Carrera: **Analista Programador**

Arquitectura de Sistemas Operativos

Módulo II

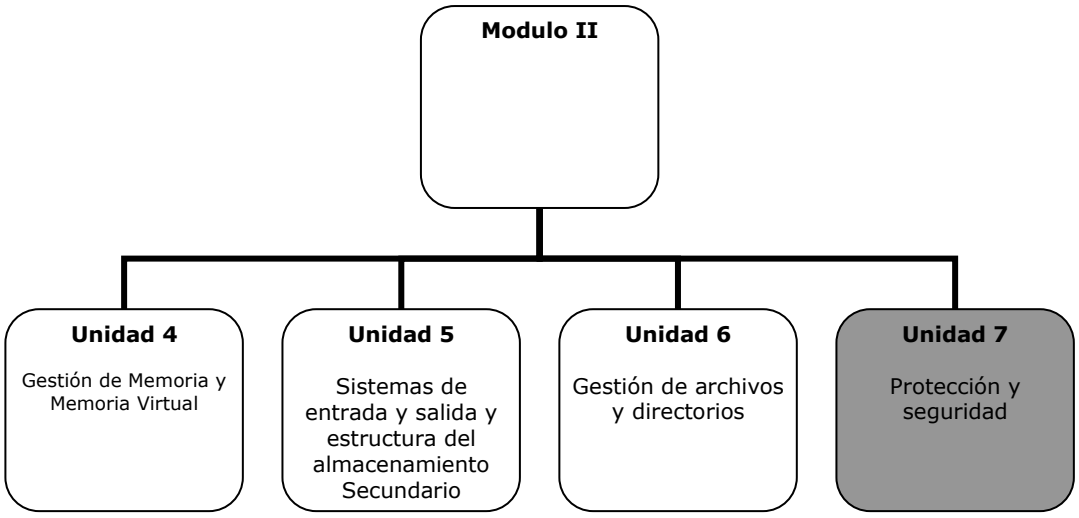
Comprender como el Sistema Operativo realiza la administración de recursos del Sistema de Computación

Unidad 7

Protección y seguridad.

Profesor Titular: Martín Ricardo.

Autor de contenidos: Romero Juan Carlos.



Presentación

Con esta unidad presentamos el último tema que consideramos relevante para esta asignatura la protección y seguridad de los sistemas de computación.

Tal como hemos estudiado los sistemas de computación a medida que pasa el tiempo se tornan cada vez más complejos y existen mayor cantidad de sistemas interconectados a través de redes. Es por ello que los SO deben dar respuesta a este cambio y un aporte muy importante es **la protección del sistema**, tema que abordaremos en esta última unidad.

¿Qué se debe proteger en un Sistema de computación, si sabemos que el mismo esta compuesto por uno o más procesadores, memoria principal, relojes, terminales, discos, interfaces de red, dispositivos de entrada y salida, archivos, procesos y usuarios?

Seguramente lo que deberíamos proteger son todos los elementos del sistema, pero pensemos en aquellos elementos que son críticos en el procesamiento de datos, en este momento todos estamos pensando lo mismo, el "procesamiento de datos" y de aquí surge procesos y datos, entonces la protección se enfoca en estos dos términos y los elementos que con ellos se relacionan, por ejemplo: los recursos del sistema que contienen a los procesos y a los archivos; la memoria, el file system, los dispositivos de almacenamiento magnético.

Para proteger hay que tener en cuenta dos conceptos importantes, la política y el mecanismo, la política define las acciones que se deben tomar para la protección y los mecanismos definen cómo se deben implementar las acciones.

Es casi intuitivo la comprensión del por qué tenemos que proteger los archivos que contienen datos, ya que el hombre actual, está rodeado de un aura de datos (pido perdón a los místicos) y de elementos tecnológicos que los almacenan y los procesan y aquí aparece el otro elemento a tener en cuenta en la protección, los procesos; sí queremos cuidar el valor de la información también debemos cuidar los procesos que procesan la datos ya que éstos son los que la generan la información para la toma de decisiones.

Por todo lo expresado hasta aquí es que esperamos que usted, a través del estudio de esta unidad, adquiera capacidad para:

- Comprender la importancia de la protección y la seguridad de los datos y los procesos.
- Entender las políticas y los mecanismos destinados a la protección y la seguridad.
- Estudiar ejemplos de protección en SO como UNIX y Multics.

- Comprender el problema de seguridad en los SO actuales y las herramientas utilizadas para implementarla.
- Estudiar las amenazas por programa y las amenazas al sistema.

A continuación, le presentamos un detalle de los contenidos y actividades que integran esta unidad. Usted deberá ir avanzando en el estudio y profundización de los diferentes temas, realizando las lecturas requeridas y elaborando las actividades propuestas, algunas de desarrollo individual y otras para resolver en colaboración con otros estudiantes y con su profesor tutor.

Contenidos y Actividades

1. Objetivos y dominios de protección

Lectura requerida

- Silberschatz A. y Galvin P.; Capitulo 19 Protección. Página 597**. En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999.

Lectura Sugerida

- Stallings W.; Capítulo 16 Seguridad. Página 695**. En su: Sistemas Operativos –Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007.
- Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección. Página 531; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007.
- Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y protección. Página 497**. En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001.

1.1. Matriz de acceso e implementación.

Lectura requerida

- Silberschatz A. y Galvin P.; Capitulo 19 Protección. **En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999. Página 597**.**

Lectura Sugerida

- Stallings W.; Capítulo 16 Seguridad **En su: Sistemas Operativos – Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007. Página 695**.**
- Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección. Página 531; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007.
- Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y Protección. **En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001. Página 497.

1.2 Sistemas de protección

Lectura requerida

- Silberschatz A. y Galvin P.; Capitulo 19: Protección. **En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999. Página 597

Lectura Sugerida

- Stallings W.; Capítulo 16 Seguridad. **En su: Sistemas Operativos – Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007. Página 695**.**
- Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección.; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007.Página 531
- Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y protección.**. En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001. Página 497.

2. El problema de la seguridad: validación y contraseñas

Lectura requerida

- Silberschatz A. y Galvin P.; Capitulo 20 Seguridad. **En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999. Página 623**.**

Lectura Sugerida

- Stallings W.; Capítulo 16 Seguridad. **En su: Sistemas Operativos – Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007. Página 689**.**
- Silberschatz A. Galvin P. Gagne G.; Capítulo 15 Seguridad. **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007. Página 559.
- Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y protección. **En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001. Página 497**.**

2.1 Amenazas, vigilancia, cifrado y clasificación de seguridad de los computadores.

Lectura requerida

- Silberschatz A. y Galvin P.; Capitulo 20 Seguridad **En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999. Página 623**.**

Lectura Sugerida

- Stallings W.; Capítulo 16 Seguridad. Página 689**. En su: Sistemas Operativos –Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007.
- Silberschatz A. Galvin P. Gagne G.; Capítulo 15 Seguridad.; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007. Página 559.
- Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y protección. **En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001. Página 497.

Trabajo Práctico Sugerido

- Trabajo Práctico Nº 14 **Protección y seguridad**

Cierre de la unidad

ANEXO

Para el estudio de estos contenidos usted deberá consultar la bibliografía que aquí se menciona:

BIBLIOGRAFÍA OBLIGATORIA

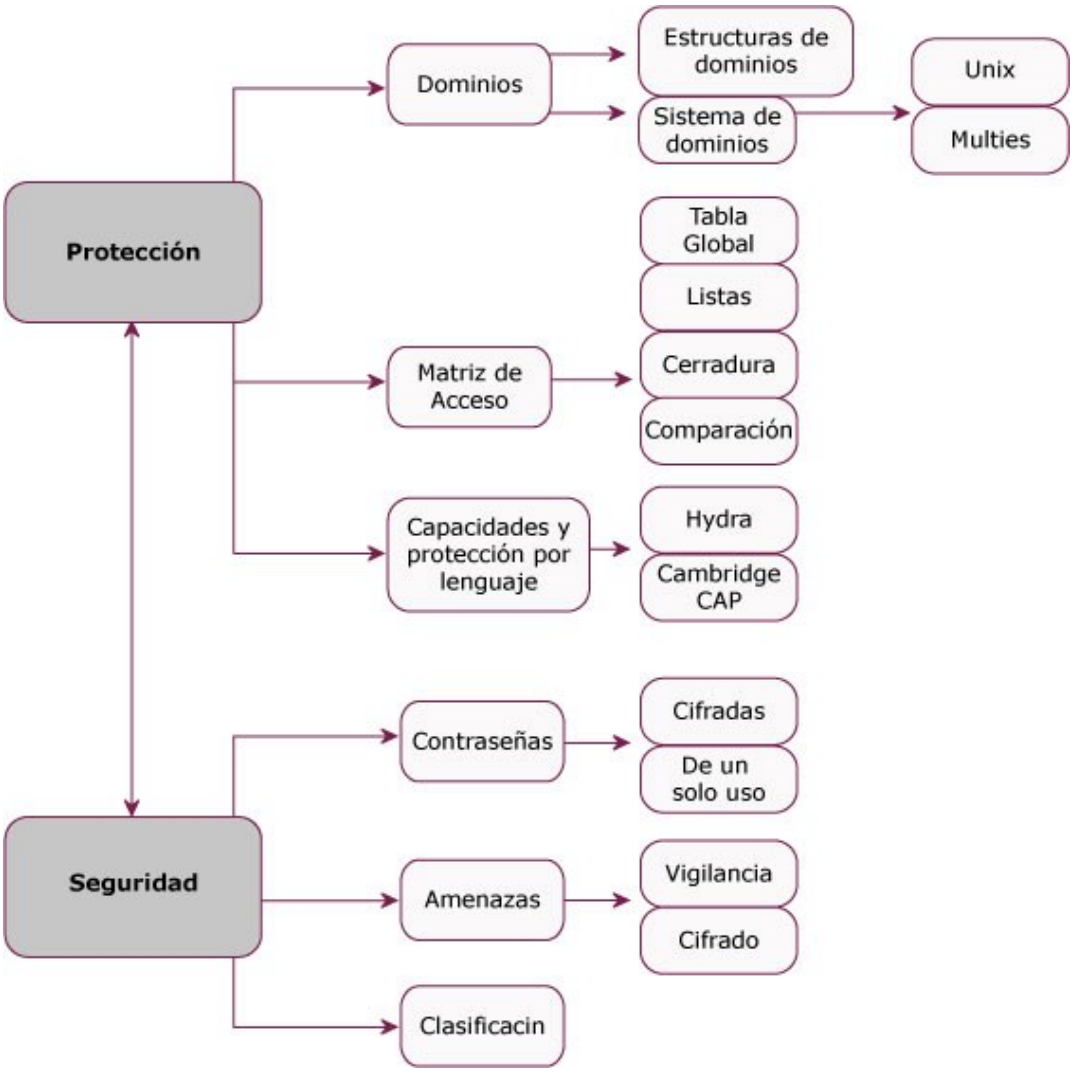
- Silberschatz A. y Galvin P.; **Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999.
- Stallings W.; **Sistemas Operativos –Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007.
- Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; **Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001.

BIBLIOGRAFIA AMPLIATORIA

- Tanembaum A. Woodhull A.; **Sistemas Operativos –Diseño e implementación-**; 2da Edición; México Prentice Hall 1997.
- Silberschatz A. Galvin P. Gagne G.; **Fundamentos de Sistemas Operativos**; 7ma Edición; España Mc Graw Hill 2007.

Organizador Gráfico

El siguiente esquema le permitirá visualizar la interrelación entre los conceptos que a continuación abordaremos. Le sugerimos que vuelva a este organizador una vez completado el estudio de la unidad, le ayudará a ordenar sus ideas.



Lo/a invitamos ahora a comenzar con el estudio de los contenidos que conforman esta unidad.

1. Objetivos y dominios de protección

Pensemos en nuestra casa como un sistema "hogar" donde la protección es algo sumamente importante, ¿cómo lograr el buen funcionamiento de todos los elementos que la forman para hacer de la casa un lugar cálido, agradable, familiar, funcional e inteligente?

Para lograr el objetivo propuesto cada artefacto que esta dentro de la casa: heladera, cocina, microondas, termotanque, calefactor, teléfono, la radio biblioteca, la sala de meditación, etc. Todo debe cumplir su objetivo y para llegar al objetivo es muy importante el buen funcionamiento de todos los elementos.

No sería bueno que la heladera no enfríe lo que corresponde o que la cocina o el calefactor tuviera una perdida de gas o que el termotanque no tuviera una válvula de presión que se active por una falla en el termostato y explote en una junta de la cañería como ocurrió una vez en mi propia casa, o que en la biblioteca no hubiera ningún libro o que la sala de meditación estuviera toda sucia y desprolija de esta manera nuestra casa no sería el "hogar" deseado.

Quizás el automóvil no debería ser un integrante de los elementos de nuestra casa, pero una lectura simple de la realidad actual nos muestra otra cosa y usaremos el auto para asociarle un conjunto de operaciones que podrían tener los autos del futuro.

Nuestro automóvil del futuro disminuiría de velocidad automáticamente cuando un sensor detecte niebla, sería tan inteligente que respetaría las señales de alta velocidad, si la velocidad máxima es 100 Km por hora, el auto no aceleraría a más de 100 Km por hora, si un cartel indica que no se puede doblar a la izquierda el auto se negaría doblar a la izquierda, se negaría seguir adelante si hay una indicación de contramano, lamentablemente, este auto reemplazaría la conciencia del ser humano, nuestro auto del futuro marca ciertamente una gran avance de la tecnología pero no marca una evolución del hombre, quizás sería mejor dejar las cosas como están.

Lo que rescatamos de nuestro auto no es su moralidad, sino las operaciones asociadas al objeto auto.

Mi recomendación es volver a releer este texto luego de estudiar los objetivos y dominios de protección y realizar una asociación entre el texto y los conceptos estudiados.

Suerte con la asociación!

Lectura requerida

Silberschatz A. y Galvin P.; Capitulo 19 Protección. Página 597**. En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999.

Lectura Sugerida

Stallings W.; Capítulo 16 Seguridad. Página 695**. En su: Sistemas Operativos –Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007.

Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección. Página 531; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007.

Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y protección. Página 497**. En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001.

Guía para la lectura

Durante o luego de la lectura de la bibliografía responda las siguientes preguntas:

- ¿Qué son los dominios de protección?
- ¿Qué es una estructura de dominios?
- ¿Qué es un sistema con dos dominios de protección?
- ¿Estudie el caso UNIX y el caso MULTICS?

1.1. Matriz de acceso e implementación.

Debería haber alguna forma de abstraer en un modelo el comportamiento de nuestro automóvil, de nuestra heladera, microondas, termotanque y de todos los objetos de la casa deseada para que el sistema que los controle tuviera información de sus comportamientos.

Para ello existe un modelo conceptual que se llama Matriz de acceso, en ella podríamos escribir los objetos en las columnas y las funcionalidades en las filas.

Por supuesto, que nuestro modelo cambiaría si los objetos no son los elementos de nuestro hogar y son los recursos del sistema de computación que pretendemos proteger, notemos que el nombre del modelo es Matriz de acceso y no matriz de funcionalidades, del nombre se deduce que lo que trata de describir la Matriz son los diferentes tipos de acceso que son permitidos sobre cada recurso.

Existen distintas formas de implementar una Matriz de acceso, aquí solo las nombraremos ya que el estudio de este capítulo de la materia nos dará todo el conocimiento de los siguientes tipos de implementación:

- Tabla Global
- Lista de acceso para objetos
- Listas de capacidades para dominios
- Mecanismo de cerradura y llave
- Comparación

Lectura requerida

Silberschatz A. y Galvin P.; Capitulo 19 Protección. **En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999. Página 597**.**

Lectura Sugerida

Stallings W.; Capítulo 16 Seguridad **En su: Sistemas Operativos – Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007. Página 695**.**

Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección. Página 531; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007.

Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y Protección. **En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001. Página 497.

Guía para la lectura

Durante o luego de la lectura de la bibliografía responda las siguientes preguntas:

- ¿Describa el uso de la matriz de acceso?
- ¿Explique tabla global?
- ¿Explique listas de accesos para objeto?
- ¿Explique listas de capacidades para dominios?
- ¿Explique mecanismo de cerradura y llaves?
- ¿Explique comparación?

1.2 Sistemas de protección

En este punto luego de haber estudiado la matriz de acceso y su implementación, usted cuenta con los conocimientos necesarios para poder presentar y entender una breve reseña de dos sistemas de protección basados en la implementación de la matriz de acceso como listas de capacidades, éstos son : el sistema de protección Hydra y el sistema Cambridge CAP.

La protección que ofrece un Sistema de Computación, se basa en la ayuda que brinda el núcleo del SO, pero a medida que ha ido aumentando la complejidad de los Sistemas de Computación y de los SO, se hizo necesario ampliar las posibilidades de protección, una de esas posibilidades es poder implementar protección desde los lenguajes utilizados por los diseñadores de aplicaciones y no solo por los diseñadores del SO.

En este punto de la unidad estudiaremos ejemplos concretos que lo ayudarán a entender los mecanismos de protección basados en capacidades y la necesidad que surge de la evolución tecnológica de ampliar la posibilidad de protección a los lenguajes de programación de aplicaciones.

Lectura requerida

Silberschatz A. y Galvin P.; Capitulo 19: Protección. **En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999. Página 597.

Lectura Sugerida

Stallings W.; Capítulo 16 Seguridad. **En su: Sistemas Operativos – Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007. Página 695**.**

Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección.; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007.Página 531

Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y protección.**. En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001. Página 497.

Guía para la Lectura

Durante o luego de la lectura de la bibliografía responda las siguientes preguntas:

- Describir el sistema Hydra y Cambridge CAP.
- ¿Cuáles son las ventajas de la protección basada en el lenguaje?
- ¿Qué ventajas tiene la protección basada en el núcleo del SO?
- ¿Cuáles son las funciones que se obtienen de la protección basada en el lenguaje?

2. El problema de la seguridad: validación y contraseñas

El problema de la protección planteado en el punto 1 de esta unidad es algo sumamente importante para lograr el buen funcionamiento de todos los elementos que forman el sistema "hogar" y hace especial referencia a lo que esta dentro de la casa.

El problema de la seguridad de la casa, hace referencia a lo que sucede desde el exterior, y plantea la posibilidad de una violación de seguridad maliciosa o accidental, por ejemplo podemos plantear la lectura o destrucción de nuestra correspondencia por personas no autorizadas.

Muchas veces el cartero deja la correspondencia dentro del buzón que está en la puerta de nuestro hogar y accidentalmente puede quedar expuesta, en este caso, cualquier persona que pasa por la calle podría tomarla y usarla maliciosamente ya que ahora conoce datos que no le pertenecen y que podría usar para cometer un delito.

Quizá esa correspondencia era algo muy importante, algo que estábamos esperando, en este caso la falta de información nos podría llevar a un problema financiero por falta de información.

Con mayor peligrosidad alguien podría entrar a nuestra casa y tomar información que no le pertenece.

Por supuesto, que este punto de la unidad se refiere a los accesos indebidos, maliciosos o accidentales, que se efectúan sobre los recursos del sistema de computación, más específicamente al acceso de los archivos, por ejemplo: usuarios que no les pertenece determinada información, por motivos maliciosos quieren conocerla, modificarla o destruirla, por otro lado estas modificaciones también se podría realizar accidentalmente.

Ante el problema de la protección y la seguridad de nuestros hogares surge la necesidad de la validación o la identificación del dueño de casa para permitirle su ingreso entonces podemos pensar en mantener todas las puertas y las ventanas de la casa con cerraduras y sólo permitir el acceso a aquella persona que tiene llaves de la puesta y la reja, de manera tal que el ingreso se hace pasando por dos validaciones de llaves.

Los SO también implementan un sistema de validación de usuarios para que pueden acceder al uso de un sistema de computación, la diferencia es que aquí la llave de la puerta es un contraseña, como la que usamos para acceder al uso de un cajero automático de cualquier banco.

En este ítem de la unidad también estudiaremos la validación y los diferentes tipos de contraseñas.

Lectura requerida

Silberschatz A. y Galvin P.; Capitulo 20 Seguridad. **En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999. Página 623**.**

Lectura Sugerida

Stallings W.; Capítulo 16 Seguridad. **En su: Sistemas Operativos – Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007. Página 689**.**

Silberschatz A. Galvin P. Gagne G.; Capítulo 15 Seguridad. **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007. Página 559.

Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y protección. **En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001. Página 497**.**

Guía para la Lectura

Durante o luego de la lectura de la bibliografía responda las siguientes preguntas:

- ¿Describa el problema de la seguridad?
- ¿Qué es la validación por contraseñas?
- ¿Qué son las contraseñas cifradas?
- ¿Qué son las contraseñas de un solo uso?

2.1 Amenazas, vigilancia, cifrado y clasificación de seguridad de los computadores.

Existen diversas formas con las cuales se puede atacar un sistema do computación, por ejemplo la ejecución de programas por parte de personas no autorizadas, programadores mal intencionados que desarrollan programas que en apariencia no provocan daños, sin embargo, parte de su código fue programado para cometer un delito, por ejemplo sumar centavos de dólar a

una cuenta bancaria o lograr que algún proceso se reproduzca muchas veces para consumir recursos del sistema, en este contexto la vigilancia del sistema se vuelve algo de suma importancia junto con la posibilidad de almacenar la identificación de los usuarios, su fecha y hora de conexión y de desconexión y las operaciones que haya realizado sobre los objetos del sistema.

En este punto de la unidad estudiaremos los aspectos relacionados con las amenazas provenientes de programadores y usuarios malintencionados, la vigilancia que se debe realizar para evitar daños, el cifrado como forma de proteger la información que se transmite entre distintas computadoras utilizando una red de transmisión y las clasificaciones de seguridad de computadoras basados en criterios de evaluación de confiabilidad de sistemas de computación del departamento de la defensa de los Estados Unidos.

Lectura requerida

Silberschatz A. y Galvin P.; Capitulo 20 Seguridad **En su: Sistemas Operativos**; 5ta Edición; México Addison Wesley; 1999. Página 623**.**

Lectura Sugerida

Stallings W.; Capítulo 16 Seguridad. Página 689**.** **En su: Sistemas Operativos –Aspectos Internos y principios de diseño-**; 5ta Edición; España Prentice Hall, 2007.

Silberschatz A. Galvin P. Gagne G.; Capítulo 15 Seguridad.; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007. Página 559.

Carretero Pérez J. De Miguel Anasagasti P. García Carballeira F. Pérez Costoya F.; Capítulo 9 Seguridad y protección. **En su: Sistemas Operativos –Una visión aplicada-**; España Mc Graw Hill, 2001. Página 497.

Guía para la lectura

Durante o luego de la lectura de la bibliografía responda las siguientes preguntas:

- ¿Qué es un caballo de troya?

- ¿Qué es una puerta secreta?
- ¿Qué es un gusano?
- ¿Qué es un virus?
- ¿En qué consiste la vigilancia de amenazas y la bitácora de auditoria?
- ¿Qué es el cifrado?
- Describa la clasificación de seguridad de las computadoras.

Trabajo Práctico Sugerido

Trabajo Práctico: **Nº 14 Protección y seguridad**

Usted encontrará las consignas de este Trabajo Práctico en el Anexo que incluimos al final de este Orientador.

Comparta sus dudas e inquietudes con sus pares y con su tutor a través de los medios de comunicación disponibles en el Campus.

EVALUACIÓN PARCIAL

Propuesta para la Integración del Módulo II

Ha llegado el momento de realizar la Evaluación Parcial del Módulo II.

Encontrará el documento con las consignas para su realización en el link correspondiente del campus virtual, en la fecha que haya estipulado el profesor tutor. Consulte el Cronograma de la Asignatura para ajustar su producción a los tiempos previstos.

Recuerde que esta instancia es obligatoria y, como tal, su realización y aprobación constituye un requisito para la presentación al examen final. Encontrará más detalles en la Unidad Introductoria de la Asignatura.

Cierre de la unidad

Esta unidad trabajamos sobre la problemática que hoy existe en el mundo de la informática, en pocas palabras este problema lo podemos resumir en "La apropiación de recursos o la destrucción de los mismos para fines maliciosos", causados por conocimiento o desconocimiento, ya sabemos que los recursos pueden ser de hardware o de software y dentro de los recursos de software encontramos a los archivos que son los objetos que guardan información, no hace falta decir que tan valiosa es hoy la información para una empresa y que tan costoso puede resultar ser la pérdida o su modificación.

Es por esto que hoy las empresas sienten la necesidad de invertir en protección y seguridad informática, el mercado no está ajeno a esta necesidad y hoy ofrece software, hardware y capacitación para formar expertos en seguridad.

Fin unidad 7

Anexo

Trabajo práctico sugerido

Trabajo práctico Nº 14: **Protección y Seguridad.**

Presentación

Este trabajo tiene el propósito de orientarlo/a para la comprensión de los temas desarrollados en la séptima unidad de esta asignatura.

Hasta el momento hemos estudiado el sistema operativo y los recursos del sistema de computación que el mismo administra, y hemos comprendido la importancia que tiene este trabajo para que el usuario obtenga el mejor rendimiento de su sistema, también sabemos que vivimos en un mundo muy complejo y no siempre las cosas que en el suceden son las que esperamos que sucedan, por eso hay que dotar a nuestro sistema de los mecanismos necesarios para proteger el acceso a los archivos, proteger los recursos de accesos indebidos, que pueda realizar algún proceso de un usuario mal intencionado.

Además debemos brindar la seguridad que garantice el uso del sistema por usuarios registrados, que impida los accesos a los usuarios no autorizados, para evitar de este modo la destrucción o manipulación maliciosa de los datos y códigos, también poder evitar la introducción accidental de incoherencias.

Este trabajo intenta favorecerle el acceso a las siguientes metas de aprendizaje:

- Analizar la protección en un sistema informático moderno.
- Entender como funcionan los dominios de protección y la matriz de acceso.
- Conocer los sistemas de protección basados en capacidades y en el lenguaje.

Le presentamos a continuación, las consignas de trabajo:

Consignas

1) ¿Qué entiende por protección, en el marco de la seguridad informática?
2) ¿Cuál es la diferencia entre dominios y matriz de acceso?

3) ¿Qué es un sistema de protección basado en las capacidades?
4) ¿Qué es un sistema de protección basado en el lenguaje?

Al finalizar, compare su producción con la grilla que incluimos a continuación.

Grilla de Autocorrección Nº 14: Protección y Seguridad

Orientaciones para la corrección

Recuerde que estas son solo orientaciones para que usted pueda comenzar a desarrollar el trabajo práctico.

Usted puede ampliar cualquiera de estos conceptos utilizando bibliografía adecuada, imaginación y creatividad.

1) La respuesta a este interrogante la podrá encontrar en la siguiente bibliografía.

Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección.; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007. Páginas 483 – 485.

2) La respuesta a este interrogante la podrá encontrar en la siguiente bibliografía.

Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección.; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007. Páginas 485 – 493.

3) ¿Qué es un sistema de protección basado en las capacidades?

La respuesta a este interrogante la podrá encontrar en la siguiente bibliografía.

Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección.; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007. Páginas 497 – 500.

4) La respuesta a este interrogante la podrá encontrar en la siguiente bibliografía.

Silberschatz A. Galvin P. Gagne G.; Capítulo 14 Protección.; **En su: Fundamentos de Sistemas Operativos;** 7ma Edición; España Mc Graw Hill 2007. Páginas 500 – 503.

Si surgen dudas u obstáculos que dificultan el aprendizaje o la comprensión de los contenidos durante la resolución de estas consignas, por favor, comuníquese con su tutor. Preséntele con claridad sus consultas para que él pueda brindarle las orientaciones que le permitirán resolverlas.