

Abstract geometric shapes composed of interconnected lines forming various polygons, located in the top-left corner of the slide.

Bienvenidos a

Ciberseguridad

Abstract geometric shape composed of interconnected lines forming various polygons, located in the bottom-left corner of the slide.




Presentación y Modalidad





Presentación

- Nombre y apellido
 - ¿Trabajan? ¿Donde?
 - ¿Conocimientos de Ciberseguridad?
 - ¿Por qué eligieron la materia?
 - ¿Qué esperan de la materia?
 - ¿Hobbies?
- 

Modalidad

- 1 parcial integrador con 2 recuperatorios.
 - Parcial incluye multiple choice y ejercicios prácticos.
 - Condiciones de aprobación del parcial:
 - 60% de la parte teórica.
 - 60% de la parte práctica.
- 2 Laboratorios con consignas a entregar.
- Cada tema visto en la materia tiene un cuestionario con fecha límite semanal que se considera como el presentismo.
 - Pueden tener como máximo 2 cuestionarios sin hacer en todo el cuatrimestre. Si adeudan más, tienen que pedir la reincorporación.
- Condiciones de regularización de la materia:
 - 80% de asistencia a clase y cuestionarios realizados.
 - Consignas de laboratorio aprobadas.
 - Examen parcial aprobado o recuperatorio aprobado.

Modalidad (cont.)

- El horario de clases es de 09:15 Hs a 12:30 Hs
- ¿Clases presenciales? ¿Virtuales?
- Al comienzo de cada clase se realiza lectura y análisis de noticias relacionadas a ciberseguridad.
 - Traer noticia leída, fecha y fuente.
- Desarrollo de los temas provistos por la cátedra.
- Medios utilizados:
 - Aula Virtual.
 - Email: si_utn@googlegroups.com.
 - Discord.

Aprobación Directa

- Para ingresar en el régimen de aprobación directa se debe contar con:
 - 80% asistencia a las clases y cuestionarios realizados.
 - Laboratorios aprobados.
 - Examen parcial aprobado con 8 o más o primer recuperatorio con 8 o más.
 - En caso de recuperar el examen parcial (sea para levantar la nota o sea por no estar aprobado) la nota final que queda es la del recuperatorio (se pisa la anterior).
 - En segundo recuperatorio no hay posibilidad de aprobación directa.

Cronograma

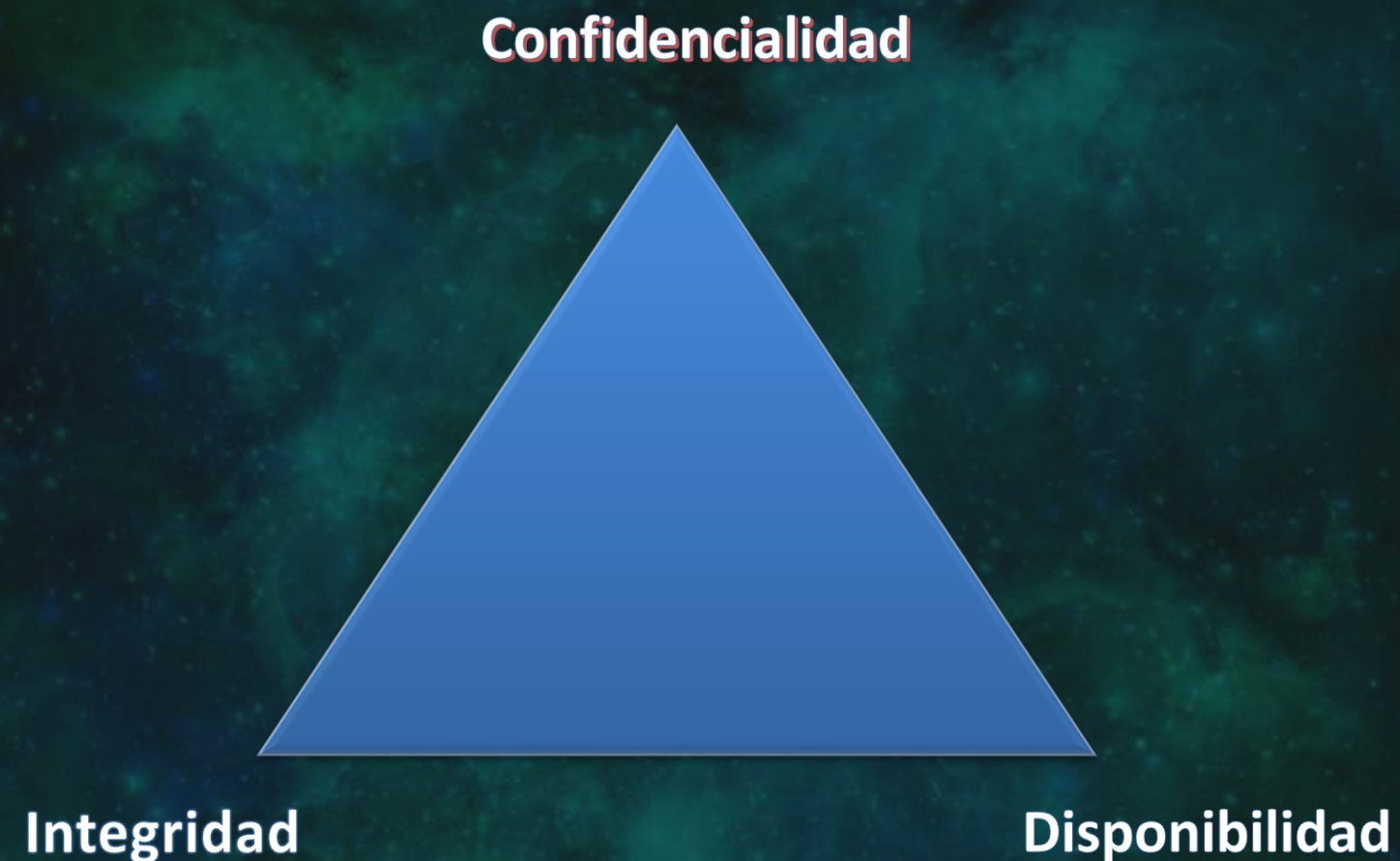
Clase N°	Fecha	Tema
1	23/03/24	Introducción a la Ciberseguridad
2	30/03/24	Control de Acceso y Gestión de la Seguridad de la Información
3	06/04/24	Criptografía
4	13/04/24	Malware y Threat Intelligence
5	20/04/24	Laboratorio I
6	27/04/24	Proceso de Ethical Hacking
7	04/05/24	Análisis Forense, Auditoría y Legislación Informática
8	11/05/24	Laboratorio II
9	18/05/24	OSINT - ING. SOCIAL
10	25/05/24	FERIADO
11	01/06/24	A DEFINIR
12	08/06/24	Nube y Tendencias. Protección de datos
13	15/06/24	Seguridad en Operaciones - Herramientas de seguridad
14	22/06/24	Administración de riesgos
15	29/06/24	A DEFINIR
16	06/07/24	PARCIAL
17	13/07/24	RECUPERATORIO Y FIN DE CUATRIMESTRE

Introducción a la Ciberseguridad



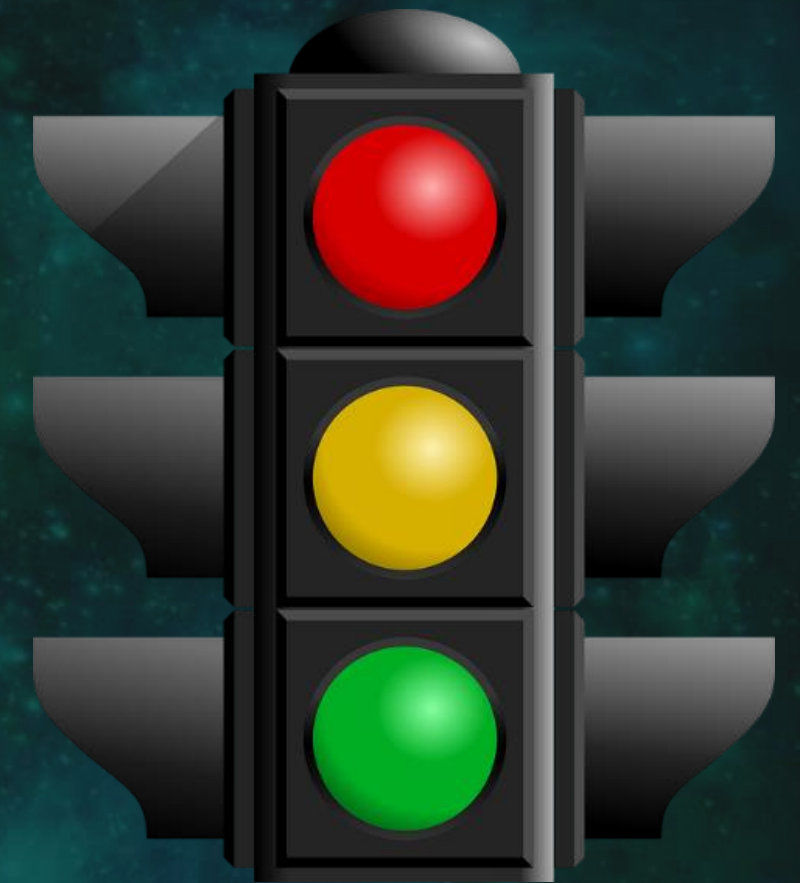
Introducción a la Ciberseguridad

La seguridad de la información es el conjunto de medidas preventivas, de detección y de corrección destinadas a proteger la integridad, confidencialidad y disponibilidad de la información.



Confidencialidad

- La información debe ser accedida únicamente por los sujetos autorizados.
- Identificación, Autenticación y Autorización.




Amenazas contra la Confidencialidad

- Ingeniería Social.
- OSINT.
- Usuarios descuidados.
 - “Una cadena es tan fuerte como el más débil de sus eslabones.”
 - “El hilo se corta por la parte más delgada.”
- Atacantes.
- Robo y divulgación de información.
- Descargas peligrosas involuntarias (Drive-by download).
- Trashing.





Medidas de protección contra la pérdida de Confidencialidad

- Clasificación de la información.
 - Mecanismos de control de acceso informático.
 - Cifrado de datos.
 - Capacitación del personal:
 - Identificación de Phishing.
 - Divulgación de información.
 - Procedimientos de acceso a la información.
- 


Integridad

- La información debe ser modificada únicamente por los sujetos autorizados.
- La información enviada por el emisor deber ser idéntica a la información recibida por el receptor.






Amenazas contra la Integridad

- Ingeniería Social.
 - Actividad de usuarios no autorizados.
 - Malware:
 - Virus: Alteran el comportamiento de los programas.
 - RATs: Controlan máquinas.
 - Falsas Alertas.
 - Sitios Peligrosos.
- 



Medidas de protección contra las amenazas a la Integridad

- Menor Privilegio.
 - Segregación de Funciones.
 - Procedimientos de control de cambios.
 - Verificación de Integridad.
 - Antivirus.
 - Firewall.
- 


Disponibilidad

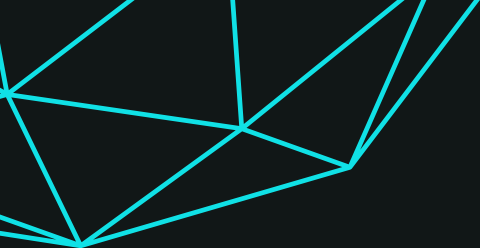
- Es la característica que intenta asegurar que la información se encuentre accesible en tiempo y forma según se requiera.






Amenazas contra la disponibilidad

- Denegación de Servicios.
 - Desastres Naturales.
 - Acciones humanas – Intencionales o accidentales.
 - Malware:
 - Worms (Gusanos): Se replican por la red.
 - Crypto-Ransomware: Cifra archivos.
- 



Medidas de protección contra amenazas a la disponibilidad

- Seguridad Física.
 - Mecanismos de tolerancia a fallos.
 - Plan de contingencia.
 - Aplicar mecanismos de defensa (firewall, segmentación de red).
 - Procedimientos operativos estándar (SOP).
- 

Rol del Responsable de Seguridad

- CISO: Chief Information Security Officer.
- Cumplir con el programa integral de Seguridad para garantizar la confidencialidad, integridad y disponibilidad.
- Gestionar los recursos necesarios para cumplir el programa integral de seguridad.
- Determinar prioridades.
- Comunicarse con la alta dirección.

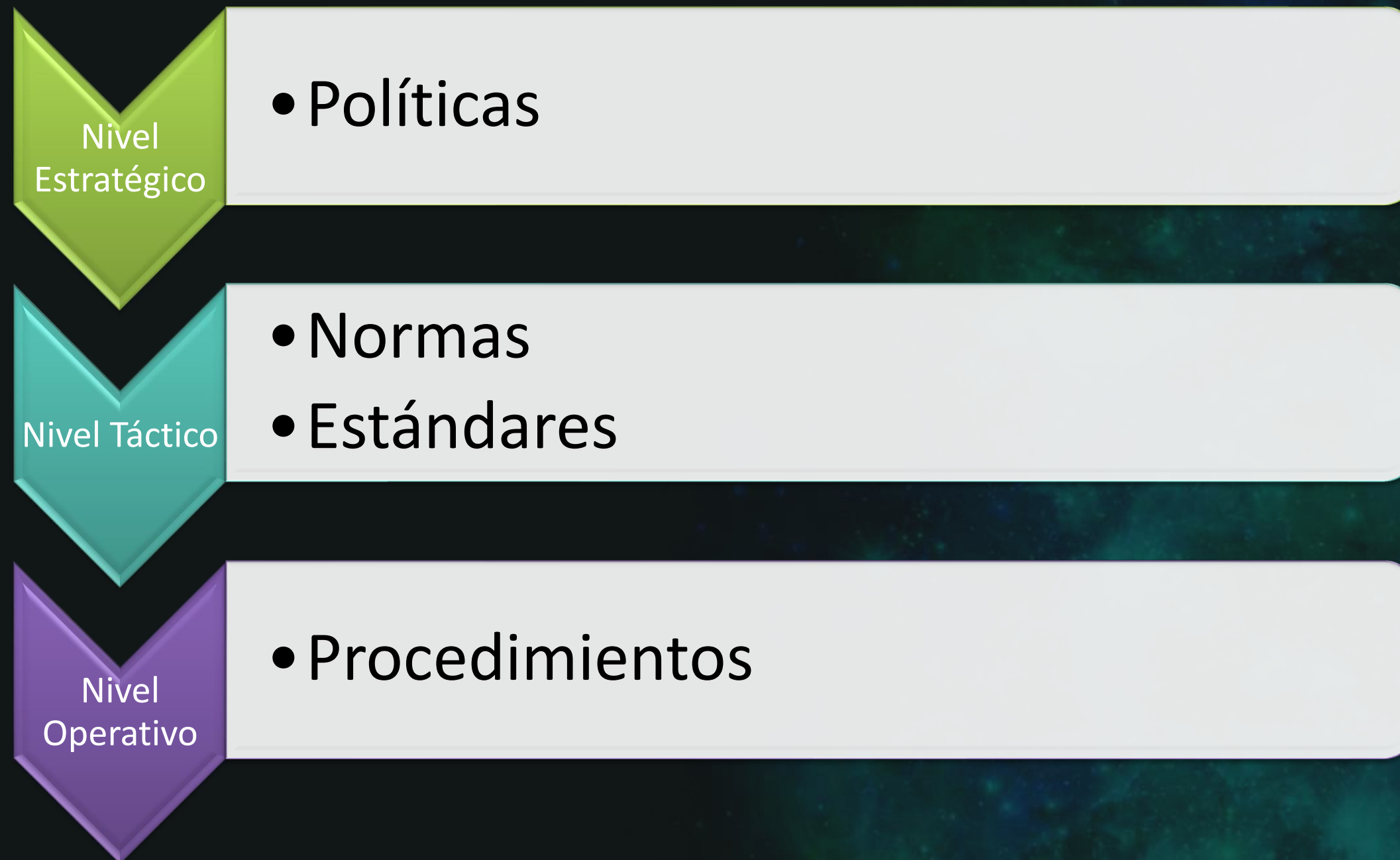


Organización

- La seguridad de la información debe ser incumbencia de la alta gerencia de la organización. NO debe circunscribirse al área de Sistemas.



Políticas, normas y procedimientos



Las políticas deben ser:

- Realizadas y aprobadas por el comité de seguridad de la información.
 - Alineadas con la estrategia de negocio.
- Comunicadas a todos los integrantes de la organización.
- Escritas en un lenguaje claro, independiente de la tecnología y sin ambigüedades.
- Definidos los roles y responsabilidades para la implementación.
- Contenido:
 - Objetivos.
 - Alcance.
 - Importancia de la seguridad de la Información.
 - Propósito de los responsables a nivel gerencial demostrando el apoyo.
 - Explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad.
 - Definición de responsabilidades para la gestión de la Seguridad de la Información.

Normas y Estándares

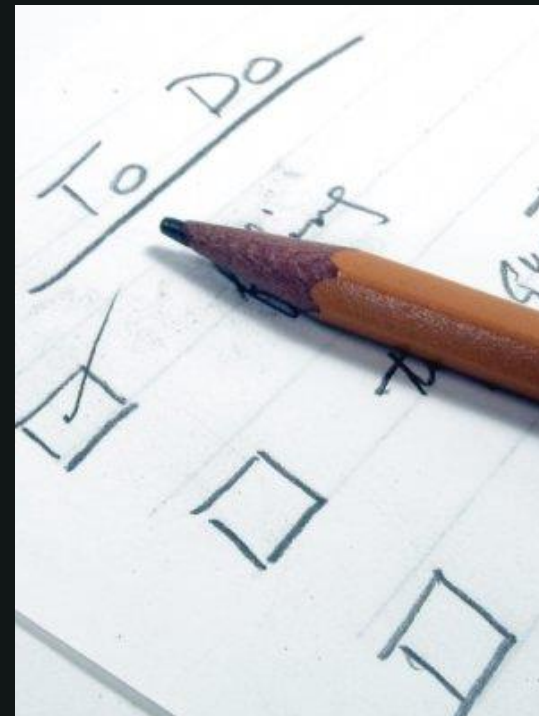
- Es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.



Procedimientos

Nivel Operativo

- Es un conjunto de pasos para cumplir las políticas y normas definidas por la organización.




Controles

- El principal objetivo del establecimiento de controles de seguridad de la información es reducir los efectos producidos por las amenazas y vulnerabilidades a nivel tolerable por la empresa.
- Controles Físicos
 - Guardias de Seguridad.
 - Cerraduras.
 - Protección del edificio.
 - Cámaras de seguridad.
 - Controles ambientales.
- Controles Técnicos
 - Control de acceso lógico.
 - Encriptación o Cifrado.
 - Identificación.
 - Autenticación.
 - Monitoreo lógico.
- Controles Administrativos
 - Políticas.
 - Estándares.
 - Procedimientos.
 - Concientización.
 - Control de Cambios.
 - Autorización.






Clasificación y controles de activos

- Clasificación:
 - Activos de información: Archivos, bases de datos, manuales, etc.
 - Activos de software: Aplicaciones, programas de desarrollo.
 - Activos físicos: Máquinas, servidores.
 - Servicios: Comunicaciones.
 - Personas.
 - Activos intangibles: Reputación, imagen de la organización.
 - Busca mantener una adecuada protección de los activos.
 - Se designa un propietario para cada uno de los activos.
 - Se debe realizar un inventario de activos.
- 



Áreas en la Seguridad de la Información

- Análisis Forense y Auditoría.
 - Análisis de Malware y Threat Intel.
 - Criptografía.
 - Seguridad en el Desarrollo de Aplicaciones.
 - Desarrollo del Programa de Seguridad.
 - Gestión de Riesgo.
 - Gestión del Programa de Seguridad de la Información.
 - Gobierno de Seguridad de la Información.
 - Marco Legal.
 - Modelos y Arquitecturas de Seguridad.
 - Continuidad del negocio y Plan de recupero de desastre.
 - Seguridad en las Operaciones.
 - Seguridad en Redes, Internet y Telecomunicaciones.
 - Seguridad Física.
 - Sistemas y Metodologías de Control de Acceso.
- 



¡Gracias!