Luis Hernández Encinas	2020	*Ciberseguridad*	Madrid	España	Consejo Superior de Investigaciones Científicas ISBN: 978-84-00-10713-0