UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA

CODIGO: 233003

CODIGO – SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA SGSI

LORENA PATRICIA SUAREZ SIERRA
(Director Nacional)

CARLOS ALBERTO AMAYA TARAZONA
Acreditador

BOGOTA, JULIO 2013

PROTOCOLO ACADEMICO

FICHA TECNICA

Nombre del curso:	Sistema de Gestión de la Seguridad de la Información.
Palabras clave:	Estándares, normas, riesgos, seguridad, metodología, análisis, auditoría, técnicas, etc.
Institución:	Universidad Nacional Abierta y a Distancia
Ciudad:	Bogotá
Autora del protocolo académico:	LORENA PATRICIA SUAREZ SIERRA
Año:	2013
Unidad académica:	Escuela de Ciencias Básicas, Tecnología e Ingeniería
Campo de formación:	Disciplinar
Área del conocimiento:	Seguridad informática
Créditos académicos:	Dos (2)
Tipo de curso:	Teórico
Destinatarios:	Estudiantes de la especialización de Seguridad Informática
Competencia General de aprendizaje	El estudiante maneja cada uno de las normativas de seguridad, de acuerdo a los estándares internacionales certificables de la ISO/IEC 27001, metodologías para identificación de riesgos, capacidad para auditar sistemas existentes de acuerdo a las normas.
Metodología de la oferta	Virtual
Formato de circulación	Campus virtual
Denominación de las unidades didácticas	Unidad 1: Gestión de la información Unidad 2: Sistema de Gestión de la seguridad

	Informática.

GLOSARIO DE TERMINOS

[1]**Amenaza:** Es todo aquella acción o elemento capaz de atentar contra la seguridad de la información.

Antivirus. Software encargado de detectar, bloquear y eliminar virus informáticos o código malicioso.

Ataque: Es la acción de interrumpir o dañar un activo de información con el objetivo de causar problemas de confiabilidad, disponibilidad e integridad. O también se puede afirmar que es cuando se materializa una amenaza de seguridad.

[2]**Código malicioso**: Software diseñado para ejecutar acciones maliciosas (como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario) y que incluye programas como virus, gusanos, troyanos y spyware. Puede utilizar como vía de diseminación, el correo electrónico, sitios de internet, redes, dispositivos móviles, dispositivos removibles (por ejemplo pen-drives).

Estándar de seguridad: Conjunto de normas o modelos diseñados con la finalidad de brindar soluciones de sistemáticas a un área del conocimiento específico.

Firewall: Un firewall o también llamados corta fuego, es un software o hardware que restringe el acceso a sitios web o una red sin autorización de acceso

Incidente de seguridad: Un incidente de seguridad es cualquier acción que atente contra la confiabilidad, disponibilidad e integridad de la información.

Ingeniería social: es la secuencia de acciones que tienen como finalidad la obtención de información, el fraude o el acceso no autorizado a sistemas informáticos, y que ha implicado en algún momento la manipulación psicológica de personas.

---

[1] Departamento de seguridad. Recuperado de http://www.seguridadinformatica.unlu.edu.ar/?q=glossary/term/14

[2] Departamento de Seguridad. Glosario. Recuperado de http://www.seguridadinformatica.unlu.edu.ar/?q=glossary/term/28

Intrusos: Es una Persona que intenta acceder a un sistema informático sin autorización, a través de técnicas y/o métodos informáticos que se lo permitan.

ISO: (International Organization for Standardization). Organización internacional de estándares

Metodología: Es un conjunto de reglas o métodos organizados de forma sistémica con el objetivo de lograr el cumplimiento de una norma o un estándar.

Phishing: Suplantación de identidad de una página o sitio Web.

[3]**Plan de contingencia:** Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

[4]**Riesgos:** Es la posibilidad de que una amenaza aproveche una vulnerabilidad y dañe un activo de información. Departamento de seguridad.

Repudio: Denegación, por una de las entidades implicadas en un a comunicación, de haber participado en la totalidad o en parte de dicha comunicación (ISO ISO-7498-2).

Seguridad lógica: Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos.

Seguridad física: Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, etc.

SGSI: Sistema de gestión de la seguridad de la información

Teletrabajo: El teletrabajo es un nuevo sistema de organización del trabajo en que la persona trabajadora desarrolla una parte importante de su trabajo fuera de la empresa y por medios telemáticos

Vulnerabilidad: Una vulnerabilidad de seguridad es un fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el fin de violar la política de seguridad del sistema. UOC. Guillermo Navarro Arribas. Introducción a las vulnerabilidades.

---

[3] Definición plan de contingencia. Recuperado de http://definicion.de/plan-de-contingencia/#ixzz2bEIjzN3w

[4] Departamento de Seguridad informática. Glosario. Recuperado de http://www.seguridadinformatica.unlu.edu.ar/?q=glossary/term/21

Wi-Fi (wireless fidelity o fidelidad sin cables): Es una red de ordenadores sin utilización de cables equivalente a la tecnología inalámbrica 802.11 para comunicación a distancia.

Wi-phishing: Wi-phishing, sustracción de datos personales a través de falsas redes públicas de acceso Wi-Fi

1. INTRODUCCION

El curso de Sistema de Gestión de la seguridad informática (SGSI), se enmarca en la especialización en el área formación disciplinar y en el componente de seguridad aplicada, con créditos académicos y una intensidad total de 72 horas con el objetivo de proporcionar al estudiante los conocimientos, normas y técnicas esenciales para la implantación de Sistemas de Seguridad de la información con calidad en cualquier organización, previa planeación y utilización de modelos, metodologías y estándares de certificación nacional e internacional.

Basado en los objetivos, el curso de SGSI, brinda la posibilidad de aplicar a nivel real en cualquier empresa, los estándares de seguridad propuestos por la ISO/IEC 27001, siendo este estándar el abanderado y certificado en el tema de seguridad. De la misma manera el curso permitirá que se apliquen herramientas de gestiones desarrolladas actualmente para llevar a cabo cada una de las etapas requeridas para la implantación y auditoria de un SGSI de calidad.

Al terminar el curso de SGSI, el estudiante estará preparado para implantar un sistema de seguridad de la información en cualquier organización siguiendo las normativas de los estándares de la ISO/IEC 27001, así mismo obtendrá las competencias esenciales para auditar un SGSI implantado en cualquier organización.

El curso del Sistema de Gestión de la Seguridad informática se encuentra organizado en dos unidades didácticas con tres capítulos cada una, repartidas de la siguiente manera: La unidad uno, contempla los capítulos, seguridad de la información, estándares de gestión de la seguridad de la información y procesos de análisis de Riesgos. La unidad 2, se compone de Plan de gestión de un SGSI, implantación de un SGSI y auditoría al SGSI.

Este curso marca su importancia en la medida en que el profesional especializado, estará en la capacidad de implantar un Sistema de Gestión de la Seguridad Informática en la organización que lo requiera, con las técnicas, métodos y planes necesarios para brindar la protección adecuada en una empresa. Así mismo está en la capacidad de desarrollar planes que brinden la continuidad de un negocio en caso de que su sistema de seguridad implantado sea vulnerado.

[5]El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. Así mismo la ISO 27001, considera que garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La metodología de aprendizaje que se plantea en el curso de SGSI, considera aspectos importantes de tipo analítico y lógico deductivo, en donde el estudiante desarrollará y/o perfeccionará su capacidad de estudio e interpretación de la información de los diferentes hallazgos obtenidos en una organización, para la implantación de medidas necesarias que eviten la ocurrencia de incidentes y le permitirá respectivamente al estudiante concluir los mecanismos apropiados para la protección y seguridad de la información en una empresa.

Las interactividades que enmarca el curso virtual de SGSI, se realiza mediante los recursos y actividades que proporciona el aula, donde el estudiante tendrá interacción con su tutor a través de los recursos de comunicación expuestos en el curso como los foros y la mensajería interna. En cuanto a las actividades, sería los trabajos individuales y grupales diseñados por el director del curso, así como actividades evaluativas como lecciones y trabajos colaborativos, entre otros. La interacción estudiante-estudiante también se presentará a través de los mismos recursos de comunicación y de las actividades colaborativas que impulsan de manera relevante la relación del estudiante con sus compañeros.

Los recursos tecnológicos utilizados en el curso son a través de la disponibilidad del curso virtual las 24 horas, así como la disponibilidad de herramientas de software que apoyan el desarrollo y aprendizaje del curso. Las fuentes documentales y demás material bibliográfico también estarán disponibles en múltiples formatos digitales (enlaces web, documentos en pdf, Word, etc.). y en la las bases de datos disponibles de la biblioteca virtual de la UNAD.

2. JUSTIFICACION

El curso de Sistema de Gestión de la información de la Seguridad Informática, marca su importancia en la especialización en la medida en que brinda las pautas, técnicas y métodos necesarios que se deben utilizar para implantar SGSI con las normas y estándares certificadas nacional e internacionalmente en el amplio tema de la seguridad informática.

[5] El portal de ISO 27001 en Español. http://www.iso27000.es/sgsi.html

El curso de SGSI, proporcionara un estudio amplio de la Norma internacional auditable ISO/IEC 27001, siendo esta la única norma que precisa los requisitos necesarios para la implantación y auditoria de un Sistema de Gestión de la Seguridad de la Información.

Las diferentes actividades evaluativas planteadas en el curso permitirá que el estudiante desarrolle habilidades de análisis e interpretación de la información obtenida en un análisis de riesgos al mismo tiempo que documentarlo, siendo esta la información determinante para la implantación de un SGSI.

El potencial que el curso brinda a los estudiantes, es indispensablemente, la forma apropiada para utilizar las técnicas, métodos y modelos que permitan la planeación y organización de un SGSI con el sello de calidad, en cualquier empresa, ya sea pequeña, mediana o grande. Así como también los protocolos y metodologías necesarias para realizar la auditoria a los SGSI.

El profesional especialista en Seguridad Informática, al terminar el curso se concientizará de la inevitable necesidad que tienen las empresas de proteger sus activos informáticos, tanto físicos como lógicos; entiéndase lógico, la información que se procesa para el funcionamiento de la empresa y físicos, todos aquellos equipos informáticos y medios de comunicación utilizados en la empresa para el procesamiento de la información. En este sentido el especialista que se desempeñe como tal, realizará los procesos y procedimientos necesarios para brindar a la organización un SGSI, apropiado y estandarizado.

La metodología aplicada para el estudio del curso, enfatiza en cada una de las actividades las competencias cognitivas para la apropiación del conocimiento, comunicativas para la interrelación personal y elaboración escrita, así como las habilidades para implementar los mecanismos de salvaguardias de la información y la respuesta inmediata a la solución de los ataques e incidentes de una empresa, en caso de presentarse. Así mismo el sistema de evaluación diseñado en el curso permitirá evaluar las competencias a través de la heteroevaluación, mediante el diseño de pruebas y la cooevaluación en el diseño de trabajos colaborativos.

3. INTENCIONALIDADES FORMATIVAS

Las intencionales formativas poseen como elementos estructurales del curso los siguientes:

- ✓ Propósitos
- ✓ Objetivos
- ✓ Competencias

- ✓ Metas de aprendizaje

3.1 Propósitos

- ✓ Fortalecer la capacidad de diseño y elaboración de documentos en el estudiante para implantar sistemas de gestión de la seguridad de la información que permita evitar los riesgos que consiguiera provocar un daño o deterioro a los activos informáticos lógicos y físicos de una organización.

- ✓ *Esbozar en el estudiante cada una de las series del estándar 27000, precisando en la serie certificable, la 27001.*

- ✓ Ejercitar la habilidad de redacción y síntesis del estudiante para formar documentos que definan la implantación de un sistema de gestión de la seguridad de la información e identificación de los riesgos en cualquier empresa.

- ✓ Preparar al estudiante sobre las formas de valoración que utilizan las normas del estándar ISO/IEC 27001 para auditar y certificar un Sistema de gestión de la Seguridad Informática.

3.2 Objetivos de aprendizaje

3.2.1 Objetivo General

Proporcionar al estudiante los mecanismos fundamentales para planificar, organizar e implementar un sistema de Gestión de la seguridad de la información SGSI, basados en las normas internacionales actuales y auditables de la ISO 27001 para la protección y conservación de la información esencial en cualquier empresa para su funcionamiento.

3.2.2 Objetivos específicos

- ✓ Lograr que el estudiante conozca y aplique la normativa de seguridad ISO 27001 y demás existentes para el proceso de implantación de un SGSI en una organización.

- ✓ Orientar al estudiante sobre las metodologías necesarias para realización de un análisis de riesgos que permita determinar los puntos vulnerables

sobre los sistemas o aplicaciones utilizadas en las empresas para su funcionamiento.

- ✓ Propiciar la utilización del modelo PDCA (planificar, hacer, verificar y actuar) como pasos lógicos necesarios para la implantación de un SGSI

- ✓ Brindar las técnicas, mecanismos y etapas necesarias para la implantación de un sistema de gestión de la seguridad de la Información.

- ✓ Proporcionar los mecanismos de control y evaluación de la implantación del SGSI por medio del sistema de auditorías para los procesos de certificación.

- ✓ Esbozar al estudiante la forma de estructurar un plan de continuidad de negocio en caso de presentarse un incidente de seguridad.

3.3 Competencias

El desarrollo del curso de Sistema de Gestión de la Seguridad Informática permitirá que el estudiante desarrolle diferentes competencias cognitivas con la apropiación del conocimiento de las normativas de seguridad de la información, las cuales proporcionan las pautas para la adopción de medidas necesarias de seguridad, con el objetivo de proteger la información como el activo más valioso en toda organización. Así mismo se apropiará de las diferentes técnicas actuales para el análisis de riesgos, implantación y auditoría de un SGSI.

La competencia comunicativa es una de las competencias más significativas que la especialización aporta a través de este curso, ya que estimula la producción escrita, siendo esta una de las tareas que el profesional especializado debe realizar a la hora de implantar y mejorar un sistema de gestión de la seguridad de la información, siguiendo los requisitos propuestos por el estándar de seguridad de la información ISO/IEC 27001. En este orden, el curso también proporcionará otras competencias que permitirán desarrollar la habilidad en el estudiante para reflexionar sobre cada los casos que se puede presentar en cualquier organización en relación a los incidentes de seguridad presentados, así como la forma apropiada para afrontar y solucionar con responsabilidad los diferentes problemas presentados en cualquier empresa referentes al tema objeto de estudio, logrando el equilibrio organizacional con el desarrollo de planes de continuidad de negocio.

3.4 Metas de aprendizaje

- ✓ Al finalizar el curso el estudiante desarrollará una evaluación final por proyecto, donde aplicará todos los conocimientos aprendidos durante el curso.

- ✓ Estará el estudiante en la capacidad de realizar informes documentales sobre el análisis de riesgos realizados en cualquier empresa.

- ✓ El estudiante desarrollará actividades que le permitirá obtener habilidades en cada uno de los temas propuestos en el curso de SGSI.

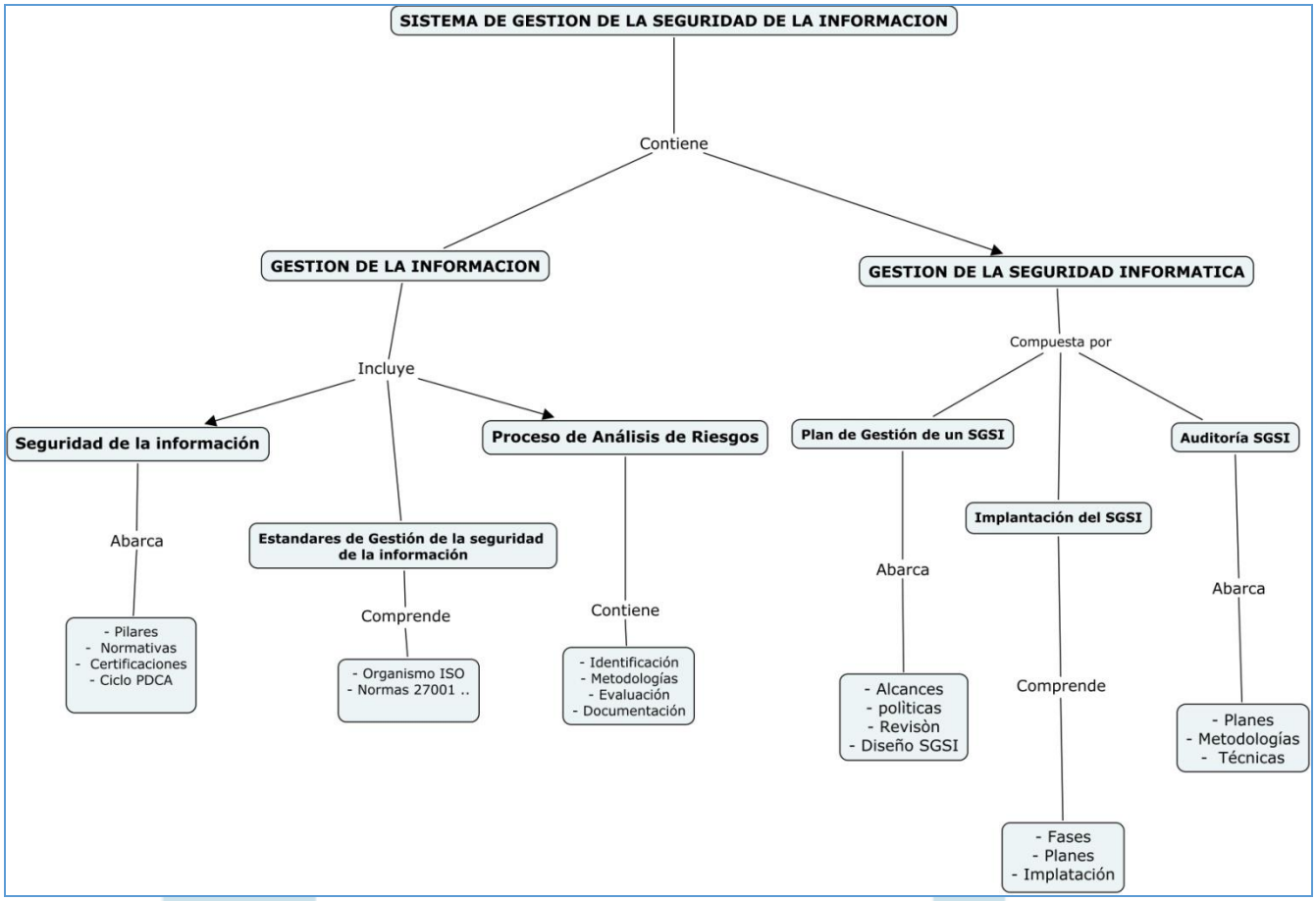
- ✓ Las actividades propuestas en el curso le permitirá al estudiante aplicar los estándares para implantación de Sistemas de Gestión de la Seguridad informática estudiadas en el curso.
- ✓ Estará en la capacidad de realizar auditorías de SGSI implantadas en cualquier organización bajo el estándar certificable ISO/IEC 27001.

4. UNIDADES DIDACTICAS

Primera Unidad	Capítulo	Temas
GESTION DE LA INFORMACION	**SEGURIDAD DE LA INFORMACIÓN**	Lección 1: Pilares de la informática Lección 2: Realidad de las empresas en seguridad de la información Lección 3: Normativas de seguridad Lección 4: ¿Cómo se estructuran las normativas de gestión de la seguridad Lección 5: Estado de implantación de normativas de seguridad de la información en Colombia.
	ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Lección 6: La organización ISO y la familia de normas ISO Lección 7: Familia de las normas ISO/IEC 27001:2005 Lección 8: La normativa ISO/IEC 27001:2005 y afines Lección 9: Integración del SGSI (ISO 27001) a ISO 9001 –- 14000 Lección 10: Consideraciones para implantación de un SGSI(norm ISO 27001) en una organización
	PROCESO DE ANALISIS DE RIESGO	Lección 11: Proceso de Identificación del riesgo Lección 12: Metodología de análisis de Riesgos Magerit Lección 13: otras metodologías Lección 14: Herramientas de apoyo al análisis de riesgos Lección 15: documentación

Segunda Unidad	Capítulo	Temas
SISTEMA DE GESTION DE LA SEGURIDAD INFORMATICA	PLAN DE GESTIÓN DE UN SGSI	Lección 16: ¿Cómo definir el alcance del SGSI? Lección 17: Estructura organizacional para el SGSI Lección 18: Política de seguridad Lección 19: Análisis de requisitos y diseño del SGSI Lección 20: Normativa legal Colombiana
	IMPLANTACIÓN DEL SGSI	Lección 21: Fases para la implantación del SGSI Lección 22: Formación y concientización del personal Lección 23: Provisión de recursos Lección 24: Plan de tratamiento de riesgo Lección 25: Gestión de continuidad de negocio
	AUDITORIA AL SGSI	Lección 26: Auditorías internas lección 27: Metodología para auditoría del SGS Lección 28: Técnicas e Instrumentos para auditorías Lección 29: Certificación SGSI Lección 30: Mantenimiento y mejora del SGSI

MAPA CONCEPTUAL DEL CURSO



5. CONTEXTO TEORICO

Así como la tecnología de la información y las comunicaciones avanza vertiginosamente, en este sentido avanzan las técnicas, métodos y aplicaciones para asegurar la información, siendo ésta para los usuarios y empresas un activo inmaterial con un alto valor, que si llegase a ocurrir pérdida, modificación, hurto, entre otros, de la información, generarían problemas que serían delicados solucionar. En tal sentido la seguridad informática es el conjunto de reglas, planes y acciones encaminadas a garantizar tres objetivos:

- ✓ La capacidad de trabajo (disponibilidad), en cuanto a que el sistema esté operativo en todo momento, o haya mecanismos de contingencia que permitan un ritmo de trabajo aceptable mientras se soluciona el problema.

- ✓ La integridad de la información (consistencia), de modo que la información puesta a disposición del usuario sea oportuna.

- ✓ La confidencialidad de los datos (confidencialidad, control de acceso, autenticación), para que cada usuario tenga acceso sólo a la información que le corresponde.

Un sistema informático se considera protegido cuando se involucra el hardware, software y toda la información que viaja a través de las redes y queda almacenada en discos duros y demás dispositivos de almacenamiento externo. Existen diversidades de ataques a todo un sistema informático más precisamente a la información con el objetivo de vulnerar los tres pilares de la seguridad informática (confidencialidad, integridad, disponibilidad y autenticidad), los cuales se clasifican en cuatro grupos:

Interrupción: Ataque causado al hardware de un sistema con el objetivo de no dejar disponible el recurso. Ejemplo: Corte de cableado de redes de comunicaciones, destrucción de equipos, etc.
Interceptación: Ataque contra la confidencialidad, en el que una información ha sido obtenida por personal no autorizado. Ejemplo: información confidencial o de uso privado accedido por un tercero a través de un medio de comunicación.
Modificación: Ataque contra la integridad y la confidencialidad en el que, además de obtener el acceso no autorizado a un recurso, también se consigue su eliminación o modificación. Ejemplo: Modificación de sitios web, eliminación de información en bases de datos, etc.).
Fabricación: Ataque contra la integridad en el que un elemento consigue crear o insertar objetos falsificados en el sistema. Ejemplo: Añadir de forma no autorizada un nuevo usuario y su contraseña correspondiente en el fichero de contraseñas.

Los mecanismos de seguridad de la información donde involucra prevención, detención y recuperación se deben realizar a través de la implantación de un sistema planificado y concienzudo, con el objetivo de preservar de manera organizada y controlada la protección a todo el sistema informático en general. Es por tanto que se han creado normativas o sistemas estándares que abarcan en gran medida todos aquellos aspectos que se deben tener en cuenta para brindar una alta protección a la información que se genera en cualquier empresa para su funcionamiento y la prestación de servicio a sus clientes. En este sentido la organización Internacional de estándares (ISO), desarrolla el estándar internacional ISO/IEC 27001, para la implantación de sistemas de gestión de la seguridad de la Información con el objetivo de crear normativas que involucre en forma planificada todos los elementos, recursos y mecanismos que se deben considerar a la hora de implantar un sistema que ofrezca a las empresas las consideraciones de seguridad necesaria para proteger sus activos informáticos (hardware, software e información).

6. METODOLOGIA GENERAL

La metodología para el estudio del curso se desarrollará de manera virtual, soportada con materiales didácticos de aprendizaje en diferentes formatos digitales, donde el estudiante podrá acceder a ella durante todo el tiempo que lo desee para su estudio y aprendizaje del curso.

El curso de Sistema de Gestión de la seguridad de la información, proporcionará al estudiante diferentes fases de reconocimiento, profundización y transferencia con el objetivo de integrar de manera planificada todos los recursos y actividades que son necesarias para la apropiación de cada una de las temáticas planteadas en el curso. De esta manera el curso virtual estará organizado por cada una de las fases que se considera debe realizar el estudiante para su mayor aprendizaje y motivación. A continuación se describe la forma como se plateará el aprendizaje en cada una de las fases anunciadas:

Fase de reconocimiento: En esta fase el estudiante a través de la exploración de los contenidos del curso, y de material didáctico complementario desarrollará actividades de reconocimiento diseñadas en el curso virtual, que le permitirá sumergirse poco a poco al conocimiento general que le proporciona el curso.

Fase de profundización: A medida que se avanza en el curso, el conocimiento se hace mas profundo porque aporta en el estudiante las herramientas conceptuales y didácticas necesarias, así como las actividades diseñadas tienen una connotación interesante que permite en el estudiante desarrollar su potencial intelectual.

Fase de transferencia: En esta fase el estudiante aplica a una realidad los conocimientos y destrezas adquiridas durante el aprendizaje del curso, así mismo desarrolla competencias y capacidades para desarrollar las fases o etapas previas y de planificación que se debe realizar en la implantación de un SGSI.

Durante el desarrollo del curso, se programaran actividades de estudio independiente por parte del estudiante, ya que al formarse adquiere un alto grado de conciencia sobre la responsabilidad que tiene con respeto a su aprendizaje, a su vez le permite desarrollar competencias lectoras, analíticas, comunicativas, entre otras para dar respuesta asertiva en cada una de las actividades propuestas en el curso. En el estudio independiente, el estudiante podrá hacerlo de manera individual y en grupos colaborativos a través de diferentes medios de comunicación sincrónica (chats, webconferencia, etc.) y asincrónica (foros, correos, etc).

El acompañamiento tutorial es la orientación institucional en las áreas y temáticas planteadas en el curso por el tutor profesional especializado, quién será la persona encargada de asesorar, orientar en los contenidos didácticos planteados en el curso, al igual que proveer información, bibliografía y material complementario

requerido para su aprendizaje en los diferentes formas, individual, en pequeños grupos colaborativos y en forma general.

Por ser un curso de dos créditos, el material didáctico está enfocado a dos unidades y tres capítulos. En cada unidad se abordan actividades que implican el reconocimiento, la profundización y la transferencia. A continuación se presentan cada una de estas actividades.

Las actividades de reconocimiento

Revisión de presaberes

En esta actividad se plantea una lección evaluativa que evalúa al estudiante su capacidad de interpretación de los temas planteados en documentos y artículos que abordan las temáticas de la seguridad de la información.

Foro general y de actores

Esta actividad de reconocimiento general son de carácter individual que permite al estudiante adentrarse en los temas inherentes al proceso de implementación de un sistema de gestión de la seguridad de la información en las empresas, identificando en forma exploratoria, los posibles activos de información utilizados por las empresas para el cumplimiento de su misión.

Así mismo en esta actividad se establece una comunicación de reconocimiento entre cada estudiante del pequeño grupo colaborativo, donde cada uno realiza su presentación y comenta las expectativas del curso.

Las actividades de reconocimiento también se desarrollan en cada unidad y se diseñan a través de lecciones evaluativas que abordan a nivel general los temas que serán estudiados en la unidad.

Actividades de profundización

Las actividades de profundización que se plantea en cada una de las unidades del curso, están compuestas por una lección de la unidad, que a través de ella se evalúa en línea los contenidos de la unidad.

También se realizan en cada unidad actividades colaborativas que permite el trabajo en equipo y la interacción grupal.

Actividades de transferencia

Las actividades de transferencia se componen de: Una lección evaluativa y un foro de trabajo colaborativo por cada unidad. Se incluye también en esta fase de transferencia en el examen final del curso un foro de trabajo colaborativo.

En las actividades planteadas en cada unidad de los trabajos colaborativos, se ve reflejada la transferencia por cuanto el estudiante realiza actividades sobre un entorno real, donde le permitirá aplicar los conocimientos adquiridos sobre los estándares de la ISO 27001.

Así mismo en el examen final, se proyecta de manera aplicada, por cuanto el estudiante organiza, profundiza y diseña instrumentos que le permita realizar la actividad de manera eficiente y eficaz.

7. SISTEMA DE EVALUACION

El sistema de evaluación se realizará de manera virtual, a través de diferentes actividades planteadas en el curso de forma individual y en trabajos colaborativos. Cada una de las actividades tendrá su puntaje. Los tipos de evaluación Coevaluación, heteroevaluación y autoevaluación se reflejan en las actividades diseñadas del curso.

La coevaluación, se ve reflejada en los trabajos colaborativos planteados en el curso, por cuanto el estudiante revisa los aportes enviados por otros compañeros, los evalúa y envía sus apreciaciones y recomendaciones al respecto para posteriormente construir un trabajo final en conjunto.

La heteroevaluación, se refleja en la evaluación que el docente tutor hace al estudiante y/o al grupo con respecto a las actividades enviadas.

La autoevaluación, se refleja en el curso, en la medida en que el estudiante autorevisa su actividad de aprendizaje a través de la rúbrica de evaluación planteada en cada actividad, antes de enviarla a evaluar por el docente.

8. SISTEMAS DE INTERACTIVIDADES

Las interactividades de tutor y director de curso con los estudiantes se abordan a través de la interactividad en el foro general del curso, el correo interno.

Las interactividades entre compañeros de grupo se refleja en el foro de reconocimiento general y de actores, los foros de los trabajos colaborativo, el foro general y la mensajería o correo interno del aula o curso virtual.

9. Recursos Tecnológicos.

Adicional al módulo de curso, presentado en diferentes formatos, el estudiante podrá utilizar material complementario presentado en la web, podrá acceder a las bases de datos especializadas a través de la biblioteca virtual, podrá utilizar herramientas o aplicativos que apoye al estudiante para realizar la actividad y podrá tener acceso a objetos virtuales de aprendizaje y objetos informativos.

Para la interactividad grupal, el estudiante también podrá utilizar otras aplicaciones externas como Skype.

10. Fuentes documentales

El estudiante podrá completar o profundizar su aprendizaje a través de diferentes medios escritos y publicados en la web. A

11. Bibliografía

Casanovas, Inés (2009). Gestión de archivos electrónicos. P 205. Argentina. Alfagrama Ediciones.

Sandoval Serrano, René Mauricio. Calidad y desarrollo organizacional a través de la certificación ISO 9000. Argentina: El Cid Editor | apuntes, 2009. p 12

Daniel cruz Allende. (2006). Gestión de la Seguridad de la Información. Universidad Oberta de Catalunya – UOC.

Rafael Estevan de Quesada. (2007). Auditoría técnica y de certificación. Universidad Oberta de Catalunya – UOC.

12. Cibergrafía

Universidad Politécnica de Madrid. Red temática de Criptografía y seguridad de la información. CRITORED. Recuperado de http://www.criptored.upm.es/

Instituto Nacional de la Tecnología de la Comunicación de España. Centro de respuestas a incidentes de seguridad TIC. Recuperado de http://cert.inteco.es/cert/INTECOCERT/;jsessionid=8D54CF8208B2AAAA4A8AD638C109B9B0?postAction=getCertHome

Organización internacional de estándares- ISO. Sistema de Gestión de la Seguridad de la Información. Portal ISO 27001 en español. Recuperado de http://www.iso27000.es/sgsi.html

Universidad Politécnica de Madrid de España (2010). Information Security enciclopedia - Intypedia. Enciclopedia de la Seguridad de la Información. Recuperado de http://www.intypedia.com/