HOJA CALENDARIO– PLANIFICACIÓN DE LAS SESIONES DE CLASE

MODALIDAD PRESENCIAL

Nombre de la asignatura	**Gerencia de la seguridad de información**	**Resultado de aprendizaje de la asignatura:**	Al finalizar la asignatura, el estudiante será capaz de aplicar adecuadamente los elementos que permitan gestionar la seguridad de la información en las organizaciones modernas y complejas de hoy a través de la planificación de riesgos de seguridad de la información, siguiendo las mejores prácticas de la industria.
Periodo	8	**EAP**	Ingeniería de Sistemas e Informática

COMPETENCIAS	CRITERIOS	ESPECIFICACIÓN DEL NIVEL DEL LOGRO	NIVEL
El Ingeniero y la Sociedad	**C1. Temas sociales, económicos, políticos, ambientales**	Analiza acontecimientos sociales, económicos, ambientales y políticos, incorporándolos como lecciones aprendidas para su futura práctica profesional.	3
	C2. Temas tecnológicos y científicos	Analiza acontecimientos tecnológicos y científicos incorporándolos como lecciones aprendidas para su futura práctica profesional.	3
Gestión de Proyectos	**C1. Diseño del proyecto**	Prepara la propuesta de proyecto para atender las necesidades identificadas utilizando herramientas de gestión de proyectos, considerando criterios técnicos, económicos y operativos.	3
	C2. Planificación de la gestión	Desarrolla un Plan de Gestión del proyecto considerando los criterios establecidos.	3
	C3. Ejecución del proyecto	Controla el avance de la implementación y genera acciones preventivas o correctivas.	3
Uso de herramientas modernas	**C1. Uso de técnicas y metodologías**	Usa técnica o metodología apropiada para la solución de un problema.	3
	C2. Uso de herramientas	Usa herramientas apropiadas para la solución de un problema.	3

Unidad 1		**Nombre de la unidad**	**Seguridad de la información e introducción a las Normas ISO 27001 y 27002**	**Resultado de aprendizaje de la unidad**	Al finalizar la Unidad, el estudiante será capaz de identificar los conceptos básicos de seguridad de la información y las normas ISO 27001 e ISO 27002	**Duración en horas**	16

Semana	Horas / Tipo de sesión	Temas y subtemas	Propósito	Actividades para la enseñanza - aprendizaje (Docente - Estudiante)	Recursos	Metodología / Estrategias	Actividades asíncronas de aprendizaje autónomo (Estudiante – Aula virtual)
1	**2T**	- Prueba de entrada - Seguridad de la información	- Al finalizar la sesión el estudiante reconoce la importancia de la seguridad de la información en las organizaciones modernas siguiendo las mejores prácticas de la industria.	**EVALUACIÓN DIAGNÓSTICA: Evaluación individual teórica/ Prueba objetiva** - **I:** Motivación y propósito de sesión. Dinámicas de presentación entre el docente y estudiante de manera asertiva. - **D**: El docente presenta el sílabo y realiza una breve introducción de la asignatura. - Se presenta el tema de Seguridad de la información y se visualiza un video. - **C**: Metacognición, síntesis y retroalimentación. - Se realiza la evaluación diagnóstica a los estudiantes.	- Gregory, H. (2018). CISM Certified Information Security Manager All-in-One Exam Guide. McGraw Hill.	Clase expositiva / lección magistral (CE-LM)	- Revisión del sílabo - Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Seguridad de la información		- **I:** Motivación y propósito de sesión. Se retoma el tema de reflexión e importancia de la seguridad de la información - **D:** Se forman equipos colaborativos para explicar y debatir respecto a la seguridad de información. - **C**: Metacognición, síntesis y retroalimentación. Se formula la reflexión de que aprendieron y cómo aprendieron.	- Gregory, H. (2018). CISM Certified Information Security Manager All-in-One Exam Guide. McGraw Hill.	Aprendizaje experiencial	

Las actividades de aprendizaje autónomo en el aula virtual son las realizadas por el estudiante. Cada semana, el docente tiene el rol de monitorear, supervisar, evaluar y retroalimentar estas actividades, además de atender los foros y las comunicaciones generadas en el aula virtual.

Universidad Continental

HOJA CALENDARIO– PLANIFICACIÓN DE LAS SESIONES DE CLASE

MODALIDAD PRESENCIAL

2	**2T**	- Confidencialidad, integridad y disponibilidad	- Al finalizar la sesión el estudiante diferencia conceptos de confidencialidad, integridad y disponibilidad para la seguridad informática de una organización.	- **I:** Motivación y propósito de sesión. - Dinámicas de presentación entre el docente y estudiante de manera asertiva. - **D**: El docente presenta el tema de la gestión de confidencialidad, integridad y disponibilidad. Explica de manera activa con la participación de los estudiantes. - **C:** Metacognición, síntesis y retroalimentación	- Gregory, H. (2018). CISM Certified Information Security Manager All-in-One Exam Guide. McGraw Hill.	Clase expositiva / lección magistral (CE-LM)	- Revisión de material audiovisual de la semana.
	2P	- Controles asociados a la confidencialidad, integridad y disponibilidad		- **I:** Motivación y propósito de sesión. - **D**: El estudiante desarrolla en equipos colaborativos los ejercicios propuestos para determinar controles relacionados a la confidencialidad, integridad y disponibilidad. - **C**: Metacognición, síntesis y retroalimentación	- Gregory, H. (2018). CISM Certified Information Security Manager All-in-One Exam Guide. McGraw Hill.	Aprendizaje colaborativo	
3	**2T**	- ISO 27001 y certificación	- Al finalizar la sesión el estudiante comprende la importancia de las normas ISO 27001 y certificación para la seguridad informática de una organización.	- **I:** Motivación y propósito de sesión. - **D**: El docente presenta el tema de ISO 21001 y certificación. - Se brinda información bibliográfica, donde los estudiantes comprenden la importancia de las normas ISO 21001 y certificación. - **C:** Metacognición, síntesis y retroalimentación	- Gregory, H. (2018). CISM Certified Information Security Manager All-in-One Exam Guide. McGraw Hill.	Aprendizaje colaborativo	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Iniciando un programa de certificación		- **I:** Motivación y propósito de sesión. - **D**: El estudiante desarrolla ejercicios de casos prácticos para determinar los criterios más importantes para conocer el proceso de certificación. - **C**: Metacognición, síntesis y retroalimentación	- Gregory, H. (2018). CISM Certified Information Security Manager All-in-One Exam Guide. McGraw Hill.	Método de casos (MC)	
4	**2T**	- Controles ISO 27002	- Al finalizar la sesión, el estudiante identifica los conceptos básicos de seguridad de la información, normas y controles ISO 27001, ISO 27002 y evaluación UD1 para la seguridad informática de una organización.	- **I:** Motivación y propósito de sesión. - **D**: El docente presenta y explica de manera activa respecto al tema de controles ISO 27002. - **C**: Metacognición, síntesis y retroalimentación	- Gregory, H. (2018). CISM Certified Information Security Manager All-in-One Exam Guide. McGraw Hill.	Clase expositiva / lección magistral (CE-LM)	- Revisión de material de investigación de la semana.
	2P	- Seguridad de la información - Certificación - Normas ISO 27001 y 27002 - Controles asociados a la confidencialidad, integridad y disponibilidad		**Evaluación del C1-SC1: Evaluación teórico-práctica/ Prueba de desarrollo** - I: Motivación y propósito de sesión. - D: se brinda las indicaciones para la evaluación de la unidad 1. - C: Metacognición, síntesis y retroalimentación.	- Prueba de Desarrollo	Método de casos (MC)	

Las actividades de aprendizaje autónomo en el aula virtual son las realizadas por el estudiante. Cada semana, el docente tiene el rol de monitorear, supervisar, evaluar y retroalimentar estas actividades, además de atender los foros y las comunicaciones generadas en el aula virtual.

Universidad Continental

HOJA CALENDARIO– PLANIFICACIÓN DE LAS SESIONES DE CLASE

MODALIDAD PRESENCIAL

Unidad	Nombre de la unidad	Metodologías de riesgo: OCTAVE, MAGERIT, NIST800-30 y Risk IT Framework, gestión de riesgos ISO 27005	Resultado de aprendizaje de la unidad	Al finalizar la Unidad, el estudiante será capaz de identificar los conceptos básicos relacionados con la gestión de riesgos, implementando también un plan de tratamiento de estos en la organización.	Duración en horas	16

Semana	Horas / Tipo de sesión	Temas y subtemas	Propósito	Actividades para la enseñanza - aprendizaje (Docente - Estudiante)	Recursos	Metodología / Estrategias	Actividades asíncronas de aprendizaje autónomo (Estudiante – Aula virtual)
5	2T	- Gestión de riesgos en la seguridad de la información	- Al finalizar la sesión, el estudiante reconoce la importancia de la gestión de riesgos en la seguridad de la información, a través de casos prácticos y con la finalidad de implementar un plan de tratamiento de estos en la organización.	- **I:** Motivación y propósito de sesión. - Dinámicas de presentación entre el docente y estudiante de manera asertiva. - **D**: El docente presenta el tema y con participación de los estudiantes explica la importancia de gestión de gestión de riesgos en la seguridad de la información. - **C**: Metacognición, síntesis y retroalimentación.	- International Organization for Standardization (ISO). (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. Recuperado de https://www.iso.org/obp/ui/#iso:std:isoiec:27002:ed-2:e	Clase expositiva / lección magistral (CE-LM)	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Identificación de riesgos		- **I:** Motivación y propósito de sesión. - **D**: El estudiante identifica y desarrolla ejercicios prácticos para los riesgos asociados a la seguridad de la información en las organizaciones. - **C**: Metacognición, síntesis y retroalimentación	- International Organization for Standardization (ISO). (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. Recuperado de https://www.iso.org/obp/ui/#iso:std:isoiec:27002:ed-2:e	Aprendizaje experiencial	
6	2T	- ISO 31000 - ISO 27005	- Al finalizar la sesión, el estudiante sustenta la importancia del ISO 3100 – ISO 27005 con casos prácticos y con la finalidad que permita ayudar a generar un enfoque para mejorar la gestión de riesgos de una organización.	- **I:** Motivación y propósito de sesión. - **D**: El docente presenta de manera activa con los estudiantes en equipos el tema de la gestión de ISO 31000 – ISO 27005. - Los estudiantes sustentan la importancia de ISO 31000 – ISO 27005. - **C**: Metacognición, síntesis y retroalimentación	- International Organization for Standardization (ISO). (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. Recuperado de https://www.iso.org/obp/ui/#iso:std:isoiec:27002:ed-2:e	Aprendizaje colaborativo	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Análisis de Riesgos		- **I:** Motivación y propósito de sesión. - **D**: El estudiante desarrolla los casos prácticos (ejercicios) para determinar la probabilidad e impacto de riesgos asociados a la seguridad de la información - **C**: Metacognición, síntesis y retroalimentación	- International Organization for Standardization (ISO). (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. Recuperado de https://www.iso.org/obp/ui/#iso:std:isoiec:27002:ed-2:e	Método de casos (MC)	
7	2T	- MAGERIT - OCTVAVE	- Al finalizar la sesión, el estudiante compara entre las metodologías MAGARIT y OCTVAVE a través de casos prácticos para mejorar la gestión de riesgos de una organización.	- **I**: Motivación y propósito de sesión. - **D**: El docente expone de manera activa el tema de la gestión de MAGERIT – OCTVAVE. - Los estudiantes mencionan las comparaciones que encuentran entre las metodologías MAGERIT – OCTVAVE. - **C**: Metacognición, síntesis y retroalimentación.	- International Organization for Standardization (ISO). (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. Recuperado de https://www.iso.org/obp/ui/#iso:std:isoiec:27002:ed-2:e	Aprendizaje colaborativo	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Evaluación y tratamiento de riesgos		**Evaluación del C1-SC2: Ejercicios desarrollados en clase/ Rúbrica de evaluación** **I**: Motivación y propósito de sesión. **D:** El estudiante desarrolla ejercicios en la clase para determinar la mejor forma de tratar riesgos. **C:** Metacognición, síntesis y retroalimentación	- Rúbrica de evaluación	Método de casos (MC)	

Las actividades de aprendizaje autónomo en el aula virtual son las realizadas por el estudiante. Cada semana, el docente tiene el rol de monitorear, supervisar, evaluar y retroalimentar estas actividades, además de atender los foros y las comunicaciones generadas en el aula virtual.

Universidad Continental

HOJA CALENDARIO– PLANIFICACIÓN DE LAS SESIONES DE CLASE

MODALIDAD PRESENCIAL

8	**2T**	- Otros marcos de gestión de riesgos	- Al finalizar la sesión, el estudiante identifica los conceptos básicos relacionados con la gestión de riesgos que permita implementar un plan de tratamiento en la organización.	- **I:** Motivación y propósito de sesión. - Dinámicas de lluvia de ideas respecto al tema. - **D**: El docente presenta y explica el tema de otros marcos de gestión de riesgos. - **C**: Metacognición, síntesis y retroalimentación	- International Organization for Standardization (ISO). (2013). ISO/IEC 27002:2013 Information technology – Code of Practice for Information Security Management. Recuperado de https://www.iso.org/obp/ui/#iso:std:isoiec:27002:ed-2:e	Clase expositiva / lección magistral (CE-LM)	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Metodologías de riesgo: OCTAVE, MAGERIT, NIST800-30 y Risk IT Framework, gestión de riesgos ISO 27005		**EVALUACIÓN PARCIAL: Evaluación teórico-práctica/ Prueba de desarrollo** - I: Motivación y propósito de sesión. - D: El docente brinda las indicaciones para la evaluación parcial. - C: Metacognición, síntesis y retroalimentación	- Prueba de desarrollo	Aprendizaje experiencial	

Unidad 3	**Nombre de la unidad**	**Planeación de continuidad de negocio BCP/DRP (Business Continuity Planning / Disaster Recovery Planning) y atención de incidentes de seguridad, NIST800-61**	**Resultado de aprendizaje de la unidad**	Al finalizar la Unidad, el estudiante será capaz de identificar los conceptos e importancia de la continuidad del negocio y la recuperación ante desastres en las organizaciones, gestionando también incidentes de seguridad	**Duración en horas**	16

Semana	**Horas / Tipo de sesión**	**Temas y subtemas**	**Propósito**	**Actividades para la enseñanza - aprendizaje** (Docente - Estudiante)	**Recursos**	**Metodología / Estrategias**	**Actividades asíncronas de aprendizaje autónomo** (Estudiante – Aula virtual)
8	**2T**	- ¿Qué es la continuidad del negocio?	- Al finalizar la sesión, el estudiante reconoce qué es la continuidad del negocio y su importancia en una empresa para mantener las funciones esenciales tras una emergencia o una interrupción.	- **I:** Motivación y propósito de sesión. - Dinámicas de presentación entre el docente y estudiante de manera asertiva. - **D**: El docente presenta el tema y plantea la siguiente pregunta. ¿Qué es la continuidad del negocio? - Los estudiantes responden la pregunta planteada en equipos colaborativos y reconocen la importancia de la continuidad de negocio. - **C**: Metacognición, síntesis y retroalimentación.	- ISACA (2014). Certified Information Security Manager - CISM. Review Manual. (13.a ed.). ISACA.	Aprendizaje colaborativo	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Importancia de la continuidad de negocio		- **I:** Motivación y propósito de sesión. - **D:** El estudiante desarrolla ejercicios para sustentar la importancia de la continuidad de negocio. - **C**: Metacognición, síntesis y retroalimentación	- ISACA (2014). Certified Information Security Manager - CISM. Review Manual. (13.a ed.). ISACA.	Aprendizaje experiencial	
10	**2T**	- Análisis de impacto del negocio	- Al finalizar la sesión, el estudiante comprende el análisis de impacto del negocio y la implementación de BIA como componente esencial del plan de continuidad comercial de una organización.	- **I:** Motivación y propósito de sesión. - Dinámicas de presentación entre el docente y estudiante de manera asertiva. - **D**: El docente presenta el tema de análisis de impacto del negocio. - **C**: Metacognición, síntesis y retroalimentación	- ISACA (2014). Certified Information Security Manager - CISM. Review Manual. (13.a ed.). ISACA.	Clase expositiva / lección magistral (CE-LM)	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Implementado un BIA		- **I:** Motivación y propósito de sesión. - **D**: El estudiante desarrolla ejercicios prácticos para desarrollar un análisis de impacto de negocio (BIA) como componente esencial del plan de continuidad comercial de una organización. - **C**: Metacognición, síntesis y retroalimentación.	- ISACA (2014). Certified Information Security Manager - CISM. Review Manual. (13.a ed.). ISACA.	Aprendizaje basado en problemas (ABP)	
11	**2T**	- Recuperación ante desastres	- Al finalizar la sesión, el estudiante organiza la importancia de la recuperación ante desastres	- **I**: Motivación y propósito de sesión. - **D**: El docente presenta el tema de recuperación ante desastres. - **C**: Metacognición, síntesis y retroalimentación.	- ISACA (2014). Certified Information Security Manager - CISM. Review Manual. (13.a ed.). ISACA.	Método de casos (MC)	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.

Las actividades de aprendizaje autónomo en el aula virtual son las realizadas por el estudiante. Cada semana, el docente tiene el rol de monitorear, supervisar, evaluar y retroalimentar estas actividades, además de atender los foros y las comunicaciones generadas en el aula virtual.

Universidad Continental

HOJA CALENDARIO– PLANIFICACIÓN DE LAS SESIONES DE CLASE

MODALIDAD PRESENCIAL

	2P	- Importancia de recuperación ante desastres	con la finalidad que un negocio pueda comenzar de nuevo sus operaciones.	- **I**: Motivación y propósito de sesión. - **D**: El estudiante desarrolla ejercicios prácticos respecto a la importancia de recuperación ante desastres en la organización. **C**: Metacognición, síntesis y retroalimentación	- ISACA (2014). Certified Information Security Manager - CISM. Review Manual. (13.a ed.). ISACA.	Aprendizaje experiencial	
12	**2T**	- Proceso de gestión de incidentes y buenas prácticas	- Al finalizar la sesión, el estudiante identifica los conceptos e importancia de la continuidad del negocio, gestión de incidencias y la planeación en las organizaciones, gestionando también incidentes de seguridad.	- **I**: Motivación y propósito de sesión. - **D**: El docente presenta el tema de proceso de gestión de incidentes y buenas prácticas. - Los estudiantes identifican los conceptos e importancia de la gestión de incidentes y buenas prácticas. - **C:** Metacognición, síntesis y retroalimentación.	- ISACA (2014). Certified Information Security Manager - CISM. Review Manual. (13.a ed.). ISACA.	Aprendizaje colaborativo	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Planeación de continuidad de negocio BCP/DRP) y - Atención de incidentes de seguridad, NIST800-61		**Evaluación del C2-SC1: Evaluación teórico-práctica/ Prueba de desarrollo.** - **I:** Motivación y propósito de sesión. - **D**: Se brinda las indicaciones para la evaluación C2. - **C**: Metacognición, síntesis y retroalimentación.	- Prueba de desarrollo	Aprendizaje experiencial	

Unidad 4	**Nombre de la unidad**	**Principios organizacionales básicos: separación de responsabilidades, mínimo privilegio, accountability y prácticas seguras de gestión de capital humano**	**Resultado de aprendizaje de la unidad**	Al finalizar la Unidad, el estudiante será capaz de aplicar adecuadamente los elementos que permitan gestionar la seguridad de la información, identificando buenas prácticas en los programas de seguridad de información, así como la importancia del capital humano en las organizaciones.	**Duración en horas**	16

Semana	**Horas / Tipo de sesión**	**Temas y subtemas**	**Propósito**	**Actividades para la enseñanza - aprendizaje** (Docente - Estudiante)	**Recursos**	**Metodología / Estrategias**	**Actividades asíncronas de aprendizaje autónomo** (Estudiante – Aula virtual)
13	**2T**	- Buenas prácticas en los programas de seguridad de la información	- Al finalizar la sesión, el estudiante interpreta la importancia de las buenas prácticas en los programas de seguridad de la información.	- **I:** Motivación y propósito de sesión. - **D:** El docente presenta diversos casos de prácticas de buenas prácticas en los programas de seguridad de la información. - Los estudiantes interpretan los casos presentados. - **C**: Metacognición, síntesis y retroalimentación.	- Gómez, A. (2011). Enciclopedia de la seguridad informática. AlfaoMega – Rama.	Aprendizaje colaborativo	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Criterios de éxito para implementar ISO 27001		- **I:** Motivación y propósito de sesión. - **D**: El estudiante desarrolla ejercicio para determinar criterios de éxito al momento de implementar la ISO 27001 - **C**: Metacognición, síntesis y retroalimentación	- Gómez, A. (2011). Enciclopedia de la seguridad informática. AlfaoMega – Rama.	Aprendizaje experiencial	
14	**2T**	- Mínimo privilegio, separación de responsabilidades, accountability	- Al finalizar la sesión, el estudiante organiza información relevante respecto al mínimo privilegio, separación de responsabilidades y accountability en los programas de seguridad de información, así como la importancia del capital humano en las organizaciones.	- **I:** Motivación y propósito de sesión. - **D:** Los estudiantes en equipos colaborativos elaboran esquemas gráficos acerca de los temas de mínimo privilegio, separación de responsabilidades y accountability. - Los equipos presentan sus organizadores para compartir con sus compañeros. - **C**: Metacognición, síntesis y retroalimentación.	- Gómez, A. (2011). Enciclopedia de la seguridad informática. AlfaoMega – Rama.	Aprendizaje colaborativo	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Determinando controles de acceso necesarios		- **I:** Motivación y propósito de sesión. - **D**: El estudiante desarrolla ejercicio para determinar los controles de acceso necesarios. - **C**: Metacognición, síntesis y retroalimentación.	- Gómez, A. (2011). Enciclopedia de la seguridad informática. AlfaoMega – Rama.	Aprendizaje experiencial	

Las actividades de aprendizaje autónomo en el aula virtual son las realizadas por el estudiante. Cada semana, el docente tiene el rol de monitorear, supervisar, evaluar y retroalimentar estas actividades, además de atender los foros y las comunicaciones generadas en el aula virtual.

Universidad Continental

HOJA CALENDARIO– PLANIFICACIÓN DE LAS SESIONES DE CLASE

MODALIDAD PRESENCIAL

15	**2T**	- Concientización	- Al finalizar la sesión, el estudiante conoce los conceptos de concientización en los programas de seguridad de información, así como la importancia del capital humano en las organizaciones.	- **I:** Motivación y propósito de sesión. - **D**: El docente presenta y brinda la lección magistral el tema de concientización. - **C:** Metacognición, síntesis y retroalimentación.	- Gómez, A. (2011). Enciclopedia de la seguridad informática. AlfaoMega – Rama.	Clase expositiva / lección magistral (CE-LM)	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Desarrollando un programa de concientización		**Evaluación del C2-SC2: Ejercicios desarrollados en clase/ Rúbrica de evaluación** - I: Motivación y propósito de sesión. - **D**: El estudiante desarrolla ejercicios para desarrollar un programa de concientización y capacitación. **C**: Metacognición, síntesis y retroalimentación.	- Rúbrica de evaluación	Aprendizaje experiencial	
16	**2T**	- Entrenamiento	- Al finalizar la sesión, el estudiante. aplica adecuadamente los elementos que permitan gestionar la seguridad de la información, identificando buenas prácticas en los programas de seguridad de información, así como la importancia del capital humano en las organizaciones.	- **I:** Motivación y propósito de sesión. - **D**: El docente presenta y brinda la lección magistral del tema de entrenamiento en la organización para producir habilidades en el tema de seguridad de la información. - **C**: Metacognición, síntesis y retroalimentación	- Gómez, A. (2011). Enciclopedia de la seguridad informática. AlfaoMega – Rama.	Clase expositiva / lección magistral (CE-LM)	- Revisión de material audiovisual de la semana. - Revisión de material de investigación de la semana.
	2P	- Examen final		**EVALUACIÓN FINAL: Evaluación teórico-práctica/ Prueba de desarrollo** - **I:** Motivación y propósito de sesión. - **D**: El docente brinda las indicaciones antes de evaluar a los estudiantes con una prueba de desarrollo. - Los estudiantes desarrollan la evaluación final. - **C**: Metacognición, síntesis y retroalimentación	- Prueba de desarrollo	Método de casos (MC)	

Las actividades de aprendizaje autónomo en el aula virtual son las realizadas por el estudiante. Cada semana, el docente tiene el rol de monitorear, supervisar, evaluar y retroalimentar estas actividades, además de atender los foros y las comunicaciones generadas en el aula virtual.