

PROCESO DIRECCIÓN DE FORMACIÓN PROFESIONAL INTEGRAL
FORMATO GUÍA DE APRENDIZAJE

1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- Denominación del Programa de Formación: **Análisis y Desarrollo de Sistemas de Información**
- Código del Programa de Formación: 228106 Versión 102
- Nombre del Proyecto: Software a la medida para el sector productivo de Soacha.
- Fase del Proyecto: Planeación
- Actividad de Proyecto: Determinar la estructura lógica del sistema.
- Competencia: Diseñar el sistema de acuerdo con los requisitos del cliente
- Resultados de Aprendizaje Alcanzar:

Aplicar políticas y mecanismos de control en el diseño del sistema de información, mediante el análisis de la vulnerabilidad de la información, siguiendo los parámetros establecidos por la organización.

- Duración de la Guía: 33 de trabajo directo, 17 Horas de trabajo independiente.

2. PRESENTACION

En esta actividad de aprendizaje se involucrarán al diseño lógico aspectos relacionados con los mecanismos de seguridad y control a implementar en el sistema. Se hace necesario revisar los conceptos sobre fundamentación de la seguridad informática específicamente en aspectos relacionados con la autorización, autenticación, protección de datos, cifrado, aspectos de la norma ISO 27000 y de la seguridad en las plataformas.

Como parte de esta definición de controles, deberá en sus equipos de trabajo realizar la segmentación de procesos y usuarios (perfiles, roles y procesos asociados) de acuerdo con el contexto de su proyecto formativo, así como la identificación de mecanismos de autenticación y protección sobre los datos.

3. FORMULACION DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de Reflexión inicial.

En toda actividad se hace necesario, no solo planear y ejecutar las actividades, sino efectuar procedimientos de control que vayan encaminados a asegurar que dichas actividades han sido ejecutadas de acuerdo a los parámetros que se habían establecido con anterioridad.

Es por ello, que para Evaluar la seguridad de los sistemas de información se requiere que en las diferentes fases del ciclo de vida de los sistemas de información, se planteen protocolos claros que permitan lograr un buen nivel de calidad en el software.

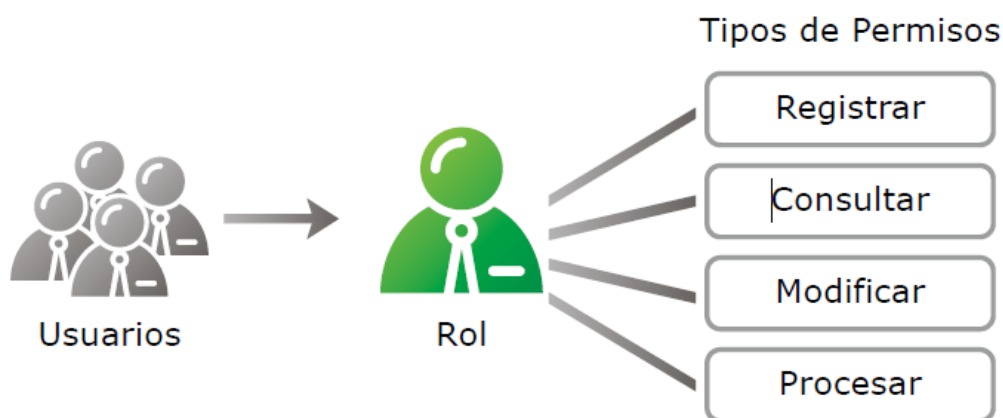
Para el diseño de estos mecanismos de seguridad y control, se debe ir de la mano de la seguridad informática, es por ello que en este tema tocaremos

varios conceptos claves de este tema tan de moda actualmente, para evitar caer en la “inseguridad informática”.

En resumen, en esta actividad de aprendizaje usted deberá:

- Fundamentarse y ampliar sus conocimientos acerca de:

* Mecanismos de Seguridad y Control.



3.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje)

Leer el compendio de los siguientes términos:

Diseño de autorización: en este ítem se deben definir los roles, permisos y privilegios de la aplicación.

Diseño de autenticación: Aquí se debe diseñar el modo en el que los usuarios se van a autenticar, contemplando aspectos tales como los mecanismos o factores de autenticación con contraseñas, tokens, certificados, etc.

También, y dependiendo del tamaño de la organización, se puede pensar en la posibilidad de integrar la autenticación con servicios externos como LDAP, Radius o Active Directory y mecanismos que tendrá la aplicación para evitar ataques de diccionario o de fuerza bruta.

Diseño de los mensajes de error y advertencia: Al diseñar estos mensajes se debe evitar que los mismos brinden demasiada información y que ésta sea utilizada por atacantes.

Diseño de los mecanismos de protección de datos: Se debe contemplar el modo en el que se protegerá la información sensible en tránsito o almacenada; según el caso, se puede definir la implementación de encriptación, hashes o truncamiento de la información

3.3 Actividades de Actividades de apropiación del conocimiento (Conceptualización y Teorización).

1. FUNDAMENTOS DE SEGURIDAD

Para definir estos dos términos se debe precisar que actualmente la permanencia y disponibilidad de los recursos en el planeta depende del aprovechamiento, manejo y conservación sostenible que se haga de ellos.

Para hablar de seguridad en las tecnologías de la información, se deben tener en cuenta TRES PILARES fundamentales sobre el manejo de los datos y la prestación de los servicios, los cuales se pueden relacionar con la sigla C.I.A.

- **Confidentiality (Confidencialidad):** Indica que la información solo es revelada a usuarios autorizados en tiempos precisos, es decir SOLO en horarios asignados.

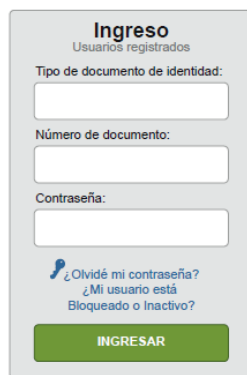
- **Integrity (Integridad):** Se refiere a la modificación de la información, para ello se debe identificar muy bien los roles de los usuarios y así definir los niveles de acceso para la manipulación de los datos.

Availability (Disponibilidad): Se refiere a la disponibilidad de la información. Para este proceso, desde el área técnica, se deben establecer medidas de seguridad, cuyo objetivo fundamental es reducir cualquier riesgo asociado, algunas de estas medidas de seguridad pueden ser:

- Identificación y autenticación de usuarios.
- Control de flujo de información.
- Confidencialidad.
- Integridad.
- No Autorización.

Estas medidas de seguridad se ponen en práctica mediante mecanismos de protección como:

- **Autenticación:** Este término se refiere a la verificación que se realiza a la identidad del usuario; este proceso generalmente se lleva a cabo cuando se ingresa al sistema, a la red o a cualquier base de datos.



Normalmente para ingresar a cualquier sistema informático se utiliza un nombre de usuario y una contraseña, aunque actualmente se están utilizando técnicas más seguras, como una tarjeta magnética, o por huellas digitales, la utilización de más de un método a la vez disminuye el riesgo de ataques a la seguridad de la información.

Al momento de construir la contraseña de autenticación del sistema tenga en cuenta las siguientes recomendaciones:

- **Característica de la contraseña:** Este aspecto se refiere al tamaño en caracteres de la misma; en la medida que la contraseña contenga un tamaño grande en caracteres y ésta sea compleja (conjunto de caracteres variado, con minúsculas, mayúsculas y números) menor será la posibilidad de ser adivinada y más difícil será burlar esta técnica.

- **Confidencialidad:** La contraseña solo la debe manejar el usuario, no puede ser conocida por nadie más. Un error muy común, es que los usuarios se prestan las contraseñas o que las escriben en un papel y éste lo dejan pegado en el escritorio, lo que permite que cualquier otro usuario conozca la contraseña, comprometiendo a la empresa y al propio dueño.

Un problema muy común entre los usuarios, es que difícilmente recuerdan contraseñas tan elaboradas. También es muy común que se utilicen palabras muy obvias como el nombre, el apellido, el nombre de usuario, el grupo musical preferido, la fecha de nacimiento, etc., que facilitan la tarea a quién quiere ingresar al sistema sin autorización.

En la actualidad existe una preocupación especial por la conservación y el logro de un desarrollo sostenible pero aun se requiere no solo de un nivel de conciencia e información, sino de acciones puntuales y claras que apunten a resolver los problemas de deterioro ambiental que cada vez son mas graves y ponen en riesgo el equilibrio y la estabilidad de todos en el planeta.

- **Control de Acceso:** Todos los sistemas que no sean de libre acceso deberán contar con control de acceso basado en roles. La autorización deberá realizarse sobre el mismo sujeto que se autentica o también podrá requerirse mayor información que permita obtener la autorización con granularidad más fina, lo que implica que se adquieren muchos recursos para administrar el bloqueo, pero se asegura la consistencia de los datos

Desarrollar la siguiente actividad:

- De acuerdo con el contexto de su proyecto de formación y tomando como referencia el material suministrado y las plantillas de especificación de requerimientos y análisis del sistema, elabore junto

con su equipo de trabajo un informe escrito en un archivo donde se describan los siguientes elementos:

- **Segmentación de procesos, perfiles y roles.**
- **Mecanismo de autenticación a implementar en el sistema**
- **Cifrado de datos: tipo de algoritmos a implementar.**
- **Procedimientos adicionales de Seguridad a implementar**
- El documento debe ser elaborado con normas Icontec vigentes para trabajos escritos, además de buenas prácticas de redacción y ortografía.

3.4 Actividades de transferencia.

- Controlar la seguridad del Sistema de Información pro, Mediante Métodos, Formularios, Claves de Acceso que permitan restringir el ingreso al software. Inicio de sesion (Acceso al Sistema)

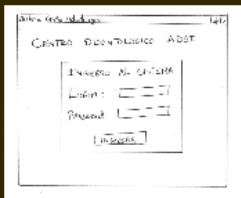

Caso de Uso: Autenticar Usuario

Sistema: Gestión Odontológica

Caso de Uso	Autenticar usuario								
Descripción	El comportamiento del Sistema debe validar el usuario que ingresa al sistema.								
Precondición	El personal debe estar registrado en el sistema para que al ingresar sus datos de login y password puedan ser validados.								
Secuencia Normal	<table border="1"> <thead> <tr> <th>Paso</th> <th>Acción</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>El personal médico al ingresar al sistema debe ingresar con un login y password asignados por el administrador.</td> </tr> <tr> <td>2</td> <td>El sistema valida el login y password.</td> </tr> <tr> <td>3</td> <td>Si los datos son validos, el sistema muestra las opciones correspondientes, dependiendo del tipo de usuario.</td> </tr> </tbody> </table>	Paso	Acción	1	El personal médico al ingresar al sistema debe ingresar con un login y password asignados por el administrador.	2	El sistema valida el login y password.	3	Si los datos son validos, el sistema muestra las opciones correspondientes, dependiendo del tipo de usuario.
Paso	Acción								
1	El personal médico al ingresar al sistema debe ingresar con un login y password asignados por el administrador.								
2	El sistema valida el login y password.								
3	Si los datos son validos, el sistema muestra las opciones correspondientes, dependiendo del tipo de usuario.								
Pos condición	El empleado ingresa al sistema.								
Excepciones	<table border="1"> <thead> <tr> <th>Paso</th> <th>Acción</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>Si los datos de login y password no son validos, el sistema informa al personal médico para que se revise y actualice la información.</td> </tr> <tr> <td>3</td> <td>Si el login y password no son validos el sistema no permite ingresar.</td> </tr> </tbody> </table>	Paso	Acción	3	Si los datos de login y password no son validos, el sistema informa al personal médico para que se revise y actualice la información.	3	Si el login y password no son validos el sistema no permite ingresar.		
Paso	Acción								
3	Si los datos de login y password no son validos, el sistema informa al personal médico para que se revise y actualice la información.								
3	Si el login y password no son validos el sistema no permite ingresar.								

Pasos para realizar la interfaz de Usuario mediante prototipos:

1. Creamos un prototipo en una hoja de papel.
2. Ahora procedemos a realizarlo utilizando una herramienta software. Para ello vamos a utilizar Balsamiq Mockups. En el Documento de apoyo llamado Crear Interfaces Balsamiq se muestra el paso a paso de la creación de la siguiente Interfaz.

Ambiente Requerido

Ambiente de Informática con 20 computadores, Acceso a Internet para los estudiantes y el instructor

ACTIVIDADES DEL PROYECTO	DURACIÓN (Horas)	Materiales de formación devolutivos: (Equipos/Herramientas)		Materiales de formación (consumibles)		Talento Humano (Instructores)		AMBIENTES DE APRENDIZAJE TIPIFICADOS
		Descripción	Cantidad	Descripción	Cantidad	Especialidad	Cantidad	ESCENARIO (Aula, Laboratorio, taller, unidad productiva) y elementos y condiciones de seguridad industrial, salud ocupacional y medio ambiente
Determinar la estructura lógica del sistema.	35 horas	videobeam Computador	1 1 1	- Fotocopias - Guías, material general de formación y talleres. - Marcadores borrables, - borrador de tablero acrílico	1 1 1	Ingeniero de Sistemas	1	Ambiente de formación Con 20 computadores, Acceso a Internet para los estudiantes y el instructor

4. ACTIVIDADES DE EVALUACIÓN

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento : Taller escrito crucigrama_diseñoInterfazUsuario.pdf	<ul style="list-style-type: none"> Trabajo en el Ambiente de Formación: Taller de Conocimientos <ul style="list-style-type: none"> de registros de novedades. 	Taller resuelto siguiendo los criterios de evaluación Lista de chequeo
Evidencias de Desempeño Desempeño durante el desarrollo de la evidencia	<ul style="list-style-type: none"> Diseña y Aplica archivos gráficos para construir la interfaz de un Sistema de Información. Observación del Orientador durante las actividades realizadas 	Desarrollo de taller utilizando las herramientas propuestas
Evidencias de Producto: Informe escrito con los conceptos Formularios para inicio de sesión según ejemplo propuesto Formulario de inicio de sesión a su proyecto asignado	<ul style="list-style-type: none"> Prototipo del Sistema de Información y la DB Informe de diseño. 	Documento que contenga la carpeta con los archivos solicitados, formato PDF y será subido a la plataforma Blackboard

5. GLOSARIO DE TERMINOS

El aprendiz determinará el glosario a partir de la consulta del significado de:

Autenticación: verificación que se realiza a la identidad del usuario.

Availability: Disponibilidad.

Confidentiality: Confidencialidad.

Directorio activo: Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Encriptación: Es un proceso para convertir la información a un formato más seguro. En otras palabras, los datos que están en un formato claro, o sea entendible, se convierten mediante un proceso matemático a un formato encriptado o codificado, o sea ininteligible. Una vez que llegan a su destino, se decodifican para poder ser legibles de nuevo, se desencriptan.

Firma digital: Proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos.

Granularidad fina: Implica que se adquieren muchos recursos para administrar el bloqueo, pero se asegura la consistencia de los datos.

Hashes: Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que sólo puede volverse a crear con esos mismos datos).

Integrity: Integridad.

Servidor: ordenador o programa que da servicios a otro conocido como cliente. En un sistema de hipertexto, un servidor dará información al navegador.

SMTP: Simple Mail Transfer Protocol. Protocolo de envío de correo electrónico.

TCP: Transmission Control Protocol. El protocolo de transporte de datos más popular en Internet.

Windows: sistema operativo desarrollado por Microsoft y basado en ventanas. Es el más popular en entornos PC. Permite el acceso a Internet mediante TCP/IP.

6. REFERENTES BIBLIOGRAFICOS

Evaluación de la Seguridad de los Sistemas Informáticos. Consultada el

2 de julio de 2013, disponible en

<http://www.slideshare.net/vidalcruz/evaluacion-de-la-seguridad-de-lossistemas-informaticos>

Introducción a la Seguridad Informática. Consultada el 15 de julio de

2013,

Disponible en

<http://recursostic.educacion.es/observatorio/web/es/software/softwaregeneral/1040-introduccion-a-la-seguridad-informatica?>

Seguridad de la Información. Consultada el 16 de julio de 2013,

disponible en

<http://csrc.nist.gov/publications/PubsSPs.html>

Villalon Huerta, Antonio (2007). Seguridad de los sistemas de información, consultada en julio de 2013

Gutierrez, Pedro (2013). ¿Qué son y para qué sirven los hash?:

funciones de resumen y firmas digitales, consultado en julio de 2013,

disponible en:

<http://www.genbetadev.com/seguridad-informatica/que-son-y-para-que>

-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

Aeris (2008), Encriptación. Consultado en julio de 2013 y disponible en

<http://www.aeris.cc/aeris/cfm/ayuda.cfm?Id=Aeris-5-2-2&Tipo=child&P>

adre=Aeris-5-2

Es.Wikipedia.org Kendall & Kendall. Análisis y Diseño de Sistemas. Sexta edición; México, Pearson Educación, 2005.

Piattini, Mario y otros. Análisis y diseño detallado de Aplicaciones informáticas de Gestión. México, Alfaomega Grupo Editor, 2005.

Escuela Superior de Informática de Ciudad Real. (8 de Febrero de 2008). Itescam. Recuperado el 4 de Julio de 2013, de <http://www.itscam.edu.mx/principal/sylabus/fpdb/recursos/r88166.PDF> En A. S. Henry F. Korth, Fundamentos de Bases de Datos. McGraw-Hill (2006). Sánchez, J. (2004).

Principios sobre bases de datos. Obtenido de: <http://www.jorgesanchez.net/bd/bdrelacional.pdf> Este documento está disponible desde las bibliotecas SENA en: <http://site.ebrary.com/lib/senavirtualsp/docDetail.action?docID=10536104&p00=uml>

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	NAIRO HERNANDEZ	INSTRUCTOR	TIC	15 de marzo 2017

8. CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)

Nombre	Cargo	Dependencia	Fecha	Razón del Cambio



Autor (es)	Cesar Augusto Moreno	INSTRUCTOR	TIC	18 de Marzo de 2020	Actualizacion
-------------------	-----------------------------	-------------------	------------	---------------------------	----------------------