UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

INGENIERÍA EN COMPUTACIÓN

Experiencia profesional en el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán.

Sustentante:

Solano Luna Nicolás.

Opción de titulación:

Informe del ejercicio profesional.

Asesor:

Ing. Antonia Navarro González.

San Juan de Aragón, México. 2009

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS.

A mis padres:

Nicolás Solano Vázquez y Guadalupe Luna Jiménez.

Por su apoyo incondicional, su ejemplo, su amor y sus consejos.

A mis hermanos:

Darío, Guadalupe, Luis y Héctor.

Por su amistad y apoyo desinteresado.

A mis sobrinos:

Oscar Alberto, Alejandro y Gabriela.

Por traer alegría y deseos de superación y colaboración a mi familia.

A mis amigos:

Mayra, Silvina, Héctor, Oscar, Francisco, Ivan, los Ramones y los Carlos, Victor, Axel y muchos otros.

Por compartir buenos momentos conmigo.

A la UNAM:

Por permitirme el acceso a una educación de calidad y por hacerme un profesionista con principios y valores.

Experiencia profesional en el Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán.

Tabla de contenido

Introducción.

Después de salir de la escuela, he laborado en diversos lugares, pero de todos ellos, el que más satisfacciones me ha dado es el actual ya que por el horario me permite seguir estudiando, además, el ambiente laboral en el Departamento de Radiología e Imagen es muy tranquilo ya que muchos de sus integrantes son jóvenes que están estudiando la especialidad de radiología.

El presente documento de realizó a partir de las experiencias que he tenido en el Instituto Nacional de Ciencias Médicas y Nutrición “Salvador Zubirán”, en el primer capítulo pretendo que el lector conozca más acerca de la Institución para la cual laboro y comprenda que una parte muy importante es la investigación y el desarrollo de recursos humanos.

El segundo y tercer capítulo trata sobre las experiencias obtenidas durante mi paso por la Subdirección de Informática.

En el cuarto capítulo se encuentra lo relacionado a las funciones que realizo en la actualidad dentro del Departamento de Radiología e Imagen.

En el último capítulo, el quinto, se encuentran las actividades adicionales que han sido de gran importancia para mi desarrollo laboral.

Finalmente en la Conclusiones, trato de resumir mi experiencia laboral vivida en el Instituto y de presentar mis planes a futuro.

Capítulo I. El Instituto Nacional de Ciencias Médicas y Nutrición “Salvador Zubirán”.

Actualmente laboro en el Instituto Nacional de Ciencias Médicas y Nutrición “Salvador Zubirán” (INCMNSZ) en el Departamento de Radiología e Imagen. Previamente laboré de enero de 2004 a junio de 2005 en la Subdirección de Informática, también del INCMNSZ.

A continuación presento las funciones y objetivos del INCMNSZ, así como de los departamentos en los que he laborado.

1.1. Presentación de INCMNSZ.

El Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán (INCMNSZ, INNSZ) es uno de los Institutos Nacionales de Salud dependientes de la Secretaría de Salud. Es una de las instituciones médicas de mayor prestigio asistencial y científico de México.

Se inauguró el 12 de octubre de 1946 con el nombre de Hospital de Enfermedades de la Nutrición. En el año de 1981 se le otorga la denominación de Instituto Nacional de la Nutrición Salvador Zubirán y ese mismo año se incrementa la capacidad de camas hospitalarias para poder otorgar atención medica de tercer nivel. El día 26 de mayo de 2000 se registra el nuevo nombre del Instituto, el cual lleva hasta la fecha.

Desde sus inicios, el Instituto se planeó como una institución médica modelo en que las actividades asistenciales sirvieran como sustento de las educativas y de investigación, pensando que sólo se puede dar buena asistencia en un ambiente académico que propicie la enseñanza e investigación científica.

1.2. Actividades del INCMNSZ.

Es una institución nacional de salud que realiza investigación, docencia y asistencia de alta calidad.

Desde el punto de vista asistencial, se dispone de 167 camas para internación de enfermos y una amplia consulta externa que da servicio a 135,000 pacientes al año con un promedio de 215,000 consultas anuales. Se atienden pacientes con una gran gama de padecimientos y se dispone del equipo de laboratorio y gabinete más moderno como auxiliares diagnósticos.

Su personal médico es de 176 especialistas, todos con varios años de entrenamiento en el país o en el extranjero. Son la Dirección de Medicina y la Dirección de Cirugía quienes tienen a su cargo la actividad asistencial en la institución.

El Instituto, a través de su Dirección de Enseñanza, ofrece en la actualidad 20 cursos de posgrado avalados por la Universidad Nacional Autónoma de México, en que se forman especialistas en distintos campos de la medicina y cirugía.

Su desempeño frente a las sociedades científicas es también muy destacado. Es la institución médica con mayor número de investigadores y con mayor producción científica en el país, siendo también la de mayor índice de impacto. Esta actividad está coordinada por la Dirección de Investigación de la que dependen los departamentos de investigación básica y de investigación médica.

El Instituto tiene los siguientes objetivos:

- Formar recursos humanos en sus áreas de especialización, así como en aquellas que les sean afines.

- Realizar estudios e investigaciones clínicas, epidemiológicas, experimentales, de desarrollos tecnológicos y básicos, en las áreas biomédicas y socio médicas en el campo de sus especialidades, para la comprensión, prevención, diagnóstico y tratamiento de las enfermedades y rehabilitación de los afectados, así como para promover medidas de salud.

- Publicar los resultados de las investigaciones y trabajos que realice, así como difundir información técnica y científica sobre los avances que en materia de salud registre.

- Promover y realizar reuniones de intercambio científico, de carácter nacional e internacional, y celebrar convenios de coordinación, intercambio o cooperación con institutos afines.

- Formular y ejecutar programas de estudio y cursos de capacitación, enseñanza, especialización y actualización de personal profesional, técnico y auxiliar, en sus áreas de especialización y afines así como evaluar y reconocer el aprendizaje.

- Otorgar constancias, diplomas, reconocimientos y certificados de estudios, grados y títulos, en su caso, de conformidad con las disposiciones aplicables.

- Prestar servicios de salud en aspectos preventivos, médicos, quirúrgicos y de rehabilitación en sus áreas de especialización.

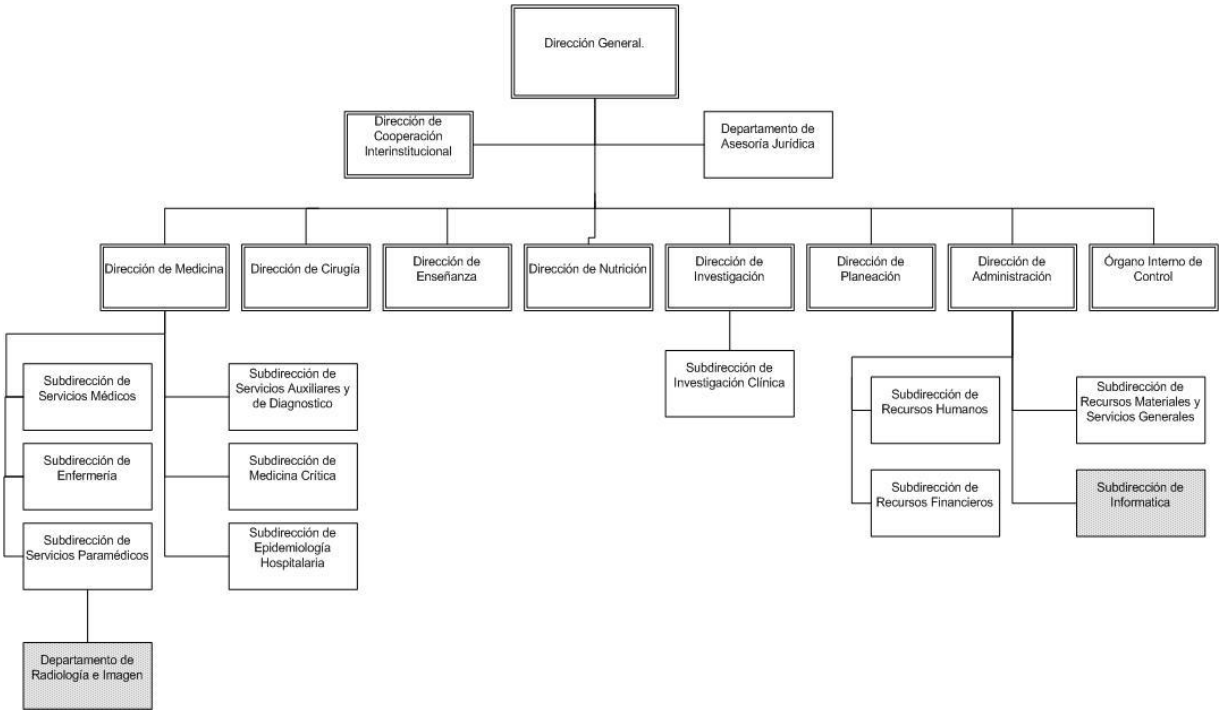
- Promover acciones para la protección de la salud, en lo relativo a los padecimientos propios de sus especialidades.
- Proporcionar consulta externa, atención hospitalaria y servicio de urgencias a la población que requiera atención medica en sus áreas de especialización, hasta el límite de su capacidad instalada.

- Actuar como órgano de consulta, técnica y normativa, de las dependencias y entidades de la Administración Pública Federal en sus áreas de especialización, así como prestar consultorías a título oneroso a personas de derecho privado; asesorar a los centros especializados de investigación, enseñanza o atención médica de las entidades federativas y, en general, a cualquiera de sus instituciones públicas de salud.

- Asesorar a los centros especializados de investigación, enseñanza o atención médica de las entidades federativas y, en general, a cualquiera de sus instituciones públicas de salud.

- Asesorar y formular opiniones a la Secretaría cuando sea requerido para ello.

- Coadyuvar con la Secretaría a la actualización de los datos sobre la situación sanitaria general del país respecto de las especialidades médicas que les corresponda.



1.3. Función de la Subdirección de Informática dentro del INCMNSZ.

La Subdirección de Informática depende de la Dirección de Administración.
Sus funciones son:

- Coordinar, supervisar y evaluar las actividades relacionadas con las áreas de Informática Medica, desarrollo y mantenimiento de sistemas y de informática en investigación para promover su adecuado funcionamiento.
- Implementar los sistemas informáticos de acuerdo a las necesidades de las diferentes áreas del Instituto.
- Establecer las medidas de seguridad informática.
- Mantener el funcionamiento de los sistemas informáticos a su cargo.
- Proporcionar cursos y asesorías al personal que labora en el Instituto.
- Asesorar a las áreas del Instituto en el proceso de adquisición de equipos de cómputo.

1.4. Función del Departamento de Radiología e Imagen dentro del INCMNSZ.

El Departamento de Radiología e Imagen depende de la Subdirección de Servicios Paramédicos y de la Dirección de Medicina

El departamento de Radiología e Imagen tiene como objetivos:

“Proporcionar servicios de apoyo diagnóstico, en estudios simples, contrastados y en estudios de alta tecnología a pacientes ambulatorios y pacientes hospitalizados, así como brindar apoyo a programas de investigación y enseñanza de las diferentes áreas del Instituto.”

Entre sus funciones se encuentran:

- Prever, organizar, dirigir y supervisar los estudios radiológicos y de imagen que se generen, a fin de satisfacer las necesidades de servicio para el adecuado diagnóstico de los pacientes usuarios.
- Diseñar planes y programas de estudios que contribuyan en la formación académica de médicos residentes.
- Participar en proyectos de investigación y difundir la información científica obtenida acerca de los avances en la especialidad de radiología.
- Organizar, dirigir y controlar las actividades necesarias para el mejor funcionamiento del departamento.
- Establecer sistemas de control que permitan el adecuado abastecimiento de materiales químicos y radiográficos, a fin de contar con el suministro necesario y satisfacer la demanda de estudios de manera oportuna.
- Prever la adquisición de tecnología que permita mantener a la vanguardia en Imagenología.
- Apoyar la actualización y capacitación de todo el personal técnico y de apoyo para asegurar la calidad del servicio.
- Vigilar el cumplimiento de la normatividad relativa a seguridad radiológica.

Cabe señalar que una de las prioridades para el Instituto es la Investigación y ha ganado muchos premios a nivel nacional e internacional, como un beneficio adicional a estas investigaciones, se forma personal altamente capacitado, el cual después al llegar a otros lugares, continua con sus investigaciones.

Además, en el Departamento de Radiología e Imagen se proporciona el mejor servicio posible a los pacientes, los cuales son en su mayoría, personas con bajo nivel socio-económico que vive en provincia y en otros casos, pacientes de otros hospitales que no tienen la infraestructura con la que cuenta el Instituto.

Capítulo II. Administración de los servidores HIS.

Actualmente el INCMNSZ cuenta con un Sistema de Información Hospitalaria (HIS por sus siglas en inglés) que se compone de dos sistemas, uno llamado SIPAM (Sistema de Paciente Ambulatorio) y otro llamado ADMINISTRATIVO.

Estos sistemas fueron desarrollados por una empresa de desarrollo de software. Dicha empresa fue contratada para el desarrollo e implementación de un Sistema de Información Hospitalaria para el Instituto el cual incluía:

- La elección de los servidores.
- La elección e instalación del sistema operativo.
- La elección del lenguaje de programación.
- La elección del manejador de base de datos.
- El desarrollo de los módulos principales del SIPAM y ADMINISTRATIVO.
- El mantenimiento de los módulos.
- El diseño y el mantenimiento de las bases de datos de los sistemas.
- Capacitación de personal del Instituto en la administración y el mantenimiento a módulos.
- Capacitación a personal del Instituto en la creación de nuevos módulos.
- La documentación del diseño, desarrollo e implementación del sistema así como manuales de usuario.

Dicha empresa decidió usar lo siguiente para la implementación de HIS.

- Servidores HP 9000.
- Sistema operativo HP-UX.
- Lenguaje de programación C y 4gl.
- Manejador de bases de datos INGRES.

Sin embargo dicha empresa se retrasó por mucho tiempo y no terminó los módulos. Al final el Instituto contrato personal de la empresa que en conjunto con los programadores terminaron los módulos de los sistemas, sin embargo los sistemas nunca quedaron como fueron diseñados, ya que los programadores empezaron a agregar cosas a sus módulos sin ninguna metodología ni un plan integral que abarcara los demás módulos.

Existió además negligencia por parte de algunos de los empleados del Instituto, ya que permitieron la liberación de la empresa sin que ésta entregara el código fuente de muchas bibliotecas de código así como manuales de administración, de operación y de la estructura de la base de datos.

El sistema SIPAM tiene entre sus funciones:

Funciones del sistema SIPAM.	
El manejo del expediente clínico.	Almacenamiento, actualización, impresión en papel, acceso mediante las terminales tontas del sistema o las computadoras que se encuentran en los consultorios y departamentos del Instituto.
Resultados y diagnósticos de estudios.	Almacena y presenta los resultados obtenidos en los laboratorios de toma de muestras y central, así como de las cirugías realizadas. Presenta también los diagnósticos de los estudios realizados en departamentos como Radiología e Imagen, Patología, Infectología, etc. Dichas consultas se pueden realizar empleando filtros para que la búsqueda sea más rápida.
Programación de intervenciones quirúrgicas.	Mantiene y actualiza el rol del personal médico y de enfermería que realizara las intervenciones así como el agendamiento de intervenciones.
Administración de citas de pacientes.	Mantiene y actualiza el agendamiento de citas de la mayoría de los departamentos como son toma de muestras, consulta externa, geriatría, neurología, dermatología, etc. Control para evitar empalmes de citas e impresión de itinerario a los pacientes.
Control de camas en el área de hospitalización.	Mantiene un control sobre el uso de camas en terapia intensiva, hospitalización, urgencias, terapia intermedia. La información recabada se emplea para la generación de estadísticas y cobro a pacientes.
Administración de las notas medicas de evolución.	Almacenamiento y actualización de las notas médicas de evolución de pacientes hospitalizados, dichos reportes son realizados en los sectores médicos que se encargan de un conjunto de camas, y después se transcriben en Archivo Clínico.
Impresión de etiquetas con códigos de barras.	Dichas etiquetas contienen el número de registro del paciente, nombre del paciente y condigo de barras con el identificador del paciente, dichas etiquetas se emplean para la generación de solicitudes de estudios en los diferentes departamentos.
Impresión de los diagnósticos y resultados de estudios.	Debido a que la legislación actual requiere de un documento físico, se imprimen los resultados contenidos en el sistema.

El servidor de Administración contiene toda la información administrativa de los pacientes, trabajadores y de las finanzas del Instituto.

Entre sus funciones se encuentran:

Funciones del Sistema ADMINISTRATIVO.	
Administra la información del paciente.	Almacena y actualiza la información demográfica de los pacientes como son el domicilio, número telefónico, fecha y lugar de nacimiento, lugar de residencia y religión, entre otras. Dicha información solo se emplea para la realización de estadísticas y para investigaciones médicas. También se les asigna un nivel socioeconómico.
Información fiscal del Instituto.	Información relacionada a las finanzas del Instituto como son: cuentas por pagar, cuentas por cobrar, facturas a proveedores, etc.
Administración de los almacenes.	Controla los movimientos de entrada y salida de los almacenes de ropa, víveres y general. Además guarda la información de existencias de artículos en cada almacén, claves de artículos, precios, fechas de entrega y generación de pedidos a almacenes por áreas usuarias.
Cobro a pacientes.	Realiza la contabilidad del costo a pagar por el paciente generado a partir de los estudios realizados, días en cama, medicamentos y material usado durante su estancia, etc. Dicho costo está relacionado al nivel socioeconómico del paciente y dependiendo de este se aplica un subsidio.
Administración de la farmacia del Instituto	Controla los artículos de la farmacia así como la generación y surtido de recetas.

Debido a que prevalecía un descontrol en los sistemas informáticos del Instituto y que existían muchas quejas por parte de los usuarios de los sistemas, se contrató a una empresa para el análisis de la situación informática, dicho análisis concluyó que muchos de los problemas con los sistemas de información eran debidos a una mala administración.

El análisis de la situación informática comenzó el mes de octubre de 2003 y terminó en diciembre de 2003, entregando al final un reporte con las fallas más importantes así como una propuesta para la solución o mitigación de los problemas.

Del análisis derivó la decisión por parte de las autoridades del Instituto de destituir al titular de la Subdirección de Informática y al jefe del Departamento de Desarrollo y Mantenimiento de Sistemas.

Después de formar parte en el equipo que realizó el análisis, el 15 de enero de 2004 ingresé al Instituto como trabajador por honorarios.

Los problemas críticos encontrados en el análisis de los sistemas eran:

- Errores administrativos de parte del subdirector y jefes de departamento.
- Infraestructura de red obsoleta.
- Inexistencia de procedimientos y políticas.
- Deficiencias en la instalación y administración de los sistemas operativos en los servidores.
- Mala administración del manejador de bases de datos.
- Un descontento generalizado del personal de la Subdirección de Informática.
- Capacitación deficiente de los operadores de los sistemas HIS.

A continuación se explican algunos problemas con mayor detalle además de la solución o acciones aplicadas para mitigar dichos problemas.

- Debido a que los sistemas SIPAM y Administrativo comparten información, las bases de datos de los dos servidores deben estar en comunicación permanentemente ya que depende una de la otra. Esto significa que en caso de que algún servidor deje de operar correctamente, el otro servidor no deberá de continuar operando hasta que se restablezca el servidor con problemas, toda vez que, en caso de que continúe un solo servidor, se corre el riesgo de que la información tenga inconsistencias.

    - Desafortunadamente este problema no puede ser solucionado en su totalidad ya que es un comportamiento inherente de los sistemas debido a su programación. Como acción para mitigar el riesgo de inconsistencia de información, se instaló el sistema de monitoreo de sistemas, el servidor de respaldo y la capacitación del personal.

- La comunicación de los usuarios con los sistemas era mediante terminales tontas, las cuales se conectaban a los servidores mediante el uso de dispositivos

DTC (Data communications and Terminal Controllers), Dichos equipos eran obsoletos ya no existían refacciones, además, la velocidad de transmisión de información era sumamente lenta.

- Se propuso su sustitución por switches, o en el peor caso, por hubs. Además se recomendó una segmentación de la red institucional en subredes. Lo anterior implicaba necesariamente el cambio de terminales tontas por computadoras conectadas a la red e instalación de nuevos nodos de red y por ende una inversión fuerte en infraestructura de redes y equipo de cómputo.

❖ Las terminales tontas se trababan regularmente y no podían continuar hasta que se reseteara el puerto en el DTC. Existía además el problema de que no estaban rotulados los puertos por lo que los operadores reseteaban todo el DTC. Al resetear el DTC muchas sesiones se terminaban de manera anormal, dando como resultado problemas con la información.

- Se generaron rótulos con el número de puerto y se pegaron en los cables y en las terminales tontas, se les pedía a los usuarios que les dieran el número de puerto a los operadores para que resetearan su terminal.

❖ Las terminales tontas se descomponían con mucha frecuencia debido a su antigüedad y no existían refacciones o eran excesivamente caras. No existía además soporte por parte del fabricante.

- De las terminales que se sustituyeron por PCs, se seleccionaron las mejores y se sustituyeron por otras localizadas en otras áreas del Instituto. Algunas terminales se conservaron para refacciones. Lo mismo ocurrió con los teclados, los cuales debido a que eran escasos, los vendían al Instituto hasta en $2,000.00 MN cada uno.

2.1 Implementación de Buenas Prácticas en administración de sistemas.

En la administración de los servidores se observó que existían muchos problemas causados por la ausencia de políticas y procedimientos, para su mejor entendimiento serán agrupados por temas.

Cuentas de usuario.

- Existían cuentas "públicas" en los sistemas (SIPAM y ADMINISTRATIVO) que eran usadas por departamentos enteros.
- La cuenta de superusuario (root) de los sistemas eran usadas por los operadores para la operación diaria.
- No existía una política de caducidad de contraseñas y las contraseñas eran débiles.
- No existían políticas de creación y deshabilitación de cuentas cuando llegaba o se retiraba personal del Instituto.

En una prueba realizada con herramientas de seguridad (John the Ripper) se obtuvieron más del 70% de las contraseñas en menos de una hora, la gran mayoría de las contraseñas eran iguales a los nombres del usuario del sistema.

Como parte de las acciones para corregir estos problemas se redujo al mínimo el uso de cuentas públicas.

Las cuentas sensibles, como la cuenta del departamento de finanzas, se modificaron y se asignaron cuentas personales a cada usuario. Se les recomendó el uso de contraseñas fuertes mediante el uso de mayúsculas, minúsculas, números y caracteres especiales, además de la recomendación de contraseñas con más de 6 caracteres de longitud. Desafortunadamente la versión del sistema operativo no permite contraseñas mayores de 8 caracteres, en caso de elegir una contraseña de longitud mayor, el sistema la trunca a 8 caracteres.

El archivo de /etc/passwd contiene la representación de la contraseña de los usuarios y puede ser vista por todos, sin embargo, aunque el sistema tenía la capacidad de ofrecer el uso del archivo /etc/shadow, ésta no fue habilitada desde la instalación del sistema operativo.

Se cambiaron las contraseñas de la mayoría de los departamentos.

Se les restringió la contraseña de superusuario a los operadores y se generaron cuentas individuales.

Se le recomendó al Jefe del departamento de Informática Médica que generara políticas de uso de cuentas de usuario en el servidor y las hiciera del conocimiento de cada usuario. Se le entregó además un documento con recomendaciones del manejo de contraseñas y de cuentas de usuarios.

Administración de sistemas de archivos y de aplicaciones en los servidores.

- Existían cuentas de usuario que tenían acceso al shell del sistema operativo teniendo como directorio home el directorio raíz del sistema.
- Prevalecía una mala administración de los permisos a directorios y archivos.
- Cambio de permisos a directorios y ejecutables del sistema operativo así como de aplicaciones de la base de datos.
- Los operadores usaban los servidores como repositorio de documentos.
- No se depuraban los archivos core.

La mala administración de los directorios y archivos era un problema delicado debido a que para “facilitar” la administración, el jefe de departamento asignó permisos de lectura, escritura y ejecución al propietario, grupo y demás usuarios del sistema (permisos 0777 en UNIX) a directorios completos, algunos compartidos por otras cuentas o usados por los sistemas SIPAM y Administrativo . Esto daba la posibilidad de que cualquier usuario con acceso a estos directorios borrara o modificara la información, afectando así a demás usuarios y áreas del Instituto.

Para la mitigación del problema se crearon scripts de inicio de sesión a las cuentas de usuario los cuales ingresaban a la aplicación de forma automática y se salían del sistema al cerrar la aplicación. Se cambiaron los permisos a directorios de los sistemas y de la aplicación. Desafortunadamente no se pudo solucionar completamente este problema debido a que los sistemas estaban programados empleando la compartición de directorios entre varias cuentas y módulos.

Se les instaló una computadora a los operadores para sus documentos y para el monitoreo de los servidores.

Se borraron los archivos core del sistema, algunos tenían varios años de antigüedad.

Bitácoras de operación y del sistema.

- No existían bitácoras de operación adecuadas, los operadores no anotaban correctamente los eventos sucedidos durante su turno.
- Las bitácoras del sistema no se respaldaban.
- Las bitácoras del sistema no se revisaban.

En caso de algún problema suscitado durante el turno nocturno, se tenía que llamar al operador a su casa para que explicara el suceso ya que no dejaba nada apuntado y el operador del siguiente turno decía desconocer totalmente el problema.

Se generó una plantilla de llenado de bitácoras integrada por campos obligatorios como fecha, hora, incidentes, comentarios, operador en turno, etc.
Tiempo después se implementó un sistema para el manejo de bitácoras con los mismos campos, el cual estaba alojado en una computadora con Sistema Operativo Linux. Dicho sistema fue programado en su totalidad por los operadores.
Se les enseñó a los operadores la forma de analizar las bitácoras del sistema en búsqueda de errores y se les solicitó que respaldaran las bitácoras del sistema.

Administración de redes.

- Mala administración de las direcciones IP asignadas.
- No existían políticas de uso de la red de datos.
- La red no estaba segmentada.
- El conocimiento en redes de los operadores era deficiente.
- No existían controles de acceso adicionales a los servidores, además, no se monitoreaba la red.

La administración de las direcciones IP se llevaba a cabo usando el archivo /etc/hosts de los servidores, en los cuales se agregaba cada dirección como un comentario y con la información incompleta. Se le solicito al jefe de departamento que cambiara de método de control de direcciones IP y que lo realizara en otro equipo diferente a los servidores, además se le recomendó que mejorara la lista agregándole campos como dirección física de la tarjeta de red (MAC), usuario responsable, departamento y extensión del usuario.

Se le pidió al Jefe de Informática Médica que entregara al usuario un documento de asignación de dirección IP y de uso de la red institucional en donde se especificaran las políticas de la red.

Se instaló un sistema de monitoreo de red. Y se escaneó la red periódicamente en busca de problemas de red generados por virus.

Control de desarrollo y modificación de software.

- Los programadores aplicaban sus actualizaciones directamente en el servidor en producción.
- No se llevaba un control de versiones.
- No existía un procedimiento formal para la solicitud de modificación de módulos.
- Los programadores podían crear bases de datos y tablas para pruebas.

Ya que no existía un servidor de desarrollo en donde se pudieran probar los nuevos módulos o las actualizaciones de las aplicaciones existentes, se le recomendó al jefe de Desarrollo y Mantenimiento de Sistemas la creación de un servidor para pruebas. Dicho servidor se instaló y configuró generando un ambiente parecido al de los servidores de producción. Se crearon cuentas de usuario a cada programador. Dicho servidor era un equipo que ya no estaba en producción pero que era de la misma arquitectura. (RISC HP).

Se le comentó al Subdirector la inexistencia de la política para la modificación de módulos de los sistemas y en conjunto con el jefe de Desarrollo y Mantenimiento de Sistemas se generó un documento.

Se asignó a dos programadores como DBA, dicho personal se encargaba de crear las bases de datos para las pruebas de los programadores.

Se instaló un servidor para el control de versiones en el servidor de desarrollo.

2.2. Mantenimiento preventivo y correctivo a equipo de cómputo del INCMNSZ.

Por razones administrativas el Instituto rescindió el contrato a la empresa de mantenimiento de equipo de cómputo, por tal motivo la Subdirección de Informática realizó dichos mantenimientos durante más de un año.

Para solventar esta nueva tarea, se solicitó personal de servicio social y se le asignó tiempo extra a programadores y operadores, además se creó la Coordinación de Soporte Técnico.

Se me encomendó la capacitación en mantenimiento preventivo a personal de servicio social ya que yo había tomado cursos de mantenimiento de computadoras en la escuela. Se les capacitó en lo referente a las partes que componen a una computadora, el manejo de los componentes electrónicos, detección de fallas de hardware, limpieza de los diferentes dispositivos y carcasa.

Se asesoró a la coordinadora de soporte técnico en la compra de kits de mantenimiento y herramienta (desarmadores, kit de puntas, pinzas de corte y punta, etc.) así como de consumibles para mantenimiento (alcohol, espuma limpiadora, Aire comprimido, etc.)

2.3. Implementación de políticas de respaldo.

Los respaldos se realizaban diariamente en las noches, sin embargo, debido al tipo de respaldo (sistema de archivos) detenían las bases de datos y por medio de un script negaban el acceso a los usuarios. Para lograr que los usuarios no usaran el sistema, cambiaban los permisos de los directorios home de cada usuario, de tal modo que no podían ingresar al sistema HIS durante dicho periodo de tiempo.

Los respaldos se guardaban en citas DDS, y existía un esquema de respaldo que no era adecuado, lo anterior debido a que como se respaldaba el sistema de archivos, existían problemas cuando se respaldaban ligas. Además el respaldo de las bases de datos era también por sistemas de archivos, por tal motivo existían muchos errores cuando se restauraban la información de los respaldos.

Los scripts de respaldo no generaban logs por lo que no se sabía si el respaldo se había hecho de manera satisfactoria o si había tenido errores.

Se diseñó un esquema de respaldo y se comenzó a respaldar el vaciado (dump) de las tablas de la base de datos, de esta manera se podía exportar la base de datos a otro servidor, además los respaldos eran de menor tamaño.

A solicitud del jefe del Departamento de Desarrollo y Mantenimiento de Sistemas se crearon scripts, los cuales le daban mantenimiento a las bases de datos, dichos scripts tenían nombres como llavlun.sh, llavmar.sh, etc.
Se mejoró el tiempo destinado a respaldos y a su vez se mejoró la calidad de los respaldos.
Los respaldos se comenzaron a realizar usando rutas relativas en vez de rutas absolutas. Lo anterior causaba muchas veces que cuando los operadores querían comprobar un archivo que se encontraba en el respaldo, dicho archivo sustituía al archivo que estaba en producción al momento de extraerlo de la cinta magnética. Se implementó la política de verificar los respaldos en el servidor de desarrollo y a generar los respaldos con rutas relativas.

2.4. Ajustes en el Sistema Operativo de los servidores HIS.

Reparticionamiento de discos duros.

El espacio en los discos duros estaba mal distribuido, directorios del sistemas como */usr* , */var* y */opt* tenían muy poco espacio a pesar de que el disco duro tuviera espacio libre sin asignar. El espacio asignado a las particiones del sistema operativo era tan poco que causaba que no se pudieran instalar nuevos programas o que no se pudieran mantener por mucho tiempo las bitácoras del sistema.

Debido al limitado espacio disponible en disco no se pudieron instalar herramientas actuales de administración en los servidores.

Se redistribuyó el espacio en los discos duros asignándole más espacio a las particiones del sistema operativo.

Se crearon particiones nuevas las cuales se emplearon para la redistribución de la base de datos debido a que el máximo tamaño de un archivo en el sistema de archivos de HP-UX es de 2 Gb y existían tablas en la base de datos que estaban llegando a ese tamaño.

Bitácoras del sistema operativo.

Los archivos de bitácoras del sistema (logs) de HP-UX se perdían después de dos reinicios.

El sistema operativo solamente tenía disponibles las bitácoras que se iban generando en la operación actual y un log histórico, lo anterior era debido a que al reiniciar el servidor, el Sistema Operativo borraba el histórico para colocar en su lugar el que hasta antes del reinicio era el de operación. Lo anterior significaba que con dos reinicios del sistema operativo se borraran los logs, perdiendo así la posibilidad de detectar errores en los servidores.

Para corregir este problema, se modificó el script donde se manejaban las bitácoras del sistema por uno en donde existía una rotación de bitácoras del sistema similar al usado en sistemas Linux en el cual se guardaban mas archivos de bitácoras y los históricos se comprimían con gzip. Lo anterior en conjunto con el reparticionamiento de discos duros permitió que se mantuvieran por más tiempo las bitácoras del sistema y dar así la posibilidad de la detección de las fallas más comunes en el sistema operativo y la generación de manuales de operación y de contingencias.

Ajustes del Kernel del sistema operativo HP-UX.

Se ajustaron parámetros del Kernel del sistema operativo HP-UX.
Dichos ajustes fueron solicitados por la empresa contratada para el soporte de las bases de datos (Ingres México), con dichas modificaciones se mejoró considerablemente el rendimiento de las bases de datos.

Sin embargo, no se pudieron realizar otros ajustes de Kernel para el mejoramiento del rendimiento del sistema operativo, lo anterior era porque el sistema operativo HP-UX solo cuenta con la aplicación de administración SAM para modificar los parámetros del Kernel.

Desafortunadamente los ajustes que se pueden realizar son muy pocos además de que no existe mucha documentación al respecto para una versión tan antigua de HP-UX.

Deshabilitación de servicios innecesarios en los servidores.

Se desactivaron servicios que no se empleaban, modificando el archivo /etc/inetd.conf y comentando las líneas de los servicios que no se deseaban. Entre los servicios deshabilitados se encontraban los servicios rlogin, rshell, echo, time y finger.

A pesar de la instalación del servicio Secure Shell (SSH), no fue posible deshabilitar el servicio de telnet, el cual es conocido por su inseguridad y obsolescencia para las comunicaciones cliente-servidor, lo anterior se debió a que los emuladores de terminales HP que se usan en las computadoras con sistema operativo Windows usan este servicio para comunicarse con el servidor.

Instalación de software de administración en los servidores.

Debido a que no existía un control de acceso diferente al del sistema operativo, se instaló el software TCPwrappers, dicho software tiene por objeto el proporcionar una mayor seguridad en el acceso a los servidores SIPAM y ADMINISTRATIVO. Mediante TCPwrappers se restringió el acceso a los servidores solo a las direcciones IP de los usuarios de cada sistema, es decir, no se le permite la entrada al sistema ADMINISTRATIVO a segmentos de direcciones IP de cuentas que usan el sistema SIPAM.

Se instaló además el servidor SSH (Secure Shell) el cual es la opción más segura y mejorada para las sesiones remotas, pero solo se usó para la administración remota de los sistemas SIPAM y ADMINISTRATIVO.

Se instalaron además gcc, gtar, bunzip2, gzip y bash para sustituir a las versiones de HP-UX ya que ofrecían mejoras considerables.

2.5. Generación de planes de contingencia y de operación.

No existían planes de contingencia y los manuales de operación no detallaban los procedimientos para llevar a cabo la operación diaria. Los operadores de todos los turnos únicamente se limitaban a llamar a algún jefe de departamento o administrador de sistemas y no intentaban reparar la falla.

Lo anterior se derivaba de una mala selección de personal y una mala capacitación de los operadores ya que se reasignó a personal de otras áreas como operadores de sistemas, esto sin tener conocimientos previos de computación.

En diversas ocasiones se asistió en la madrugada o en fines de semana a resolver el problema debido a que el operador no tenía el conocimiento necesario para seguir las instrucciones, detectar las fallas y repararlas.

Con la implementación de la rotación de bitácoras, se realizó una base de conocimiento sobre las fallas más comunes en los servidores, así como la forma de resolverlos. Se detallaron los procedimientos de operación así como la generación de respaldos. Se generaron además planes de contingencia en donde se describieron detalladamente los procedimientos para la recuperación de los servidores en las fallas que se presentaban con más frecuencia. Se recopiló la información de contactos útiles como son los teléfonos de casa y celular del Subdirector de Informática, Jefes de Departamento y Administradores de Sistemas, Bases de Datos y de Redes; así como

los teléfonos y contactos de los proveedores de servicios. La información anterior se integró en un solo documento del cual siempre existía una copia en el SITE.

2.6. Curso de SO Linux a personal informático.

Debido al deficiente nivel de conocimiento presentado por operadores de los sistemas SIPAM y ADMINISTRATIVO, se determinó en conjunto con el Departamento de Selección y Capacitación de Personal que se impartiera un curso de sistema operativo Linux básico.

A dicho curso se invitó a administradores de sistemas de otras áreas del Instituto como hematología, infectología, microbiología, biblioteca y recursos humanos, además de personal del Departamento de Mantenimiento y Desarrollo de Sistemas.
Se determinó que sería de más utilidad un curso de Linux en lugar de uno de HP-UX (UNIX) debido a que en ese entonces se planeaba cambiar a la mayor brevedad el HIS (sistemas SIPAM y ADMINISTRATIVO) a un sistema sobre plataforma Linux.

Algunos de los temas que se dieron durante este curso fueron:

- Historia del Sistema Operativo LINUX.
- Partes y componentes de una computadora.
- Particionamiento de discos duros.
- Sistema de archivos usados en UNIX o Linux.
- Instalación de sistema operativo Linux.
- Niveles de arranque.
- Montaje y desmontaje de sistemas de archivos.
- Estructura de directorios en LINUX
- Servicios.
- Permisos de archivos y directorios.
- Administración de usuarios.

- Instalación de software y actualización del Sistema Operativo.
- Programación en Shell.
- Análisis de bitácoras.
- Monitoreo del sistema Linux.

Al finalizar el curso, los operadores estaban más familiarizados con los comandos del sistema operativo y eran capaces de realizar las instrucciones que se les daban de una forma más rápida y con menos errores, además, eran capaces de entender las salidas de la ejecución de dichos comandos, así como de aplicar filtros para hacerla más legible o enviar la salida a algún archivo para su análisis posterior. En algunos casos, eran capaces de hacer comentarios en caso de que observaran algún comportamiento extraño del sistema operativo o las bases de datos de los Servidores SIPAM o ADMINISTRATIVO.

En el caso de los demás administradores de sistemas, se les brindó el apoyo para que instalaran Linux en computadoras dentro de sus Departamentos y nuevos servicios, además de brindar el soporte en caso de dudas.

2.7. Soporte técnico a usuarios.

Se capacitó a personal de la subdirección y de servicio social en temas como:

- Desinfección de los sistemas operativos infectados por virus.
- Configuración de impresoras en red para usuarios con aplicaciones en Windows y DOS.
- Recuperación y borrado de cuentas de administrador.
- Configuración de grupos de trabajo para la compartición de recursos entre equipos de cómputo del mismo departamento.
- Reinstalación del sistema operativo.
- Respaldos de la información del usuario como documentos de texto, hojas de cálculo, imágenes, presentaciones, artículos médicos, correo electrónico, etc.
- Generación de imágenes de discos duros.

También se atendieron reportes en equipos de cómputo con sistemas operativos UNIX y Linux, configuración de impresoras y problemas con la red de datos. Además se atendieron reportes urgentes y reportes que no había podido resolver el personal de servicio social.

En el siguiente capítulo presento las actividades realizadas para cubrir los requerimientos de la Subdirección de Informática que no habían sido solventadas anteriormente, peor que eran muy importantes.

Capítulo III. Implementación de nuevos servicios en la Subdirección de Informática.

3.1. Servidor Web interno.

A solicitud del subdirector se realizó la instalación de un servidor Web en una computadora con sistema operativo Linux, dicho servidor tenía como finalidad fungir como un repositorio en el cual se pudieran almacenar manuales y artículos relacionados a Base de Datos, sistemas operativos y otros relacionados con la operación de la Subdirección de Informática.

Se instaló Apache Web Server y se configuró para ser compatible con PHP, se generaron cuentas de usuario a los programadores para que comenzaran a programar en un ambiente web. Se restringió el acceso a esta información usando el módulo htaccess de Apache, además de la asignación de los permisos necesarios en los directorios con información.

3.2. Servidor de compartición de archivos e impresión para el Departamento de Desarrollo y Mantenimiento de Sistemas.

Además del servidor de web, se instaló en el mismo servidor Linux el servicio para la compartición de archivos (File Sharing).

Mediante este servicio los programadores del departamento de Desarrollo y Mantenimiento de Sistemas compartieron información relacionada a los módulos asignados del sistema HIS. Además sirvió como un repositorio en donde guardaban los respaldos de sus programas.

Se instaló y configuró el servicio SAMBA para permitir el acceso desde las computadoras Windows de los programadores, además se configuró para permitir el acceso únicamente al segmento de red de la Subdirección de Informática así como a los usuarios con cuenta en el sistema.

Además del directorio home de cada usuario se creó un directorio público en el cual podían subir información para compartir con otros programadores.

3.3. Servidor de correo con web para la subdirección de informática.

Se realizó la instalación de un servidor de correo interno para la Subdirección de Informática el cual tenía como propósito el establecer un medio de comunicación entre personal de la subdirección y el Subdirector de Informática o los Jefes de Departamento.

Se instaló y configuró la aplicación Horde como Webmail y Qmail como servidor de correo electrónico (SMTP).

Se empleó este servicio además como un medio de asignación de tareas al personal de la subdirección así como un medio para avisos en general dentro de la Subdirección de Informática.

Se crearon cuentas a programadores, operadores y personal administrativo.

3.4. Servidor de pruebas para el Departamento de Desarrollo y Mantenimiento de sistemas.

Debido a que no existía un servidor en el cual se probaran los nuevos desarrollos, se instaló un servidor con un ambiente similar al de los servidores en producción. Para

esto se reutilizó un servidor HP que ya no estaba subutilizado debido a que dicho equipo tenía limitaciones en cuanto a memoria y disco duro.

Se reinstaló el sistema operativo con la versión usada en los servidores de producción, se le instalaron además herramientas como bash, SSH y se le deshabilitaron los servicios que no eran necesarios.

Debido a la limitación de espacio en disco se le agregaron sistemas de archivos en red mediante NFS (Network File System) en donde se tenían las aplicaciones tanto del servidor del SIPAM como del Administrativo, de tal manera que este servidor se pudiera comportar como cualquiera de los dos Servidores en producción montando los directorios específicos.

Se instalaron y configuraron además, dos instancias del manejador de base de datos. Este servidor podría desempeñarse además como un sustituto en caso de alguna falla severa en los servidores que se encuentran en producción.

Se generaron scripts para cambiar de directorios e instancia de base de datos y hacer más fácil el intercambio de servidores.

3.5. Servidor de Sistema de Archivos en Red.

Se instaló un servidor para compartición de espacio en disco mediante sistemas de archivos en red (NFS), los cuales eran montados en el servidor de pruebas y en los servidores de respaldo.

Este servicio fue instalado en un servidor con Sistema Operativo Solaris, el cual fue configurado para deshabilitar servicios no utilizados y cerrar puertos que no eran necesarios (Hardening de Sistema Operativo).

Se configuró el Servidor NFS para permitir el montaje solo a las direcciones IP de los servidores en producción y de desarrollo.

3.6. Servidor Proxy para personal de la subdirección de informática.

La subdirección de Informática solo tenía acceso a Internet en las computadoras del Subdirector y de los Jefes de Departamento, sin embargo, este servicio era requerido por el personal de la Subdirección de Informática.

Se evaluó y contrato el servicio de ADSL, el cual estaba conectado a un servidor Linux. Dicho servidor era dedicado para esta función específica y no proporcionaba ningún servicio adicional.

Se instaló y configuró el firewall de filtrado de paquetes Iptables con la postura general de negar el acceso a todo y aceptar solo lo específicamente permitido. Entre las políticas se incluyeron el no aceptar ninguna conexión desde internet al servidor excepto las relacionadas a conexiones previamente establecidas, es decir, no aceptar conexiones nuevas desde Internet hacia la LAN, no se aceptaban conexiones al servicio SSH del servidor excepto a las direcciones IP de los administradores y solo desde la tarjeta de red conectada a la LAN, no se permitían conexiones del mismo segmento de la LAN por la interfaz conectada a Internet.

Se instaló además el servidor proxy Squid, el cual fue configurado usando diferentes perfiles en los cuales se restringían sitios Web por nombre, por palabras en la URL, por contenido, por horario y además con un límite de ancho de banda para cada perfil de usuarios. No implementaba cache debido a que no contaba con mucho espacio en disco ni memoria RAM.

3.7. Implementación de ruteadores basados en Linux.

La red Institucional se contaba con segmentación de subredes, todo equipo conectado a la red institucional tenía una máscara de red 255.255.0.0. Lo anterior era debido a que nunca hubo un diseño de la red, de hecho, no se contaba con un mapa de red ni con el número de nodos en cada área en el Instituto.

Debido a la configuración plana de la red, el tráfico generado afectaba a muchos equipos y en caso de infección por virus de una computadora, ésta no se podía ubicar fácilmente.

Existía además la necesidad de crear nuevas redes, a las cuales se decidió asignarles un segmento nuevo y conectarlas a la red institucional por medio de ruteadores. Debido a que el tráfico por estos ruteadores no iba a ser demasiado, se emplearon computadoras antiguas con el Sistema Operativo Linux.

A dichos ruteadores Linux no se les instaló el ambiente grafico ni servicios extras por no ser necesarios para su correcto funcionamiento y administración.

Se crearon ruteadores para comunicar las redes de Radiología e Imagen, Toma de Muestras, Capacitación de personal e Informática.

Para interconectar los ruteadores se creó también una red adicional la cual usaba Ethernet, a diferencia del backbone que ocupaba Token Ring. Dicha red sirvió para ir migrando la red a Ethernet.

Durante mi estancia laboral en la subdirección de Informática obtuve mucha experiencia ya que yo era el administrador de los sistemas más importantes del Instituto, además, apliqué muchas de las cosas aprendidas en los trabajos previos como el trato para con los usuarios y también desarrolle otras como el manejo de un grupo al dar un curso.

Conocí además a personas con mucha experiencia en manejo de personal y en cuestiones administrativas, y al involucrarme laboralmente con ellos, aprendí del buen ejemplo.

Laboré en la Subdirección de Informática como administrador de sistemas en el periodo de enero de 2004 al junio de 2005.
Desde junio de 2005 a la fecha, me encuentro laborando en el departamento de Radiología e Imagen como administrador de sistemas.

Capítulo IV. Administración de servidores en el Departamento de Radiología e Imagen.

Actualmente el departamento de Radiología e Imagen cuenta con los sistemas PACS (Picture Archiving and Communications System) y RIS (Radiologic Information System) principalmente. Dichos sistemas requieren de una infraestructura de red robusta debido al volumen generado por la transferencia de imágenes, soporte técnico a los usuarios y personal que administre los sistemas.

Por tal motivo es necesario el apoyo de personal informático para este Departamento ya que con el crecimiento del departamento, crece también la necesidad de tener personal dedicado para este departamento.

4.1. Administración de servidores PACS.

El sistema PACS administra todo el flujo de imágenes radiológicas digitales provenientes de diferentes modalidades (equipos de radiología general, ultrasonidos, tomógrafos, resonadores magnéticos, angiografos, mastografos y endoscopios) y el envió de los estudios a las estaciones de diagnóstico y visualización.

El sistema PACS está conformado por 2 servidores en clúster de alta disponibilidad, los cuales están conectados a un arreglo de discos de 13 TB. Dichos servidores generan dos servidores virtuales, uno de aplicación y otro de base de datos. Al ser un clúster de alta disponibilidad, en caso de que algún servidor falle, el otro servidor toma su lugar y toma las aplicaciones que estaban en el servidor que falló. El arreglo de discos tiene redundancia mediante RAID 5 además de redundancia de los controladores de discos.

El sistema almacena las imágenes en el arreglo de discos, y la información asociada a

cada estudio se guarda en la base de datos del sistema PACS. Dicha base de datos guarda datos que son empleados para búsqueda y generación de estadísticas:

- Identificador de paciente.
- Apellido y nombre del paciente.
- Fecha de estudio.
- Grupo de estudio.
- Descripción del estudio.
- Modalidad.
- Fecha de envío al sistema.
- Iniciales del técnico radiólogo que realizo el estudio.
- Reporte asociado al estudio.

El sistema PACS incluye aplicaciones para su administración entre las que se encuentran:

Administración de usuarios.

Proporciona un interfaz para la creación, modificación, bloqueo y eliminación de cuentas de usuario del sistema y de grupos de usuarios, permisos a grupos y cuentas de usuario para el acceso a la aplicación de diagnóstico o a la de visualización, lista de grupos de estudios que pueden ser visualizadas, lista de servidores o estaciones de trabajo en las que pueden usar el navegador de pacientes y enviar imágenes a dichas estaciones de trabajo, permisos para el guardado de imágenes medicas en la estación de visualización, permiso para imprimir imágenes medicas en placas, permiso para habilitar la grabación de estudios radiológicos a CD's o DVD's.

Configuración del sistema PACS.

Interfaz para la configuración general del sistema PACS desde donde se puede configurar:

- Configuración general del sistema PACS, donde se encuentra el nombre del sistema

PACS, su dirección IP, AEtitle.

- La integración con el sistema RIS para asociar las imágenes con los estudios en RIS, la asociación de los reportes diagnósticos hechos en RIS con las imágenes medicas de dicho estudio en PACS.
- Configuración de los perfiles de estaciones de diagnóstico en donde se incluyen número de monitores, orientación de monitores, ubicación del monitor de administración.
- Lista de estaciones de diagnóstico con su respectiva configuración de nombre de la estación, dirección IP, AEtitle, numero de monitores de diagnostico.
- Configuración de las impresoras de placas con su nombre, dirección IP, AEtilte, tamaño de placas, máxima definición de la impresora.
- Configuración del grabador de CD's y DVD's con su nombre, dirección IP, AEtilte.

Monitoreo del sistema PACS.

Existen aplicaciones para el monitoreo de las licencias ocupadas, estado de los módulos del sistema PACS, estado de la cola de estudios por enviar y recibir, logs de los estudios enviados y recibidos.

Proporciona además la interfaz para el diagnostico de imágenes medicas, desde la cual se pueden realizar mediciones en las imágenes, modificación del contraste y el brillo de la imagen, rotación de imágenes, magnificación de la imagen, establecer niveles de ventana determinados para cada tipo de estudio, grabación de videos , grabación de los estudios en CD's o DVD's, guardado de imágenes en formatos Dicom, bmp, jpeg, tiff y gif, redistribución de las imágenes en los monitores de acuerdo a la modalidad, impresión de las imágenes en placas, y reconstrucciones de tomografías y resonancias magnéticas.

Por medio de un servidor WEB provee la aplicación para las estaciones de visualización en donde se pueden realizar mediciones, cambios de contraste, brillo, tamaño de la imagen, rotación de la imagen y un sistema de chat para consultas entre los médicos usuarios y los médicos radiólogos, además de la posibilidad de guardar imágenes a las estación de visualización, lo cual, por cuestiones de seguridad esta

deshabilitado.

Entre las funciones realizadas como administrador del sistema PACS del departamento de radiología e Imagen se encuentran:

- Mantener la operación continua y la confiabilidad del sistema PACS integrado a la red de Imágenes del Departamento de Radiología e imagen del Instituto.
- Identificar y resolver problemas que afecten la operación normal del sistema PACS y los sistemas de información e imágenes relacionados.
- Realización de las tareas y actividades regulares de operación y manutención preventiva, requeridas para la gestión y uso de imágenes diagnosticas, en los equipos asociados al sistema PACS (respaldos, reportes de conformidad, etc.).
- Generación y entrega de reportes de gestión y operación del servicio de radiología.
- Optimizar el costo operacional y de mantención de los sistemas de PACS y sus sistemas integrados.
- Comprobar el estado de los sistemas de archivos de los servidores de PACS.
- Comprobar el estado del arreglo de discos.
- Comprobar el estado de las tablas de las bases de datos mediante el uso de scripts.
- Manejo de usuarios del sistema PACS.
- Configuración de parámetros del sistema PACS.
- Configuración de aplicación de visualización en las terminales de diagnostico.
- Configuración de las estaciones de visualización.
- Corrección de datos erróneos al momento de la captura de datos del paciente.
- Configuración de modalidades para integrarlas a la red DICOM.
- Impresión de placas de imágenes de pacientes.
- Administración de la computadoras de diagnostico.
- Administración de las computadoras con cliente Web.
- Administración de las estaciones de reconstrucción de imágenes de corazón y neurología.
- Administración de los servidores para impresión de imágenes médicas en placas.
- Administración de personal de informática en el departamento de Radiología e Imagen.

4.2. Administración de servidores RIS.

El departamento de Radiología e Imagen cuenta además con el sistema RIS (Radiologic Information System) el cual administra todo el flujo de la información de un paciente en el departamento de Radiología e Imagen.

El sistema RIS está compuesto por 6 servidores, cada uno realiza una función que en conjunto conforman al sistema RIS. Existe un servidor de Base de Datos, un servidor de lista de trabajo (worklist), un servidor de reconocimiento de voz, un servidor de dictados y diccionario de palabras, un servidor de respaldos y un servidor de reserva.

El flujo de trabajo del sistema RIS es el siguiente:

1. Ingreso de datos del paciente en caso de no existir en el sistema.
2. Agendamiento de citas de estudios con asignación de sala y tiempo de duración.
3. Recepción del paciente en el sistema el día de su cita.
4. Envío de la lista de trabajo a cada modalidad, es decir, los estudios que se harán ese día en determinada sala.
5. Llenado de notas del paciente como son, alergias, enfermedades y medio de trasporte (caminando, silla de ruedas, camilla)
6. Notas sobre el material utilizado en el estudio.
7. Notas sobre incidentes con el paciente o con el equipo durante el estudio.
8. Interpretación del estudio por el médico radiólogo.
9. Envío del diagnostico del estudio al sistema SIPAM.
10. Impresión del reporte del estudio para el paciente y para el archivo clínico.

A cada usuario de le define un perfil, los perfiles pueden ser modificados, borrados o creados.

Entre los perfiles del sistema RIS se encuentran:

- Programador de citas:
    - Es el asignado al personal de la recepción.
    - Puede generar citas y modificarlas.
    - Solo puede entrar al módulo de agenda.
- Técnico radiólogo:
    - Asignado a los técnicos radiólogos.
    - Puede generar citas de su departamento (Tomografía, Resonancia Magnética, Radiología general, Mastografía) pero no puede modificar las citas que han sido programadas por él.
    - Solo puede entrar al módulo de agenda.
- Médico residente
    - Puede generar citas de cualquier departamento.
    - Tiene acceso al módulo de diagnóstico pero solo puede generar diagnósticos preliminares.
    - Puede entrar al módulo de agenda y de diagnóstico.
- Medico radiólogo.
    - No puede generar citas.
    - Puede generar diagnósticos definitivos y puede modificar los diagnósticos preliminares.
    - Cuenta con reconocimiento de voz.
    - Solo puede entrar al módulo de diagnóstico.
- Administrador de sistema.
    - Puede entrar a todos los módulos.
    - Puede generar citas y modificarlas.
    - Puede crear, eliminar o modificar cuentas de usuario.
    - Puede configurar las salas y horarios. Puede generar nuevos estudios.

Una vez realizado el estudio, el técnico o médico residente da por terminado el estudio y entonces puede ser interpretado en el módulo de diagnóstico.

Existen dos niveles de firma de reportes:

- Firma 1: Se le asigna a los médicos residentes, dicha firma no libera el diagnóstico y no

es enviado al sistema SIPAM, además si se imprime, coloca una leyenda en donde indica que es un diagnóstico preliminar. Este diagnóstico puede ser borrado o editado por un usuario con firma 2.

- Firma 2 o firma definitiva: Se les asigna a los médicos adscritos, jefe de residentes y residentes de cuarto año. Dicho reporte no puede ser borrado, solo, se puede agregar comentarios al final del reporte. El sistema RIS libera los reportes con firma 2 y los imprime para el archivo clínico.

El sistema RIS cuenta además con un módulo de reportes en el cual se realizan reportes del funcionamiento del sistema RIS, reportes de estadísticas de rendimiento de personal, número de estudios diagnosticados, número de estudios de determinada modalidad, tiempos desde el arribo del paciente para su estudio hasta su diagnostico.

También tiene un módulo para la administración de usuarios en donde se definen nombres de usuario en el sistema, nombre del usuario , contraseña, contraseña para la firma, módulos a los cuales tiene acceso el usuario, asignación de perfil de usuario, habilitación de reconocimiento de voz, definición de permisos.

El sistema RIS también proporciona un módulo para el control de inventario de equipo del departamento de Radiología e Imagen, pero dicho módulo aun se encuentra en periodo de implementación.

Entre las funciones realizadas como administrador del sistema RIS se encuentran:

- Administración de los servidores de RIS.
- Administración de usuarios del sistema.
- Administración de licencias de reconocimiento de voz.
- Configuración del sistema para días festivos.
- Administración de salas de estudios. En caso de falla de equipo, se cancela en el sistema la sala para que el sistema no asigne estudios en dicha sala.

- Administración de lista de estudios, por ejemplo, agregar estudios de un protocolo

nuevo.

- Administración de la lista de trabajo para las modalidades. Si un equipo nuevo llega, se debe de agregar a la lista de modalidades que recibirán la lista de trabajo. Así mismo, se elimina su configuración si el equipo es dado de baja.
- Generación de nuevos reportes.
- Administración de las computadoras con cliente RIS.

4.3. Administración de la red DICOM de Radiología e Imagen.

Además de la administración de los sistemas RIS y PACS, soy encargado de la red de Imagen.

Entre mis funciones se encuentran:

- La identificación de nuevos requerimientos, por ejemplo, creación de nodos nuevos.
- Detección y corrección de problemas relacionados con la infraestructura de red.
- Análisis de tráfico de la red de datos.
- Administración del segmento de red 192.9.200.X/24 que fue asignado al Departamento de Radiología e Imagen.
- Administración del segmento de red 10.10.50.X/24 que fue asignado para la red de Imagen fuera del departamento de Radiología e Imagen.
- Administración de la red DICOM. Lo cual incluye las direcciones IP de los segmentos, nombres en la red DICOM (AEtitle) y puertos para las aplicaciones y para la lista de trabajo.
- Administración del ruteador/firewall Linux que tiene como función comunicar los dos segmentos de red previamente mencionados, además controla el tráfico hacia la red de Radiología.
- Administración de los Switches administrables y no administrables.
- Administrador del equipo de la VPN.

4.4. Administración de servidor VIPA.

Servidor de respaldo del sistema PACS el cual cuenta con un robot de cintas LTO 2 con capacidad de 20 cintas y 2 de limpieza. Dicho servidor tiene también la posibilidad de agregar archivos en formatos diferentes al DICOM, los cuales son relacionados por medio del nombre y del registro del paciente. Dichos archivos pueden ser agregados mediante una interfaz WEB y pueden ser consultados por el mismo medio. Por razones de seguridad dicho servidor se encuentra ubicado en otro edificio.

El servidor VIPA recibe los estudios del PACS durante la noche, en el sistema PACS se define la cantidad de estudios a ser respaldados.

Dicho servidor no está instalado en su totalidad debido a que se requiere que respalde los resultados del departamento de Laboratorio Central y aun se encuentran en la fase de diseño de la interfaz.

La aplicación Web se configura para crear cuentas de usuario para la visualización y permitir solo a determinados usuarios la posibilidad de agregar archivos no DICOM.

4.5. Mantenimiento preventivo a equipo de cómputo del Área de radiología e Imagen.

En caso de que los equipos relacionados con los sistemas PACS o RIS se encuentren muy sucios, se les da mantenimiento preventivo. Existe un contrato de mantenimiento pero existen áreas en donde las computadoras se ensucian más.

También realizo la función de enlace con el departamento de Ingeniería Biomédica para el reporte de equipo médico y levantamiento de reporte con el proveedor, además de ser responsable del seguimiento del reporte.

Además tengo contacto constante con personal del área de Mantenimiento del hospital para lo relacionado a fallas de luz, goteras en salas donde existe equipo de cómputo, problemas con aire acondicionado y fallas de UPS.

4.6. Implementación de nuevos requerimientos.

Debido a nuevos servicios que son requeridos por personal médico y administrativo, se han instalado diversas soluciones para satisfacer dichas necesidades.

Servidor de Compartición de archivos.

Debido a la necesidad de los médicos de tener un repositorio para las imágenes medicas, instalé un servidor Linux con SAMBA.
Este servidor se emplea para respaldo de las imágenes de casos interesantes, los cuales serán presentados en sesiones médicas o en congresos, además, al emplear este servidor para el copiado de imágenes en memorias USB, se evita la propagación de virus en la red de Radiología e Imagen.

Restricción de equipos en el Departamento de Radiología e Imagen.

Debido a que las terminales de visualización usan el Sistema Operativo Windows y que los usuarios deben ser administradores para el correcto funcionamiento de la aplicación, se tomó la decisión de restringir las cuentas de usuario para que solo puedan ejecutar el navegador y no puedan explorar el disco duro, no puedan visualizar las unidades de almacenamiento, no puedan acceder a la línea de comandos, no ejecute el autorun de los dispositivos y no puedan ingresar al panel de control.
Dicha restricción se realiza usando software de Microsoft para computadoras compartidas.

Instalación de un sistema de monitoreo de red.

Se instaló un sistema de monitoreo para el checado de los servidores de PACS., RIS, VIPA, ruteadores Linux, Conexión remota y equipos de comunicación. El sistema empleado para monitorear es Nagios, se pretende en un futuro contratar el servicio para el envió de mensajes SMS en caso de contingencias.

Al encontrarme en un área que se está desarrollando de forma continua y al ser el INCMNSZ una de las instituciones con mejor equipo tecnológico para el diagnostico de imágenes medicas en el país, es necesario que el departamento de Radiología e Imagen cuente con personal informático capacitado.

Es impresionante la diversidad de equipos que existen en el área de Radiología e Imagen, y para todos y cada uno de ellos debo de involucrarme y coordinarme con el personal de las empresas fabricantes para que se puedan instalar correctamente.

Como ejemplo de la diversidad de equipo, el Instituto cuenta con ultrasonidos y equipos de radiología general portátil que usan Windows como sistema operativo, estaciones de trabajo para reconstrucción de imágenes con sistemas operativos Linux y los servidores con sistema operativo UNIX.

Al ser el departamento de Radiología e Imagen un área crucial para el diagnostico de la enfermedades de los pacientes, se requiere que esté operando de forma ininterrumpida por lo que trato de involucrarme lo más posible para poder resolver problemas en los diferentes equipos sin tener que esperar a los ingenieros de servicio de los diferentes fabricantes.

Por tal motivo me encuentro en capacitación continua por los ingenieros de servicio y trato de aplicar los conocimientos adquiridos para mejorar el funcionamiento del departamento.

Capítulo V. Actividades adicionales.

Entre las actividades que he realizado y que forman parte de mi experiencia laboral se encuentran:
Impartición de cursos, soporte técnico a usuarios, mantenimientos preventivos y correctivos, instalación de redes, configuración de equipos de comunicación, instalación y configuración de servidores para nuevas aplicaciones, migración de servidores Windows a Linux y apoyo en auditorias informáticas.

5.1. Curso de Administración de PACS.

Como parte de la instalación del sistema PACS, se me envió a un curso en Estados Unidos, Dicho curso tuvo una duración de 5 días de los cuales el primero fue de administración de UNIX y los 4 restantes del sistema PACS.

Durante dicho curso se me capacitó en la administración del sistema PACS viendo a detalle cada módulo que comprende al PACS, además se vieron los siguientes temas:

- Ubicación de las bitácoras del sistema PACS.
- Problemas comunes.
- Procedimiento para la corrección de datos del paciente.
- Administración de usuarios.
- Asignación de nuevas modalidades en el sistema PACS.
- Redes DICOM.
- Grabación de CD’s con los estudios de los pacientes.
- Scripts para checar el sistema operativo y bases de datos.
- Administración de estaciones de diagnostico y de estaciones de visualización.
- Manejo de interfaces para el monitoreo del clúster, el arreglo de discos y el UPS.

5.2. Diplomado de Seguridad Informática.

Se cursó el diplomado de Seguridad en Informática impartido por la UNAM como un complemento a la educación obtenida durante la carrera, además de que me sirvió para mejorar aspectos relacionados con la seguridad informática en mi lugar de trabajo.

Después de tomar el diplomado, pude mejorar aspectos de la seguridad en los servidores, la red y los clientes. También fui capaz de instalar una VPN para el acceso remoto a los servidores e inclusive apoyé en auditorias informáticas en otros sitios.

El diplomado contó con los siguientes módulos, de los cuales menciono los puntos principales y conceptos importantes.

Módulo 1. Problemática y definición de seguridad informática.

Historia de la Información.

El manejo de la información es realizada a través de nuestros 5 sentidos. La información obtenida es entonces almacenada, organizada y después sirve para crear nueva información. Para la transmisión de la información es necesaria una tecnología, un medio de almacenamiento externo y la tecnología inversa, por ejemplo, para la transmisión de la información por medio de la escritura, se emplea la tecnología de saber escribir, el medio de almacenamiento es un papel o piedra y la tecnología inversa es saber leer lo escrito.

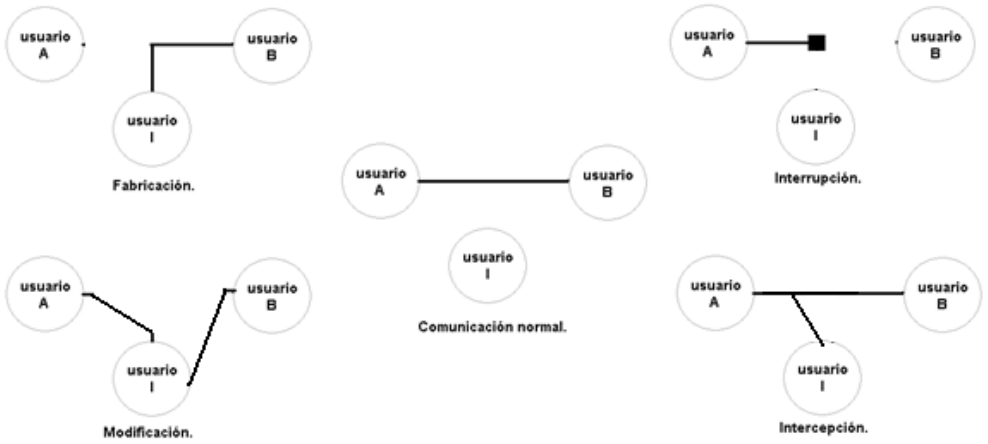
Características de la Información.	
Confidencialidad.	Que solo determinados entes reciban la información.
Integridad.	Que la información se mantenga sin distorsiones o errores, es decir, que la información no cambie.
Autenticidad	La certeza del origen de la información.
Disponibilidad	Que la información se encuentre lista para usarse cuando se la solicite.

Conceptos de Seguridad Informática.

Sistema de cómputo.	Conjunto formado por la colección de hardware, software, medios de almacenamiento, datos o información, y personas involucradas.
Vulnerabilidad	Cualquier debilidad que pueda usarse para causar daño. El punto más débil de un sistema consiste en el punto de mayor vulnerabilidad.
Amenazas.	Cualquier circunstancia con el potencial suficiente para causar daños al sistema.
Algoritmo.	Es una serie finita y ordenada de pasos para resolver un problema. Los ataques a los algoritmos son procedimientos matemáticos, es decir, son ataques por criptoanálisis.
Protocolos.	Son una serie de pasos para llevar a cabo una tarea específica, usando uno o más algoritmos. Los ataques a los protocolos explota la forma en que implementan los algoritmos, son la mayoría de todos los ataques.
Atacante.	Pueden ser personas, procesos o dispositivos, también son llamados intrusos, enemigo, hacker, cracker o ente malicioso. Los atacantes tienen por objetivo obtener la información en claro o la llave para su descifrado, acceder a los recursos del sistema o solo molestar.

Existen cuatro tipos de amenazas principales que explotan las vulnerabilidades:

1. Interrupción: No permitir que se use un recurso.
2. Intercepción: Alguien o algo no autorizado logra el acceso a algún activo del sistema.
3. Modificación: Cuando se logra acceso al sistema y se pueda cambiar la información, agregando o quitando partes de esta.
4. Fabricación: Generación de información falsa.



Ataque: Acción que explota una vulnerabilidad.

- Ataques pasivos: Solo afectan la confidencialidad, usualmente son la antesala a los

ataques activos. Por ejemplo, lectura o fisgoneo de mensajes, análisis de trafico de red.

- Ataques activos: Afectan la integridad y autenticidad, además de la confidencialidad. Por ejemplo, engaño, suplantación, replica y modificación de mensajes, negación de servicio.

Principales activos a proteger:

- Hardware.
- Software.
- Datos.

Servicios de seguridad: definen los objetivos específicos a ser implementados a través de los mecanismos de seguridad. La arquitectura de seguridad OSI reconoce 5 clases de servicios:

Servicios de Seguridad Informática.	
Confidencialidad.	Garantizar que la información solo pueda ser accesada por las partes autorizadas.
Autenticación.	Garantizar que los participantes de una comunicación sean quienes dicen ser. Garantizar la autenticidad de origen de los datos, que vengan de donde dicen venir. Está muy relacionada con el control de acceso.
Integridad.	Que la información permanezca sin modificaciones hasta que un ente autorizado la modifique.
Control de acceso.	Protege activos del sistema contra accesos y uso no autorizados. Se implementa mediante modelos y técnicas propias.
No repudio.	Proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje, o haber sido originario o destinatario de una acción.

Mecanismos de seguridad: consisten en alguna funcionalidad específica para algún servicio de seguridad. Se agrupan en específicos (Cifrado, firma digital, Integridad) y obicuos o no específicos (Niveles de seguridad, Detección de eventos).

Módulo 2. Criptología.

Servicios de seguridad: Es lo que se busca obtener en cuestiones de Seguridad Informática.

Mecanismo de seguridad: Es el “como” se obtienen los servicios de seguridad.

Servicio	Mecanismo
Confidencialidad	Cifrado
Autenticación	Protocolos criptográficos y firma digital
Integridad	Funciones Hash
Control de acceso	Modelos (Bell, Lapadula)
No repudio	Firma digital
Disponibilidad	No se puede asegurar

Criptología.

Es la ciencia para ocultar información.

Criptología.	
Criptografía.	Parte de la Criptología que permite el cifrado y descifrado de la información. Emplea algoritmos de cifrado.
Criptoanálisis.	Ataques a los algoritmos para que a partir del criptograma y conociendo el algoritmo empleado, se pueda deducir el mensaje original buscando patrones. Normalmente usa las matemáticas como su mejor herramienta usando muchas disciplinas como estadística, probabilidad, teoría de números y algebra.
Esteganografía.	Ocultar información dentro de otra información, sin embargo, al ser seguridad por oscuridad el algoritmo no puede ser público.

Criptosistema: Implementación de un algoritmo criptográfico

Algoritmo criptográfico: Emplea funciones para el cifrado del mensaje (M) y el descifrado del Criptograma (C) . Las funciones para el cifrado (fc) y descifrado (fd) pueden ser distintas y además pueden usar llaves (k).

Algoritmo de cifrado → $f_{kc}(M) = C\ funcion\ de\ cifrado$

Algoritmo de cifrado → $f_{kd}(c) = M\ funcion\ de\ descifrado$

Si Kc = Kd es criptografía simétrica.

Si Kc ≠ Kd es criptografía asimétrica.

Si no hay K entonces son funciones Hash

Criptografía simétrica.

Existe el acuerdo previo de un secreto (la llave). El acuerdo de llave no forma parte del algoritmo de cifrado. Emplea operaciones como sustituciones y permutaciones.
Solo existe una llave, esta se usa tanto en el cifrado como en el descifrado.

Para un mensaje M, su función de cifrado se denota por:

$$E_k(M) = C$$

Y para el descifrado:

$$D_k(C) = M$$

Clasificación de algoritmos de llave secreta.

Los algoritmos se pueden clasificar por flujo y por bloques.

- Algoritmos por flujo:
  - Cifran un bit/byte a la vez.
  - Son más fáciles de analizar matemáticamente.
- Algoritmos por bloque:
  - M se divide en bloques de **n** bits.
  - C es de la misma longitud que M.
  - Pueden comportarse como los algoritmos de flujo.

Los algoritmos también se pueden clasificar de acuerdo al tipo de operaciones que emplean.

- Sustituciones: Mapeo de caracteres.
  - Corrimientos: Emplean el mismo alfabeto y solo recorren posiciones en el, el ejemplo más común es el algoritmo Cesar, el cual recorre cada letra tres posiciones quedando: a=d, b=e, c=f, d=g … x=a, y=b, z=c. El criptoanálisis se realiza con análisis de frecuencias.
  - Sustituciones simples: Se emplea una sustitución carácter a carácter, se crea una tabla en donde se define que carácter representa al carácter real. El criptoanálisis es por análisis de frecuencias.

- Polialfabéticos: Se emplean varios alfabetos, un carácter se sustituye en un alfabeto y al siguiente, el carácter se sustituye usando otro alfabeto. El criptoanálisis es el ataque del péndulo en el cual se calcula t (periodo=1/frecuencia) y se hace el método de análisis de frecuencias sobre cada alfabeto.

- Permutación o Transposición: Se emplean matrices y se sustituyen lo caracteres cambiando la posición, por ejemplo sustituyendo renglones por columnas. También es propenso al ataque de análisis de frecuencias.

De lo anterior se obtiene que lo mejor de los algoritmos que emplean permutación es la difusión de datos y lo mejor de la sustitución es la confusión. A los algoritmos que usan la confusión y la difusión se les llama producto.

Criptografía asimétrica o de llave pública.

Todos los algoritmos de cifrado asimétrico emplean un par de llaves, las cuales son creadas, usadas y desechadas juntas. De estas llaves una es pública y otra privada, la llave publica se coloca en un directorio accesible a todos, si alguien quiere comunicarse con A busca su llave pública y cifra el mensaje con esta llave, solo A puede descifrarlo ya que solo él conoce su llave privada.

El cifrado de llave pública es computacionalmente muy costosa.

PKI es una infraestructura para la generación de llaves y el manejo de los certificados digitales.

La funciones para el cifrado son:

$$E_{kpriv}(M1) = C1, \quad E_{kpub}(M2) = C2$$

Y para el descifrado:

$$D_{kpub}(C1) = M1, \quad D_{kpriv}(C2) = M2$$

Funciones Hash.

También llamadas funciones de digestión, compendio o dispersión. Generan una salida fija sin importar el tamaño de la entrada. Cuando se aplica la función hash a un

mensaje, se obtiene su valor hash el cual es un identificador o huella digital de un mensaje.

$$h(M) = vh$$

Las funciones hash con salida de 64 bits son muy pequeñas tendrían muchas colisiones, por lo tanto la mayoría de las funciones hash producen 128 bits de salida.

La resistencia a colisiones de una función hash determina que tan difícil es encontrar dos mensajes aleatorios M y M', tales que H(M)=H(M').

Algoritmos de cifrado empleados actualmente.	
Criptografía simétrica.	DES (Data Encryption Standar), 3DES. AES (Advanced Encryption Standar).
Criptografía asimétrica.	RSA para cifrado y descifrado. Diffie Hellman para acuerdo de llaves. El Gamal => DSA para firma digital.
Funciones Hash.	MD5 (Message Digest V5) SHA (Secure Hash Algorithm).

Módulo 3. Aplicaciones criptográficas.

En este módulo se vio la creación de protocolos seguros.
También se revisaron los principales algoritmos criptográficos que son usados en la actualidad.
RSA. Nombrado así por sus tres inventores Ron Rivest, Adi Shamir y Leonard Adleman. RSA basa su seguridad en el problema de factorizar números muy grandes.
Diffie-Hellman. Para el intercambio de llave seguro.
DSA. Es una variante de los algoritmos de firma de Schnorr y ElGamal.
DSA y Diffie Hellman basan su seguridad en la dificultad de calcular algoritmos discretos en un campo finito.

Módulo 4. Control de acceso.

Historia del control de acceso.

Perímetro: es una barrera que impide el acceso franco, debe de identificarse y diferenciarse el interior y el exterior. Pueden existir varias capas de perímetros. Un perímetro debe ser vigilado.

Un perímetro debe cubrir las tres dimensiones, es decir, no basta con las paredes, debe de asegurarse el piso y el techo. Debe de existir un centro de monitoreo del perímetro el cual debe estar lejos del perímetro pero con comunicación estable, además debe de contar con un equipo de respuesta rápida.

En los perímetros deben de realizarse bitácoras de entrada/salida y se debe verificar el no retorno, es decir, no puedes entrar si no has salido y no puedes salir si no has entrado. En el caso de que existan más perímetros, los perímetros interiores al ser más pequeños se pueden controlar mejor y se pueden implementar listas de control de acceso.

Pasos del control de acceso:

- Registro: Es el inventario de todo el sistema, si llega algo nuevo, se debe de agregar al inventario, si algo se va, se debe de quitar del inventario.
- Identificación: se establece quien puede entrar y quien no, es decir, quien es parte del inventario y quién no.
- Autenticación: Comprobar que se es quien se dice ser.

Autenticación.

Al inicio se usaban signos distintivos, después se desarrollaron las metodologías santo y seña (Challenge and Response). No se dice autentificación.

Tipos de autenticadores y mecanismos que los implementan.	
Algo que se conoce.	Verificación de Passwords.
Algo que se tiene.	Token.

Algo que se es.	Biometría.
Algo que determina la posición geográfica.	GPS.

Autenticación basada en biometría:

Para que una característica sea un buen autenticador, debe ser único para cada ente y no debe cambiar fácilmente, además debe poder representarse matemáticamente.

La forma de autenticación tiene los siguientes pasos:

- La persona deposita características al registro.
- La descripción matemática se guarda en la lista de usuarios.
- El dispositivo de captura recibe la característica y la compara con la descripción matemática que hay en el registro del sistema.

El dispositivo de captura debe ser idéntico en el registro y verificación.

La autenticación biométrica se puede dividir en biometría conductual y biometría biológica.

- Biometría conductual: Característica en la conducta de cada ente, por ejemplo, la verificación de firmas autógrafas midiendo la velocidad de escritura, las pausas y las separaciones del papel, también el ritmo y velocidad con el que se escribe en un teclado,
- Biometría Biológica: Medición de alguna característica del cuerpo. Por ejemplo: La huella dactilar, geometría de la mano, verificación de la voz, análisis de la retina o del iris, reconocimiento de rostros.

Autenticación basada en geoposicion:

Emplean los satélites de los sistemas de GPS, con dicha señal generan una llave de geoposicion, además incluye la hora.

La segunda fase del control de acceso consiste en impedir que el usuario ejecute algo que no está permitido en las políticas. Dichas políticas deben estar dirigidas a preservar

la confidencialidad, integridad, autenticidad y disponibilidad.

Modelos de control de acceso.

- Discrecional: también llamado voluntario. Permiten a un usuario negar o aceptar el uso de sus archivos y se implementan mediante bits de permiso, lista de control de acceso.
- Mandatorio u obligatorio: El usuario no controla la autorización de acceso de información, a los usuarios se les asigna un nivel de autorización de acceso, la información también se clasifica de acuerdo a su sensibilidad. La autorización de acceso se basa en comparar las etiquetas de los objetos y los sujetos. Un ejemplo de este tipo de control de acceso es el modelo de Bell-LaPadula y el de Biba
- Optimista: Es un modelo que hace factible un relajamiento de las estrictas condiciones del control de acceso. Se confía en el administrador, es decir, las violaciones a los controles se permiten siempre y cuando se auditen minuciosamente, con la hipótesis de que todos los accesos son bien intencionados.

Módulo 5. Administración de seguridad.

Algunos puntos clave en la administración de la seguridad son los siguientes:

- Conocer y comprender los objetivos de la organización. Estos deben ser consensados entre el personal de la organización.
- Definir políticas de seguridad que regulen el uso adecuado de los recursos de cómputo y que sean compatibles con la normatividad interna y externa.
- Establecer controles con base en el análisis de riesgos.
- Manejar incidentes.

La misión de seguridad de una empresa se obtiene de la misión principal, se toman las palabras clave y se generando una misión que apoyada en la seguridad informática ayude a conseguir la misión principal. Dicha misión de seguridad debe definirse en consenso, de preferencia usando un método para evitar discusiones inútiles
Una opción es usar el método Delphi para lograr el consenso.

Una Política de Seguridad es el conjunto de lineamientos que regirá el buen uso de los recursos informáticos y de cómputo de una Organización. Refleja los principales objetivos de la Organización y cómo la seguridad contribuye a alcanzar tales objetivos (Misión de Seguridad). En ella se describen tanto los derechos como las obligaciones a que están sujetos los diferentes tipos de usuarios.

Previo a la definición de las políticas de seguridad se debe de tener una idea de cómo esta la seguridad en la organización, para esto de deben de definir los activos críticos, evaluar los riesgos yl usar herramientas hacker.

Elementos a considerar para el desarrollo de las políticas.	
Protección de los recursos. Clasificación de los recursos. Separación de funciones. Monitoreo. Mínimo privilegio. Mejores prácticas y guías.	Redundancia. Continuidad. Actualización. Cultura. Administración.

Posturas adoptadas en el desarrollo de políticas de seguridad.	
Nada está permitido.	Paranoico
Lo que no está expresamente permitido está prohibido.	Prudente
Lo que no está expresamente prohibido está permitido.	Permisivo
Todo está permitido.	Promiscuo

Las herramientas de apoyo dan un enfoque de cómo lograr los objetivos de las Organización.

Dichas herramientas son:

- Estándares
  - Especifican tecnologías, parámetros o procedimientos cuyo uso uniforme beneficiará a la organización. Son obligatorios

- Recomendaciones
  - Son el reconocimiento de que no siempre es apropiado imponer estándares por costo,

factibilidad (o porque aún no existen)

- Procedimientos
  - Conjunto de pasos detallados que hay que seguir para lograr objetivos específicos de seguridad

Las políticas de seguridad deben de considerar sanciones, dichas sanciones deben estar por escrito. Se pueden poner sanciones genéricas y un comité define que sanción aplica. Las políticas deben estar firmadas por el más alto nivel, de esta manera se evita que existan niveles en los que no apliquen las políticas.

Análisis de riesgos.

Definiciones para el Análisis de Riesgos.	
Amenaza.	Un evento con el potencial de causar un acceso no autorizado, la modificación, revelación o destrucción de información, sistema, servidor o proceso. Se clasifican en naturales (terremotos, inundaciones, incendios) y humanas (negligencia, ignorancia, vandalismo, espionaje)
Vulnerabilidad.	Debilidad, defecto o falla de diseño.
Riesgo.	Probabilidad de que una amenaza explote una vulnerabilidad.
Control o mecanismo.	Medida de protección de los activos informáticos.
Activo informático.	Datos, información, sistemas de cómputo, software, hardware o cualquier elemento de tecnología de la información.
Proceso crítico.	Proceso que impacta directamente en la consecución de los objetivos de la organización.

Beneficios de un Análisis de riesgos:

- Identifica los puntos débiles de la infraestructura informática de la Organización.
- Permite la selección de las medidas de protección.
- Determina donde es necesario contar con esquemas de recuperación de desastres y continuidad de negocio.
- Permite realizar las políticas de seguridad mejor adaptadas a las necesidades de la organización.

Existen análisis de riesgos cualitativos y cuantitativos. Los análisis cualitativos no determinan valores numéricos por lo que los resultados son subjetivos, además no

existe la base para demostrar el costo-beneficio, pero tiene como ventaja que los cálculos son muy sencillos. Los análisis cuantitativos están enfocados a determinar valores numéricos (generalmente monetarios) así como el costo de sus posibles pérdidas. Es fácil mostrar el costo-beneficio en términos comprensibles, pero sus cálculos suelen ser complejos.

Pasos del Análisis de Riesgos.	
1. Enunciar el alcance.	6. Estimar el impacto total de la amenaza.
2. Conformar el equipo de desarrollo.	7. Identificar medidas de protección.
3. Identificar amenazas.	8. Realizar un análisis costo-beneficio.
4. Priorizar amenazas.	9. Ordenar las medidas de protección con prioridades.
5. Determinar la prioridad en función del impacto.	10. Reportar en resultado del análisis.

Estándares.

Los estándares tienen como función servir de punto de referencia para identificar los controles necesarios en diversas situaciones en la que están involucrados los sistemas de información.

ISO 17799. Es un conjunto de controles que incluyen las mejores prácticas en seguridad de la información. Esta organizado en 10 secciones.

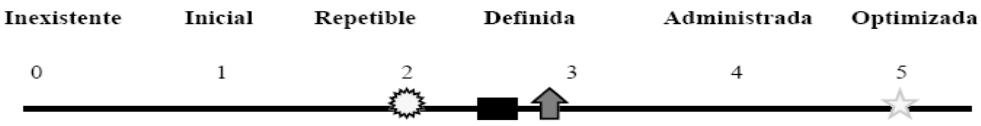
1. Información de las políticas de seguridad.
2. Organización de la seguridad.
3. Clasificación de activos y su Control.
4. Control de acceso.
5. Administración de comunicaciones y de las operaciones.
6. Desarrollo de sistemas y su mantenimiento.
7. Administración de la continuidad del negocio.
8. Seguridad del personal.
9. Seguridad física y ambiental.
10. Cumplimiento.

Modelos de madurez.

Los modelos de madurez para el control de procesos consisten en un método de

puntaje en el cual la Organización se califica. Existen 5 niveles de madurez.

Se establece un nivel de madurez para cada uno de los 34 procesos de COBIT, entonces se hace un grafico en donde queda representado el estado actual de la organización, el estado actual de la industria (competencia), el estado actual de los estándares internacionales y la estrategia de la organización para mejorar.



LEYENDA PARA LOS SÍMBOLOS USADOS	LEYENDA PARA LAS CLASIFICACIONES USADAS
Situación actual de la empresa	0 Inexistente - los procesos de administración no se aplican en absoluto
Lineamientos Estándar Internacionales	1 Inicial - Los procesos son ad hoc y desorganizados
Mejor Práctica de la Industria	2 Repetible - Los procesos siguen un patrón regular
Estrategia de la Empresa	3 Definida - Los procesos son documentados y comunicados
	4 Administrada - Los procesos son monitoreados y medidos
	5 Optimizada - Las mejores prácticas son seguidas y automatizadas

.

Módulo 6. Detección de intrusos y sobrevivencia de sistemas.

Debido a que la seguridad al 100% no existe, deben de existir métodos para la detección de intrusos. Por ejemplo:

1. Análisis de bitácoras. Casi cualquier programa tiene un sistema de bitácoras en donde se pueden configurar el comportamiento de las bitácoras, por ejemplo, donde se guardan, el nivel de reporte, etc. Sin embargo su análisis manual es tedioso y es difícil de identificar problemas al instante. La solución es emplear herramientas que analizan las bitácoras por nosotros.
2. Monitores y análisis de la actividad de los usuarios. Contar con elementos que permitan detectar si existe alguna alteración en el comportamiento e los usuarios.
3. Reconocimiento de ataques conocidos. Debido a que en la mayoría de los ataques se emplean herramientas creadas por otros intrusos, se puede obtener las características de determinado ataque y así es posible su detección.

4. Monitoreo del tráfico de la red. La gran mayoría de los ataques pasan por la red. Una

computadora que monitorea el tráfico de la red es capaz de detectar los ataques en tiempo real.

5. Verificación de la integridad de los archivos críticos del sistema. Los atacantes suelen modificar algunos archivos para asegurar su reingreso al sistema, una herramienta para detectar estas modificaciones es la verificación de la integridad de los archivos importantes.
6. Auditoria de la configuración del sistema y sus vulnerabilidades. Aunque no es parte de la detección de intrusos, si es un elemento que reduce el número de intrusiones.

Tipos de Intrusos.	
Intrusos externos.	Es alguien externo a la organización, este caso se da desde Internet. Les resulta más difícil la intrusión en servidores bien administrados. Al no conocer a fondo la empresa no saben cuáles son sus puntos críticos y tardan más tiempo, por ejemplo, en conocer la topología de la red, en conocer los servidores y los servicios proporcionados por estos.
Intruso interno.	Conoce muy bien la Organización y tiene acceso a los sistemas. Usualmente no son personal técnico, por tal razón les cuesta más trabajo.
Intrusos disfrazados.	Se disfraza como otro usuario, usualmente debido a descuidos con las contraseñas, es decir, contraseñas a la vista o contraseñas simples.
Usuarios abusivos.	Aquellos usuarios legítimos del sistema que exceden sus facultades y hacen un mal uso de sus privilegios, por ejemplo, un usuario que crea otro usuario o que ve la información de otros usuarios.

Sobrevivencia de sistemas: toda vez que un sistema ha sido comprometido, se deben seguir los siguientes pasos:

1. Detección: se debe de detectar los archivos modificados y recuperarlos de un respaldo.
2. Sacar al intruso: Buscar booby traps o rootkits en el sistema ya que es usual que el intruso deje un acceso para poder entrar. En algunos casos ajustar las políticas en los firewalls.
3. Reconstruir el sistema: Corrección de errores (bugs) y el análisis a fondo de la intrusión. Mejorar el sistema de acuerdo a lo encontrado en el análisis.

Módulo 7. Código malicioso.

Código Malicioso. Programa que tenga como objetivo causar algún tipo de ataque.

Al ser un programa, cualquiera que pueda programar, es capaz de hacer código malicioso. Es el problema de seguridad más costoso.
Algunos tipos de códigos maliciosos son:

Virus.
Un virus es un programa o parte de uno que está infectado y que tiene la propiedad de generar otros virus o copias de sí mismo, además es capaz de propagarse a otras computadoras por diferentes medios (floppy, USB, red, etc).

Un virus necesita dos cosas para funcionar: ser ejecutado por un usuario o proceso y estar en un ambiente adecuado. Por ejemplo, un virus en Windows, deja de ser un virus si se pasa a un Linux ya que no puede ejecutarse.

Al ser programas, los virus pueden realizar cualquier cosa que la computadora permita hacer a la cuenta infectada, por lo que si la cuenta es la de administrador, el virus puede hacer todo lo que un administrador.

La destructividad de los virus depende de que tan poderoso sea el sistema que infectan, por ejemplo, un virus en los servidores tiene más poder que uno en una computadora normal que no tiene tantos recursos ni tanta información.

Los virus que se replican a sí mismos se llaman gusanos o replicadores y son los que se propagan más rápido. Los virus que generan virus que no son iguales al original son los virus polimórficos y los multipartitas. Los virus polimórficos cambian un poco su estructura mientras que los virus multipartitas pueden entrar a diferentes tipos de archivos y de acuerdo a esto se comportan de diferente forma.

Clasificación de virus informaticos.	
Primera generación.	No requerían el uso de herramientas para su detección y eliminación. Detectables a primera vista. Tenían síntomas muy aparentes ya que solían sobrescribir otros archivos.
Segunda generación.	Requerían de herramientas simples para su detección y eliminación. Mantiene la funcionalidad de los programas infectados. Dejan algunos cabos sueltos como la modificación del registry de Windows, directorios nuevos y longitud de archivos que crece en el mismo tamaño.
Tercera generación.	Utilizan mecanismos de ocultación. Requieren de programas especializados para su detección y eliminación. Detectores o scanners que buscan determinadas secuencias de bits en un archivo.
Cuarta generación.	Polimórficos, cada copia es distinta. Requieren de detectores algorítmicos que intentan determinar si una secuencia de bits pudo haber sido producida por el motor de mutación de un virus.

Principales daños causados por virus.	
Bromas	Como el virus ping-pong, ya casi no existen.
Destrucción de información.	El virus borra archivos, sin embargo esto lo delata por lo que no lo hacen regularmente.
Alteración de la información.	Pueden cambiar datos, el daño se ve hasta después, un respaldo reciente no sirve. Los virus se agregan a los archivos para su propagación posterior, por ejemplo, un virus en forma de macro.
Secuestro de la información.	Cifran los archivos de determinada extensión. La llave para el descifrado solo la puede obtener el intruso. Una vez que el virus ha cifrado los archivos, le muestra al usuario las instrucciones para que pueda descifrar sus archivos. Usualmente le pide dinero o le pide que compre algo por internet.
Saturación de recursos.	A veces por accidente o por un mal diseño en los virus, por ejemplo, un virus que genera muchas copias de sí mismo y satura el espacio en disco.
Bloqueo de recursos.	Bloquea el uso de dispositivos como las memorias USB, algunos virus no permiten que se ejecuten herramientas del sistema o bloquea el mismo antivirus.

Programas para pruebas de penetración.

Debido a que estos programas contienen una amplia variedad de ataques, suelen ser usados por los intrusos para entrar a los sistemas informáticos.

Por ejemplo la suite MetaSploit que es muy fácil de usar y se encuentra disponible en Internet.

Caballos de Troya.

Obtiene su nombre por la similitud con la Iliada. En términos de código malicioso, son programas que parecen buenos y que aparentemente realizan una función inofensiva, pero que dentro contienen virus o software espía.
Los caballos de Troya no son considerados virus debido a que no se replican a sí mismos.

Programas espía.
Se trata de código malicioso que tiene por objeto obtener información para después usarla. El ejemplo más común son los keyloggers que capturan los teclazos y así obtienen contraseñas, también pueden recabar información del comportamiento de los usuarios para enviarles propaganda especifica.

Ataques DOS (Denial Of Service).
Son ataques que tienen como fin el negar los recursos del sistema a los usuarios legítimos, es decir, afectar la disponibilidad de los recursos informáticos.
Todos los recursos finitos del sistema son susceptibles a ataques de DOS, por ejemplo, el CPU, el espacio en disco, la memoria, el acceso a la red eléctrica y de datos, etc.
Existe la negación del servicio por inanición del producto y por la sobrecarga del servicio.

No existe forma de evitar los DOS, sin embargo algunas medidas que pueden ayudar a retrasarlos son:

- Deshabilitar servicios que no se usen.
- Habilitar cuotas a los usuarios.
- Particionamiento adecuado de discos y montaje de sistemas de archivos con los parámetros adecuados.
- Monitorear los recursos y establecer patrones de comportamiento.
- Invertir en equipos de redundancia.

Algunas herramientas de DOS son Fapi, Trinoo, TFN y para la detección de DOS se

encuentran Shaft y mstream.

Módulo 8. Seguridad en sistemas operativos.

Sistema Operativo. Es un administrador de recursos (memoria, disco duro, procesador, dispositivos de entrada y salida).

Normas de seguridad de Sistemas Operativos.
Hacer uso de normas y estándares. Organizaciones como la IEEE, ANSI y algunos estándares de facto como Word, Excel, o el puerto Centronics.

En cuestión de seguridad en sistemas operativos existe la norma TCSEC (Trusted Computer System Evaluation Criteria) más conocido como el libro naranja de la serie Rainbow. Dicho libro clasificaba los sistemas operativos de la siguiente forma:

Clasificación de Sistemas Operativos.			
Clase	**Característica**	**Subclase**	**Descripción**
D	Protección mínima.		No pasa las pruebas
C	Protección discrecional.	C1. Protección de seguridad discrecional.	Responsabilizacion por auditoria
		C2. Protección por acceso controlado.	Encapsulamiento de recursos, responsabilizacion logica
B	Protección obligatoria.	B1. Protección por seguridad etiquetada.	Modelo de políticas, etiquetas para sujetos y objetos
		B2. Protección estructurada.	Modelos formales, canales encubiertos, control de la configuración, auditoria.
		B1. Dominios de seguridad.	Vigilancia ineludible y probada, soporte para la administración de seguridad, auditoria segura.
A	Protección verificada.		Documentación y vigilancia de origen a fin.

A pesar de que el libro naranja fue escrito en 1983, contiene principios que no cambian,

por lo que se puede emplear para la comparación de los sistemas operativos.
Además de los niveles de seguridad se necesitan políticas de seguridad, la rendición de cuentas (Accountability) y los mecanismos de seguridad.

Para la elección de los niveles de seguridad se necesita conocer el modo de operación del sistema.

Modos de operación.	
Sistemas dedicados.	Maneja sujetos y objetos del mismo nivel. Se encuentra aislado y su seguridad es primordialmente seguridad física. Prácticamente cualquier sistema puede operar en este modo.
Alto nivel.	Todos los usuarios tienen el más alto nivel de seguridad. Solo da protección mínima entre usuarios. Maneja controles de acceso mínimos a los datos.
Compartamentalizados.	Es un sistema de alto nivel dividido en compartimentos. No todos los usuarios pueden accesar a todos los compartimentos. Protege los datos para que no salgan de su compartimento.
Multinivel.	Sujetos y objetos con varios niveles. Identificación y autenticación de los usuarios. Controla el acceso a los recursos y emplea etiquetas. Tiene rastros de auditoría para determinados eventos. Hay una validación externa de la seguridad del sistema

Principios básicos en la seguridad de Sistemas Operativos:

- Principio de las funciones mínimas necesarias. Se aplica a usuarios aplicaciones y sistemas y establece que se les debe otorgar las menores funciones con las que puedan operar correctamente.
- Instalación pensando en la seguridad. Usualmente la instalación default de los sistemas operativos tienen muchos servicios que no son necesarios y que luego se tienen que deshabilitar, por lo tanto, es recomendable el instalar un sistema deshabilitando los servicios que sabemos no vamos a usar y no instalar los que no estamos seguros para que son.
- Nunca instalar “Todo” el sistema o aplicación.
- Cuando se necesite instalar un servicio, instalar la versión más estable y más segura, por ejemplo, para acceso remoto usar SSH en vez de Telnet.
- Instalar mecanismos adicionales de seguridad como IDS.

Módulo 9. Herramientas y protocolos.

Este módulo tuvo como objetivo dar a conocer algunas herramientas de seguridad, permitiendo relacionar la teoría obtenida en los demás módulos con el funcionamiento de dichas herramientas, además de dar a conocer algunos protocolos de seguridad.

Se realizaron prácticas con Snort (IDS), John the Ripper (Password Cracker), FreeS/WAN (VPN) e IpTables (Firewall), WireShark y TcpDump (Sniffers) y NMAP (scanner de puertos).

Módulo 10. Seguridad en redes y en WEB.

Una red puede verse como una computadora. Dicha computadora es masivamente paralela y los datos y programas estarían dispersos.

Internet.
Es una federación de redes de computadoras que emplean los mismos protocolos. Las redes que conforma Internet están conectadas mediante circuitos telefónicos de alto desempeño.
En Internet hay una diversidad enorme de computadoras, desde supercomputadoras hasta computadoras personales.

Las amenazas principales de Internet son:

- Intercepción de datos en tránsito.
- Acceso a programas remotos.
- Modificación de datos y programas al vuelo.
- Bloqueo de tráfico selecto.
- Denegación de servicio.

- Inserción de una repetición de una secuencia.

Los sistemas operativos incluyen mecanismos de control de acceso para impedir que accesen a sus servicios personas no autorizadas. El sistema más usado es el de santo y seña.

- El usuario tiene que identificarse como un nombre de usuario en el sistema.
- En caso de que el sistema reconozca este nombre se usuario, le solicita el autenticador o autenticadores.

Sin embargo, quien quiera que conozca el nombre de usuario y la contraseña, será considerado por el sistema como el usuario legitimo al que pertenece información confidencial. Si el que accede a esta información no es el usuario real, entonces se está realizando una suplantación o un robo de identidad.

Algunos ataques cibernéticos son:

Ataques Cibernéticos	
Hombre en medio.	El intruso se hace pasar por cada una de las partes, se cifra el trafico del usuario al intruso y del intruso al servidor. El intruso descifra y cifra el trafico que pasa por el obteniendo el trafico en claro.
URL ofuscados.	Ofuscan el nombre del servidor: • Decimal: http://201.34.89.120 • Octal: http://0311.0042.0131.0170 • Hexadecimal: http://0xC9.0x22.0x59.0x78. O codificación de datos de maneras alternas. Unicode, Unicode UTF-8, %hexhex.
Cross Site Scripting.	Cuando se tienen varias ventanas abiertas, todas están mutuamente accesibles, incluyendo las ventanas de otros sitios.
Ataques encubiertos.	Marcos escondidos. Suplantar el contenido de una página. Superposición de imágenes.
Obtención de datos del uso.	Captura de flujos de clicks.
Vulnerabilidades de los clientes.	Uso de la combinación de Internet Explorer con Media Player para ejecución de código. Corrupción de la memoria que se asigna a una aplicación mediante Real Player.

Métodos de defensa en clientes y servidores.	
Clientes	Servidores.

Protección de la computadora.	Autenticación de los servidores.
Correo electrónico más sofisticado.	Verificación de la correspondencia institucional.
Uso de la capacidad de los navegadores.	Vigilancia del dominio.
Correo electrónico firmado.	Servicios de compuertas.
Capacitación y sensibilización de los usuarios.	Servicios administrados.

Intranet.

Es una red que usa la tecnología de Internet en forma local y que se mantiene controlado.

Se emplean para mejorar la comunicación dentro de la empresa, logrando así una mejor productividad.

A diferencia de Internet se establece un perímetro y un dominio de la administración de la seguridad, se elabora una lista de usuarios.

Los requisitos para una Intranet son:

- Confidencialidad.
- Integridad de la información.
- Autenticación de origen.
- Autenticación de destino.
- Autorización de acceso.

Para lograr el control sobre una Intranet se requiere:

- Un perímetro vigilado. Físico y lógico.
- Un solo punto de acceso. Es más fácil controlar solo un punto.
- Vigilancia del estado de los componentes. Por ejemplo SNMP.
- Autorización para uso de diversos servicios. Por ejemplo Kerberos.
- Vigilancia de medios. Cobre, fibra, inalámbricos.

Extranet.

Se trata de dos o más Intranets conectadas a través de Internet.

Responde a la necesidad de empresas distribuidas geográficamente que requieren el intercambio de información entre sus empleados.

Para prevenir el acceso no autorizado entre redes se emplea un cortafuegos (firewall). Dicho equipo examina los paquetes que viajan entre el servidor y el cliente.
La ubicación de los servidores es dentro de la zona desmilitarizada (DMZ). Esta zona se encuentra detrás del cortafuegos, pero aislada la Intranet, permitiendo solo trafico determinado entre la DMZ y la Intranet.

Seguridad en cómputo móvil.
Los problemas con los dispositivos portátiles son:

- Que no se cuenta regularmente con políticas, estándares y prácticas de uso.
- Es difícil lograr la autenticación de los usuarios.
- No se responsabiliza a los usuarios.
- Existe una gran cantidad de pérdidas y robos.
- Usualmente faltan respaldos.
- Bitácoras limitadas.
- Sistemas no acotados.
- Falta del camino confiable.

Redes locales inalámbricas.
Redes ad hoc. Cada computadora tiene una tarjeta y se comunican directamente entre sí.
Redes convencionales. Se comunican con redes cableadas mediante el uso de puntos de acceso que funcionan como ruteadores. El punto de acceso conecta entre si las redes alámbricas e inalámbricas y permite enviar y recibir datos entre clientes alámbricos e inalámbricos.

La admisión a las redes inalámbricas es de la siguiente forma: Todo dispositivo que comparte el secreto de una red inalámbrica se convierte en miembro de esa red.
El punto de acceso y los dispositivos transmiten señales identificadoras que establecen la pertenencia y permiten el enlace.

Cortafuegos (Firewall).

Mecanismo para implementar políticas de seguridad.

Simplifica la administración de la seguridad de una o varias redes.

Ayuda a controlar el acceso de grupos de usuarios a servicios.

NO DEBE SER EL UNICO PUNTO DE FALLA.

Clasificación de Firewalls	
Firewall de aplicación: Funcionan para una red. Trabajan a nivel de capa de aplicación. Son específicos de cada aplicación. Actúan como un intermediario (Proxy). Pueden tener cache. Existen transparentes y no transparentes. Tranparentes: Menos complicados de instalar y el programa cliente no percibe su existencia. No transparente: Se tienen que configurar los clientes.	**Firewall personales:** Solo protegen a un equipo en la red. Usualmente solo filtran puertos. **Firewall de filtrado de paquetes:** Funcionan para una red. Basados en los encabezados de la capa de red y de transporte, también por interfaces. Analizan paquetes de múltiples protocolos. Normalmente transparentes al usuario.

El esquema de distribución de grupos, servicios y firewalls depende de cada organización. Para definir un esquema se necesita:

Identificar las personas, los servicios, los equipos y las redes actuales y se agrupan.

Después se definen las políticas:

- Para cada grupo de personas se define una red.
    - Para cada red se definen los servicios y destinos validos.
        - Para cada servicio se identifican horarios y reglas especiales.(filtros, autenticación, NAT, etc.)

Para las políticas existen dos posturas:

- Todo lo que no está expresamente prohibido está permitido.
- Todo lo que no está expresamente permitido está prohibido.

Algunos componentes externos al firewall que deben cuidarse son:

- Usuarios.

- Seguridad física.
- UPS.
- Cables de poder.
- Aplicaciones.
- Protocolos de ruteo.
- Hubs, switches, ruteadores, cableado.
- IDS y otros firewalls.

Módulo 11. Seguridad en bases de datos.

Los requerimientos básicos en que debe tener una base de datos en cuestión de seguridad son:

- Integridad física de la BD. Se logra mediante los sistemas de respaldos y recuperación.
- Integridad lógica de la BD. El uso de log o journal.
- Integridad semántica. Asegurar la consistencia lógica de datos modificados por valores de datos dentro de conjuntos de datos permitidos.
- Integridad operacional. Asegurar la consistencia lógica de datos durante transacciones concurrentes. Existe un módulo llamado manejador de concurrencia.
- Registro de eventos y de auditoría. Habilitar el registro de los accesos a los datos para operaciones de lectura escritura, se puede emplear un analizador de logs y elegir un nivel alto de detalle.
- Integridad de datos. Protección contra la modificación impropia de datos y contra la modificación no autorizada de los datos.
- Control de acceso a la BD.
- Autenticación de los usuarios.

Amenazas para las BD.

- Accidentes naturales, errores o bugs de software, errores humanos.
- Uso malicioso de las BD.
- Fallas de hardware o software que corrompan datos.

La autenticación de los usuarios puede realizarse por el sistema operativo o por el manejador de base de datos (DBMS), sin embargo, si se elige la autenticación por sistema operativo, se restringirá la entrada a la BD ya que todos los sistemas deben ser compatibles con el sistema operativo de la BD.

Tipos de integridad de datos.	
Dominio	Requiere que un conjunto de valores sean validos para una columna específica. Se implementa mediante la verificación de validez y se puede forzar restringiendo el tipo de datos, formato o rango de valores permitidos en una columna. Verificación del valor nulo. Verificación del valor por omisión (default). Verificación de valor (check).
Entidad	Requiere que todos los renglones de una tabla tengan un identificador único. El valor de una llave primaria puede cambiarse del nivel de integridad requerido entre la llave primaria y otras tablas. Llave primaria. Restricciones UNIQUE.
Referencial	Asegura que las relaciones entre la llave primaria (en una tabla referenciada) y las llaves foráneas (en una tabla referenciante) siempre se mantenga. Un renglón en una tabla referenciada no puede ser borrado y si una llave foránea hace referencia a ese renglón, tampoco la llave puede modificarse.

Algunas de las formas para forzar la integridad de datos son mediante:

- Integridad declarativa. La operación que viola la restricción no se efectúa, se aborta. La violación de restricciones produce una excepción que debe ser atrapada por la aplicación que generó la excepción.
- Restricciones de llave.
- Valores por omisión.

- Integridad procedimental. Ofrece mecanismos de control de integridad de datos más complejos que los declarativos. Este tipo de control es reactivo a diferencia del

declarativo que es proactivo. El lenguaje es dependiente del DBMS. Pueden propagar en cascada los cambios en una BD.

- Criterios definidos en scripts.
- Triggers (desencadenadores) y procedimientos almacenados.

Transacción. Conjunto de operaciones básicas en una BD vista como una sola entidad. Garantiza ser atómica (indivisible) para propósitos de recuperación.
Inicia con BEGIN TRANSACTION y termina con COMMIT (terminación normal) o ABORT (terminación a normal).

Propiedades de las transacciones en una Base de Datos.	
Atomicidad.	Es un paquete indivisible. No se puede ejecutar solo un parte.
Consistencia.	Solo modifican los datos de sus instrucciones.
Aislamiento.	Las transacciones concurrentes no interfieren entre sí.
Durabilidad.	Los datos no se modifican en el transcurso del tiempo.

Si se emplean bloqueos directamente en la base de datos, se pueden producir dead locks, aunque algunos emplean timeout para la liberación de bloqueos, sin embargo, es preferible usar un nivel de aislamiento como atributo de una transacción.

Niveles de aislamiento de transacciones.	
Read uncommited.	No resuelve ningún problema.
Read commited.	Resuelve el problema de lectura sucia.
Repetible read.	Resuelve lectura no repetible.
Serializable.	Resuelve fantasmas.

Casi todas los DBMS usan el nivel de aislamiento Read Commited debido a que los otros errores son poco comunes. Con el nivel serializable la base de datos tiene un rendimiento muy pobre.

Inferencia en BD.

La inferencia es la posibilidad de obtener información confidencial a partir de datos no confidenciales.

Practicas recomendadas.

- Restringir el acceso físico al servidor de bases de datos.
- Establecer mecanismos de seguridad al sistema operativo sobre el que está instalado el DBMS.
- En caso de que sea un servidor con sistema operativo Windows, instalar un antivirus y mantenerlo actualizado.
- En un ambiente Web, instalar el DBMS en un servidor distinto al servidor Web.
- Aislar mediante un firewall al servidor mediante filtrado de paquetes a los puertos que usa el DBMS.
- En caso de ser necesario, instalar un NIDS especializado en BD.
- Cambiar contraseñas default y colocar contraseñas fuertes.
- Eliminar cuentas demo.
- Parchar el DBMS.
- No permitir que las aplicaciones consulten o manipulen directamente la base de datos mediante SELECT, INSERT, UPDATE o DELETE. Emplear procedimientos almacenados.
- En las aplicaciones restringir la ejecuciones de instrucciones dinámico.
- Impedir que las aplicaciones acepten instrucciones SQL de los usuarios y las ejecuten sobre la base de datos.
- Consultar datos mediante vistas en lugar de otorgarles acceso a las tablas de la base de datos.
- Evitar reporteadores que permitan la construcción de SQL.
- Cifrar la información sensible.
- Habilitar la auditoria de acceso al sistema operativo y al servidor de base de datos. Revisar el registro de auditoría buscando eventos fallidos.
- Monitorear y proteger los archivos de logs.
- Definir y aplicar una política de respaldo periódico, almacenar los medios de respaldo en un lugar seguro y realizar verificación de los respaldos.

Módulo 12. Buenas prácticas y tendencias futuras.

Este módulo fue un repaso de los anteriores módulos, además incluyo temas de vanguardia en seguridad informática.

La NSA (National Security Agency) está proponiendo el uso de curvas elípticas para cifrado simétrico, asimétrico y hash. Lo anterior debido a que el número de bits usado en curvas elípticas es menor al de RSA.

Para poder saber cómo estamos en cuestiones de seguridad informática, es necesario tener un punto de comparación, para esto se emplea el ISO.

Se aplican cuestionarios sobre cada área de la seguridad informática, existen cuestionarios genéricos, sin embargo, el responsable de seguridad tiene que adaptar el cuestionario al entorno en el cual se está haciendo el análisis.

En el caso de que se use software como Calius o Proteus, se le proporciona como entrada los resultados de los cuestionarios aplicados y estos dan como resultado reportes basados en el ISO.

Sin un cuestionario es llenado de forma errónea, va a contaminar e diagnostico, se pueden emplear los reporteadores para graficar el incumplimiento.

Después de tener el diagnostico, este se cifra y se entrega, además se hace hincapié en el capítulo que requiere prioridad.

Las buenas prácticas son recomendaciones, no son obligatorias ni validas en todos lados y solo 4 buenas prácticas son elementales.

1. Desarrollo de políticas de seguridad.

2. Clasificación de la información.
3. Cifrado de información altamente clasificada.
4. Autenticación fuerte para control de acceso a los sistemas.

Buenas Prácticas.	
Políticas de seguridad. Establecer políticas de seguridad que sean comprensivas. Desarrollar un documento de políticas de seguridad de la información. Revisar las políticas de seguridad de la información. Actualizar el documento.	**Seguridad de la corporación.** Establecer organización de seguridad interna. Crear un comité activo para la seguridad de la información dentro de la corporación. Coordinar implementación de la seguridad de la información. Crear un comité interdisciplinario. Asignar responsables de la seguridad de la información. Establecer proceso de autorización para la actualización de la corporación. Usar acuerdos de confidencialidad para proteger la información. Mantener relaciones con otras organizaciones.
Activos organizacionales. Después del análisis de riesgos se establece el responsable de los activos organizacionales. Realizar un inventario de los activos. Clasificar la información. Usar procedimientos de manejo y etiquetado. Un medio que respalda información de varios niveles de clasificación debe ser clasificado con el nivel más alto.	**Seguridad física y ambiental.** Usar perímetros de seguridad física para proteger áreas sensibles. Uso de áreas de seguridad para proteger aplicaciones Usar controles de entrada físicos para proteger áreas sensibles. Aislar y controlar puntos de acceso público. Usar guías de trabajo para proteger áreas seguras. Asegurar oficinas, cuartos y aplicaciones de amenazas naturales.
Seguridad de recursos humanos. *Antes de emplear* Definir roles y responsabilidades de seguridad. Verificar los antecedentes de todo el personal nuevo. Usar contratos que incluyan clausulas de confidencialidad, entrega de productos y de operación de los productos. *Durante el empleo* Acordar con los jefes las medidas de seguridad. Programas de entrenamiento de seguridad de la información. Crear procesos disciplinarios para infracciones de seguridad. *Al término del empleo.* Asignar responsables para terminaciones o reasignación. Asegurarse de que los activos sean regresados. Remover derechos de acceso a la información.	**Proteger equipamiento.** Usar equipo y estrategias de protección. Asegurarse que las utilerías de soporte son confiables. Asegurar cables de poder y comunicaciones, no deben ser visibles en su trayecto. Mantenimiento al equipo de la corporación. Protección al equipo fuera del SITE de computo. Controlar equipo de desecho y reuso. Control de uso de los activos fuera del SITE.
Monitoreo de información. Establecer y mantener los registros de auditora. Monitorear las bitácoras de las aplicaciones. Proteger los sistemas de logs así como los archivos de logs. Registrar actividades del administrador de sistemas. Registrar errores. Sincronizar la hora en todos los sistemas.	**Comunicaciones y operaciones.** Establecer procedimientos y responsables. Documentar los procedimientos de operación. No tomar datos reales para el ambiente de desarrollo ya que la seguridad es menor. Segregar obligaciones y responsabilidades. Separar el ambiente de desarrollo y el de aplicación. Control de cambios para aplicaciones y sistemas.

Buenas prácticas	
Protección de redes. Establecer controles de seguridad de redes. Controlar a los proveedores de servicio. Uso de firewalls, NIDS, monitores de red, segmentación de la red.	**Control de manipulación de medios.** Manipular discos removibles. Transportación segura de medios físicos. Control de almacenaje mediante inventario de dispositivos y fechas de almacenaje
Control de acceso a servicios de redes. Definir políticas de uso de la red. Conexiones remotas solo por canales cifrados. Control de acceso para configurar y monitorear puertos. Restringir redes compartidas.	**Establecer procedimientos de respaldo.** Respaldar información y software. Procedimientos de frecuencia. Procedimientos de prueba de recuperación. Checar vida útil del medio. Copia de respaldos fuera de sitio para información critica.
Establecer controles de ruteo de red. Usar herramientas como Nmap, Nessus, etc para evaluar la seguridad de la red. Nunca enviar contraseñas por canales promiscuos	**Control de acceso.** Manejo de derechos de acceso. Establecer manejo de contraseñas. Establecer privilegios y derechos de acceso de usuario. Proponer buenas prácticas de acceso. Exhortar a los usuarios a proteger sus equipos y sus contraseñas
Control de acceso a aplicaciones e información. Restringir acceso por usuarios y personal de soporte. Aislar aplicaciones sensitivas.	
Controlar procesos de desarrollo y soporte. Establecer procedimientos formales de control de cambios. Restringir cambios de software. Control de desarrollo de software por terceros.	**Control de acceso a los sistemas operativos.** Establecer procedimientos seguros de logon. Identificar y autenticar a todos los usuarios. Establecer un sistema de manejo de contraseñas. Controlar el uso de las herramientas del sistema. Usar límites de sesión para proteger la información. Restringir los tiempos de conexión a áreas de alto riesgo.
Uso de controles criptográficos para proteger la información. Implementar una política de uso de controles criptográficos. Establecer un sistema de manejo seguro de llaves.	
Control de outsourcing. Control de entregas. Manejo de acuerdos. Monitorear avances. Control de cambios.	**Establecer manejo de vulnerabilidades.** Manejo de incidentes de seguridad. Reporte de eventos de seguridad o debilidades. Reportar debilidades en sistemas y servicios.

Conclusiones.

El primer trabajo que tuve fue en el mismo lugar en donde realice mi servicio social, y no solo yo me quede a trabajar, también otros compañeros que estaban estudiando Ingeniería en Computación en la ENEP Aragón (ahora FES).

Allí conocí a personas que después me invitaron a formar parte en diversos proyectos. Lo anterior debido a que fui considerado como un elemento útil para buena realización de proyectos informáticos. En ninguno de los empleos que he tenido realicé entrevista de trabajo, esto debido a que previamente conocían mi trabajo y me han tenido la confianza para involucrarme en sus proyectos.

Creo sin duda alguna que la educación que recibí durante mi estancia en esta escuela, me ha ayudado a resolver los problemas con los que me he enfrentado en mi vida laboral, ya que si bien en cierto, no se puede preparar a los alumnos de ingeniería en computación para toda la diversidad de empleos involucrados con las tecnologías de la información, si se nos prepara para ser autodidactas, para evaluar y desarrollar nuevas herramientas, para formar grupos interdisciplinarios y para desarrollar proyectos que mejoren nuestros respectivos lugares de trabajo, además, me han enseñado los valores de la constancia, responsabilidad y deseos de superación.

Afortunadamente durante mi experiencia laboral he tenido como jefes a personas que me han tenido paciencia y que me han dado las facilidades para tomar cursos ya sea dentro de la dependencia o fuera de esta, además, han tomado en cuenta mis opiniones en los proyectos informáticos en los que he participado, demostrando la confianza que se me tiene.

Por otro lado, me es muy gratificante el hecho de que he podido resolver la mayoría de los problemas por mí mismo, y por tal motivo recibir el reconocimiento de mis jefes y mis compañeros de trabajo, además me es gratificante el enseñar a las demás personas involucradas con las Tecnologías de la Información.

A pesar de que soy una persona que le gusta su trabajo y que considero que lo realizo adecuadamente, se también que esta carrera es de capacitación continua, por tal motivo, es una de mis principales prioridades el seguirme capacitando. Actualmente estoy cursando la Maestría en Ingeniería en Seguridad y Tecnologías de la Información en el Instituto Politécnico Nacional y una vez terminada, pretendo seguirme capacitando en Informática Médica.

Finalmente, como lo he escrito en la introducción, me considero un profesionista formado gracias al apoyo de muchas personas, a las cuales no tengo forma de agradecerles, empezando por mi familia, mis profesores y compañeros estudiantes que me inculcaron el gusto por la lectura y la computación, además de mis jefes y compañeros de trabajo que me siguen incentivando para que me siga capacitando.

Glosario.

ADMINISTRATIVO: Sistema que administra la información no medica (nivel socioeconómico, dirección, etc.) de los pacientes del Instituto.

Backbone: Parte principal de una red de datos compuesta por equipos y enlaces robustos.

Bugs: Errores de código sin mala intención que pueden ser explotados por un ente malicioso.

DBA: Data Base Administrator: Administrador de la Base de Datos.

DDS: Digital Data Storage: tipo de cinta para realizar respaldos.

DICOM: Digital Imaging and COmmunication in Medicine. Estándar para distribuir y ver imágenes medicas sin importar su origen.

Dirección IP: Numero que identifica a una computadora en una red. Se compone de 32 bits.

Dirección MAC: Media Access Control. Numero que identifica a una tarjeta de red. Se compone de 48 bits.

DTC: Data communications and Terminal Controlers, equipos de comunicacion de datos para terminales tontas.

HIS: Hospitalary Information System. Sistema de Información Hospitalaria. En el Instituto eta compuesto por el sistema SIPAM y el sistema ADMINSTRATIVO.

Kernel: Núcleo del sistema operativo, es el que provee la interacción con el hardware.

LAN: Local Area Network. Red de área local, red pequeña limitada por extensión geográfica.

Linux: Sistema operativo similar a UNIX creado por Linux Trovals. Muy popular debido a que su código fuente se distribuye gratuitamente.

NFS: Network File System. Sistema de archivos en red, se usa para compartir todo un sistema de archivos entre varios equipos conectados en una red.

PACS: Picture Archiving and Communication System. Sistema de comunicación y archivado de imágenes. Sistema de computo para el resguardo, recopilación y distribución de imágenes medicas.

Proxy: Firewall de aplicación, se ubica en la capa 7 del modelo OSI, puede ver el contenido de los paquetes y filtrarlos.

RAM: Random Access Memory. Memoria de acceso aleatorio. Espacio en donde el sistema operativo guarda información temporal.

RIS: Radiologic Information System. Sistema de información radiológica. Sistema de administración de información radiológica referente al paciente, es complemento de un sistema PACS.

RISC: Reduced Instruction Set Computer. Forma en la cual un procesador maneja las instrucciones.

Root: Cuenta del sistema para administrar sistemas operativos Linux y UNIX.

Rootkit: Conjunto de herramientas para conseguir el acceso al sistema comprometido después de una ataque exitoso.

SIPAM: SIstema del Paciente AMbulatorio. Sistema que administra la información Medica de los pacientes del Instituto.

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

UNIX: Sistema operativo creado en la década de los 70, Debido a su buen diseño se usa principalmente para servidores.

VIPA: Versatile Intelligent Patient Archive. Sistema de respaldo del sistema PACS, también sirve para almacenar información diferente al estándar DICOM.

VPN: Virtual Private Network. Red privada virtual. Permite la comunicación privada a través de una red pública entre dos segmentos controlados de una red.