UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

CARRERA DE SISTEMAS INFORMATICOS

ANALISIS DE VULNERABILIDADES FISICAS Y DE ACCESO LOGICO AL CENTRO DE COMPUTO DE LA CLINICA HUMANITARIA FUNDACION PABLO JARAMILLO C.

Estudiante:

Tcnlg. Miguel Juela León.

TUTOR

Ing. Pablo Tamayo

Cuenca Ecuador.

Noviembre 2011

UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS

CERTIFICA:

Que el presente trabajo de investigación “Análisis De Vulnerabilidades Físicas Y De Acceso Lógico Al Centro De Cómputo De La Clínica Humanitaria Fundación Pablo Jaramillo C.”, realizado por el Tecnólogo Miguel Juela León, egresado de la facultad de Ingeniería de Sistemas, se ajusta a los requerimientos técnico-metodológico y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación.

Cuenca, 29 de Noviembre de 2011.

_____

Ing. Pablo Tamayo.
DIRECTOR DE TESIS.

UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS

Acta de sesión de derechos

Yo, Tcnlg. Miguel Juela León, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: "Forma parte del Patrimoniode la Universidad la propiedad intelectual de las investigaciones,trabajos científicos o técnicos y tesis de grado que se realicen através, o con el apoyo financiero, académico o institucional(operativo) de la Universidad"

Cuenca, Noviembre 7 del 2011

_____

Tcnlg. Miguel Juela León

UNIVERSIDAD TECNOLOGICA ISRAEL

FACULTAD DE SISTEMAS

CERTIFICADO DE AUTORIA

Los contenidos, argumentos, exposiciones, conclusiones son de responsabilidad del autor.

_____

Tcnlg. Miguel Juela León

DEDICATORIA

El presente trabajo de graduación está dedicado principalmente a Dios por bendecirme todos los días con todo lo necesario para poder seguir adelante en todos los bueno y malos momentos, a aquellas personas que día a día me brindaron su apoyo, amor y comprensión para poder llegar a ésta etapa tan anhelada en mi vida, ellas son mis hijas Ma. Emilia y Daniela Michelle, a mi esposa por su apoyo y comprensión y sobre todo a mi madre que se sacrificó por mucho tiempo por mí y a mí hermano que sea un ejemplo a mejorar,

AGRADECIMIENTO

Este largo camino de preparación no hubiera sido posible gracias a cada uno de los familiares, amigos,conocidos y la institución en la que laboro y que confió en mí la Clínica Humanitaria Fundación Pablo Jaramillo C., en este punto de mi vida es necesario hacer una pausa y decir gracias a cada una de ellas al igual que a los profesores de la Universidad Israel la que me albergo por varios años y en donde me brindaron el conocimiento, la experiencia y amistad, al Ing. Pablo Tamayo quien como tutor me apoyo con su experiencia, tiempo y amistad sincera para la culminación de este trabajo.

RESUMEN

Cada día la implementación de los centros de cómputo tienden a una mayor complejidad debido al grado de seguridades y de tecnología que en ella se ejercen, estos lugares son considerados áreas críticas, considerando que en este centro se gestiona o se almacena la información de una institución, teniendo en cuenta que cada institución considera a su información como el activo de su empresa es necesario tomar todas las medidas que lleven a precautelar ésta información.

El presente trabajo ha sido realizado en el centro de cómputo de la Clínica Humanitaria Fundación Pablo Jaramillo C. el mismo que tiene por objeto realizar un análisis de las vulnerabilidades de acceso físico y lógico con la finalidad de ayudar a implementar políticas que permitan mitigar estos hallazgos.

La información recabada con relación al análisis es particular a la Clínica Humanitaria y las conclusiones y recomendaciones que en ella se determinan son ajustadas a su realidad.

SUMMARY

Every daythe implementation ofdata centerstend to be morecomplex dueto the degree ofassuranceand technology thatitis exercised, these places are consideredcritical areas,considering that in thiscenter is managedor storedinformation froman institution, taking into accounteach institutionconsiders itsinformation asan assetof your company isnecessary to take allprecautionarymeasures that lead tothis information.

Thiswork has beenperformed inthe datacenterFoundationHumanitarianPabloJaramilloC.the sameis to conductan analysisof the vulnerabilities ofphysical accessand logicalin order tohelp implementpolicies tomitigate thesefindings.The information collectedin relation to theparticularanalysis istheHumanitarianClinicand the conclusions andrecommendationsthereinare adjustedtodeterminetheir reality.

TABLA DE CONTENIDO

LISTA DE CUADROS Y GRÁFICOS

LISTA DE ANEXOS

Documento entregable a la Clínica Humanitaria Fundación Pablo Jaramillo

CAPÍTULO I

1. INTRODUCCION

1.1. Tema de investigación

Análisis de vulnerabilidades físicas y de acceso lógico al centro de cómputo de la Clínica Humanitaria Fundación Pablo Jaramillo C.

1.2. Planteamiento del problema

1.2.1. Antecedentes

Cada día la implementación de los centros de cómputo tienden a una mayor complejidad debido al grado de seguridades y de tecnología que en ella se ejercen, estos lugares son considerados áreas críticas o focos sensibles a ataques, considerando que en este centro se gestiona o se almacena la información de una institución, el procesar la información de una empresa nos indica que allí se almacena información de todo tipo propia de la empresa ya que si tenemos en cuenta que todo está automatizado y que toda la información se encuentra digitalizada tenemos que esa información es la vida de la empresa y que la perdida de la misma llega a causar serios problemas tanto de gestión interna como legales y de funcionamiento de la empresa en base a estas premisas la información de las empresas o instituciones son consideradas como el activo fijo de valor incalculable.

Nos enfrentamos a una situación en la que la seguridad se considera un complemento irrelevante y por lo tanto es usual omitirla en el montaje de los centros, y añadirla más tarde o simplemente considerarla como un servicio externo que será suministrado por otros. Esto tiene unas consecuencias muy negativas en la seguridad de dichos centros que están funcionando, y ha llevado a un creciente escepticismo por parte de los empresarios que observan que su información se

encuentre amenazado ya que hay un gran abismo entre la seguridad informática y la realidad en nuestro país.

En el año 1994 los delitos cometidos tenían la peculiaridad de ser descubiertos en un 95% de forma casual. Podemos citar a los principales delitos hechos por computadora o por medio de computadoras son:

- ✓ Fraudes
- ✓ Falsificación
- ✓ Venta de información

Entre los hechos criminales más famosos en los E.E.U.U. están:

✓ El caso del Banco Wells Fargo donde se evidencio que la protección de archivos erainadecuada, cuyo error costo USD 21.3 millones.

✓ El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.

✓ El caso de un muchacho de 15 años que entrando a la computadora de la Universidad de Berkeley en California destruyo gran cantidad de archivos.

✓ También se menciona el caso de un estudiante de una escuela que ingreso a una red canadiense con un procedimiento de admirable sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomo el control de una embotelladora de Canadá.

✓ También el caso del empleado que vendió la lista de clientes de una compañía de venta de libros, lo que causo una pérdida de USD 3 millones.

Casos en los cuales se realizaron estudios de seguridad Informática

Los delitos cometidos utilizando una computadora han crecido en tamaño, forma y variedad.

1.2.2. Diagnóstico o planteamiento de la problemática general

1.2.2.1. Causas

Cada empresa tiene como política el mantener como acceso a su sistema informático el uso de claves, sin embargo los usuarios no cuentan con la capacitación adecuada para precautelar su clave de acceso.

El libre acceso al centro de cómputo y la manipulación de las estaciones de trabajo por personas ajenas a la institución por falta de políticas de seguridad.

Las redes internas de las empresas se pueden definir como redes hibridas por la comunicación que necesitan establecer de manera privada pero entre sitios distantes, en donde los accesos por medios guiados no son factibles o la movilidad así lo requiere.

Los host implementados en una red cuentan con seguridades propias que permiten una administración e implementación de políticas que mejoran la seguridad en el tráfico de datos pero estas configuraciones no siempre se encuentran activadas o configuradas adecuadamente.

1.2.2.2. Efectos

Al no contar con una cultura de seguridad informática los usuarios se vuelve una de las vulnerabilidades más explotadas por los intrusos que desea conocer hurtar o destruir la información que posee la institución.

El no controlar el acceso al centro de cómputo permitirá que las personas no autorizadas logren hacer daño de manera directa a la información albergada, al igual que por una estación de trabajo que no cuenta con los permisos adecuados.

Las vulnerabilidades se hacen evidentes, al no contar con políticas bien definidas para los accesos de los equipos que necesariamente deben pertenecer a la red y al ser detectada por intrusos que están al asecho de los descuidos de quien

implementa estos host sin seguridad se convierte en un punto de acceso para los intrusos que pretenden obtener información de una manera ilícita y con fines negativos.

1.2.2.3. Pronóstico

El capacitar a cada usuario que se encuentra con permiso asignados al sistema al igual que la administración de las claves que tengan un vencimiento en tiempos definidos los mismos que permitirán que cada usuario realice de manera forzada el cambio de su clave.

Se pretende realizar accesos no permitidos con herramientas de hacking las mismas que nos permitirá obtener el grado de vulnerabilidad que son sujetos los equipos o host de la red

Se verificara quienes tienen acceso al centro de cómputo y cuál es la necesidad para el acceso al mismo, y el trabajo específico que deben realizan.

1.2.2.4. Control del pronóstico

Cada usuario debe estar en la capacidad de gestionar la seguridad de su clave al igual que su host de acceso a la red teniendo presente que él es parte de la custodia que se pretende dar a la información.

El determinar las vulnerabilidades que los host de la red corporativa son sujetos nos servirá para determinar el grado de vulnerabilidad y que tipo de políticas de seguridad se deben implementar para contrarrestarlas.

Es de vital importancia otorgará rangos y permisos que deben tener cada persona que accede a centro al igual que la negación de acceso a personas ajenas al centro.

1.2.3. Formulación de la problemática específica

1.2.3.1. Problema principal

¿Cómo verificará la seguridad de acceso físico y lógico al centro de cómputo de la Clínica Humanitaria Fundación Pablo Jaramillo C.?

1.2.3.2. Problemas secundarios

¿Los permisos de acceso al sistema informático tienen un control?

¿Los puntos de acceso a la red alámbrica e inalámbrica se encuentran controladas?

¿Cómo se controla el acceso por roles que tiene cada usuario a la BD del sistema informático?

1.2.4. Objetivos

1.2.4.1. Objetivo General

Análisis de vulnerabilidades físicas y de acceso lógico al centro de cómputo de la Clínica Humanitaria Fundación Pablo Jaramillo C, cuando se accede a la BD del Sistema Informático debido a que la Clínica Humanitaria al ser una entidad de salud en la que toda su información se encuentra gestionada mediante un software y la información procesada se almacena en una base de datos y teniendo en cuenta que existen 140 usuarios habilitados para acceder al sistema, se genera un problema por parte de los usuarios al momento de gestionar la seguridad de su clave,

1.2.4.2. Objetivos Específicos

- ✓ I Marco teórico.

- ✓ II Investigar al acceso físico y lógico al centro de cómputo cuando se accede a la BD del Sistema Informático.
- ✓ III Generar políticas de acceso lógico al sistema médico informático de acuerdo a cada uno de los roles de los usuarios.
- ✓ III Establecer políticas que permitan gestionar los rangos de seguridad de acceso físico al centro de cómputo por parte del o los administradores de dicho centro.

1.2.5. Justificación

1.2.5.1. Teórica

Los centros de cómputo al ser los lugares en el que reposa y procesa gran cantidad de información de las empresas es el lugar en el que la seguridad para éste activo tan preciado de la institución se debe brindar, sin embargo al realizar un rápido análisis del medio, podríamos decir que las políticas de seguridad en mayor medida se han implementado a nivel de Bancos y de algunas corporaciones en las que ya han sufrido un intrusión de alguna persona no autorizada y los resultados han sido de pérdidas económicas cuantiosas, es por esa razón que en la actualidad cada empresa que maneja su centro de cómputo con información sensible se ve en la necesidad de implementar políticas y normas de seguridad.

La implementación de dichas normas o políticas de seguridad permiten que la información mantenga los conceptos de seguridad que son integridad, privacidad y disponibilidad, el poder garantizar que estos conceptos se cumplan en el centro de cómputo conlleva de tiempo, esfuerzo y de un plan que sea sostenible en el tiempo, al igual que sea actualizado y revisado a lo largo del periodo en el que se encuentra vigente, ya que de esta manera estaremos garantizando que cada una de las políticas definidas en un inicio se mantenga acorde a las necesidades y

cambios que se produzcan a lo largo del tiempo en dicho centro, debemos estar convencidos que la tecnología no se detiene sino que por el contrario a cada instante se encuentra transformándose y por ende un centro de cómputo se encuentra en un proceso constante de actualización e innovación tanto tecnológicamente como en medidas de seguridad.

1.2.5.2. Metodológica

El propósito de realizar el análisis de las vulnerabilidades de acceso físico al centro de cómputo es con el fin de poder contrarrestar los errores que se generan al momento de que una clave de acceso es compartida o no se tiene la precaución de cerrar la sesión en la que se encuentra trabajando, de igual manera la impacto que tiene en la información manipulado incorrectamente.

Es necesario realizar inicialmente un proceso de revisión de los usuarios que se encuentran dados de alta en el sistema, al igual que cada uno de sus roles asignados mediante las claves de acceso y si su perfil se encuentra alineado con los permisos o roles otorgados en el sistema para la manipulación de la información.

1.2.5.3. Práctica

En necesario realizar un correcto análisis de los usuarios que se encuentran dados de alta en el sistema con roles de acceso sobre la base de datos y cuál es el trabajo que se encuentran desarrollando con el sistema informático. Es necesario conocer si el sistema informático cuenta con controles de modificación de datos los cuales nos permitirán conocer cuáles son los registros modificados erradamente.

1.2.6. Marco de referencia

1.2.6.1. Marco teórico

La seguridad informática incluye actividades continuas para monitorear el cumplimiento o no de las políticas a través de métodos formales e informales y el reporte de las deficiencias encontradas

Entendemos por seguridad informática el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, confidencialidad y disponibilidad, considerando también que la seguridad de un centro de cómputo se da cuando hay confianza en él mismo, el comportamiento del software es el esperado y la información almacenada se encuentra Inalterada y accesible, las acciones, herramientas y dispositivos con el objetivo de mantener la integridad, confidencialidad y disponibilidad de la información.

1.2.6.2. Marco espacial

El lugar en el que se va a realizar el proyecto es en el centro de cómputo de la Clínica Humanitaria Fundación Pablo Jaramillo C.

1.2.6.3. Marco temporal

El tiempo que se empleará en desarrollar el tema será de seis semanas tiempo en el cual se realizará el análisis de vulnerabilidades y las posibles soluciones que se deban implementar.

1.2.7. Metodología y cronograma

METODOLOGIA DE ANALISIS DE RIESGO

1.2.7.1. Estudio inicial.- Es el establecer los colaboradores, determinar el lugar informático en el que se va a llevar a cabo el estudio, con el fin de conocer el área es necesario diseñar un check list para obtener información de importancia

del centro lo que nos permitirá realizar una evaluación inicial verificar los manuales de políticas y reglamentos,

1.2.7.2. Procedimientos y técnicas de auditoria Existen objetivos de control y procedimientos de auditoria que después de evaluar los riesgos es necesario identificar las fortalezas y debilidades en los controles existentes basados en la información recopilada para posteriormente generar el correspondiente informe el mismo que debe ser redactado de manera objetiva para la gerencia, la misma que debe tener la disponibilidad para implementar los correctivos necesarios al igual que mantener las revisiones periódicas de los seguimientos emprendidos.

1.2.7.3. Evaluación de Riesgo.- La evaluación de riesgos determina las vulnerabilidades amenazas y riesgos para generar un plan de controles que contemplen los criterios de un centro de cómputo seguro mediante los parámetros de disponibilidad, confidencialidad e integridad de la información, teniendo en cuenta los siguientes puntos:

- **La probabilidad de amenaza**
- **El impacto sobre el centro en base a los parámetros de disponibilidad, confidencialidad e integridad de la información.**

1.2.7.4. Determinación de la probabilidad.- Es necesario tomar en cuenta los siguientes parámetros para determinar la probabilidad que ocurra un evento

- Origen de la Amenaza
- Causa de la vulnerabilidad.

Se deben clasificar las probabilidades de que una vulnerabilidad potencial sea explotada por una fuente de amenaza en alta, media-alta, media, media-baja y baja.

MATRIZ DE CALIFICACION DE VULNERABILIDADES	
Nivel	**Definición**
Alta=5	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo.
Media-Alta=4	La amenaza está fundamentada y es posible.
Media=3	La amenaza es posible.
Media-Baja = 2	La amenaza no posee la suficiente capacidad.
Baja = 1	La amenaza no posee la suficiente motivación y capacidad.

1.2.7.5. Numero de ocurrencias del evento en un periodo.- Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de información, modificación de datos, utilizamos información obtenida de ciertas publicaciones tecnológicas con relación similar a los eventos que se desea estudiar. De esta manera se define una escala en la cual, a una probabilidad alta, le asignamos el valor P=5, para una probabilidad media le asignamos el valor P=3 y por último para una probabilidad baja le asignamos el valor P=1, esta asignación se define en proporción directa al número de veces que el evento puede ocurrir en un periodo preestablecido. Para el caso P=5 se considera que ocurre al menos dos veces al año.

1.2.7.6. Identificación de Vulnerabilidades.- Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se utilizan herramientas como listas de verificación y herramientas de software que determinen las vulnerabilidades.

Seguridad en las aplicaciones Críticas se define las aplicaciones que son críticas para la organización y por cada una de ellas se obtendrá una matriz de riesgo. Es importante considerar que las aplicaciones están soportadas por: Sistemas operativos, hardware servidor, redes LAN y WAN, y el Centro de cómputo.

1.2.7.7. Análisis del impacto y el factor de riesgo. El próximo paso en la metodología que estamos describiendo, es poder determinar el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, para ello se deben considerar los siguientes aspectos

- Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.
- La importancia crítica de los datos y el sistema (importancia a la organización).
- Sensibilidad de los datos y el sistema.

1.2.7.8. Identificación de Controles En esta fase se evaluarán las conclusiones de la valoración y la matriz de riesgo con el fin de identificar los controles que mitiguen los riesgos encontrados.

1.2.7.9. Definición de Políticas.- Las Políticas de seguridad dependen de la cultura de la organización. Por esta razón las políticas y procedimientos deben estar hechos a la medida, según los requerimientos específicos de cada organización. Para la definición de las políticas y procedimientos se realiza un

proceso de validación en conjunto con la organización con el fin de generar políticas y procedimientos que se ajusten a esta. Como punto de partida para la definición de las políticas se tendrá como referencia el análisis de riesgo realizado.

1.2.7.10. Alcance de las Políticas.-

Seguridad en la Organización

- Roles y Responsabilidades de Seguridad de la Información
- Políticas para el manejo de la información.

Clasificación de la Información

- Importancia de la información según la organización

Administración de las operaciones de cómputo y comunicaciones

- Políticas sobre el uso del correo electrónico
- Políticas sobre el uso de clave de acceso.
- Políticas sobre el uso de recursos.

1.2.7.11. DEFINICION DE ESTANDARES.- Es la definición cuantitativa o cualitativa de un valor o parámetro determinado que puede estar incluido en una política o procedimiento, Algunos de los principales estándares a definir son:

- Longitudes de contraseñas
- Histórico de contraseñas
- Eventos a registrar en Log’s

1.2.8. Cronograma

CRONOGRAMA DE ACTIVIDADES						
Tiempo / **Actividades**	Semana1	Semana2	Semana3	Semana 4	Semana 5	Semana 6
Control de seguridad a nivel de usuario con permisos de acceso al sistema informático.						
Control de los puntos de red de acceso tanto alámbrico como inalámbrico.						
Bitácoras de control para servidores, climatización del centro de cómputo, respaldos de archivos del centro de cómputo						
Rangos de accesos para el o los administradores del centro de cómputo.						
Conclusiones y Recomendaciones.						

CAPITULO II

2. MARCO DE REFERENCIA

2.2. Marco teórico

2.2.1. Clínica Humanitaria Pablo Jaramillo C. Esta institución es un centro de salud de segundo nivel el mismo que se encuentra funcionando por más de veinte años, la institución cuenta con servicios especializados de consulta externa en el área de Ginecología, Pediatría, Medicina Interna, además cuenta con auxiliares de diagnóstico como: Ecografía, Rayos X, Colposcopia, Laboratorio, cuenta también con especialidades como Odontología, Dermatología, Traumatología, Cirugía Pediátrica, de adulto, Cirugía Plástica y Otorrinolaringología, cuenta con el área de Emergencia, Farmacia, Psicología, Consejería y el área dedicado a los jóvenes "Espacio Joven" de igual manera cuenta con el área de hospitalización en lo que sobresale la atención a las madres embarazadas y a los niños es decir Gineco-obstetricia y Pediatría teniendo una área para los niños prematuros de Neonatología y un quirófano para las diferentes cirugías que se encuentran programadas.

La clínica se encuentra formada por un grupo humano de 140 personas las mismas que se encuentran distribuidas en las diferentes áreas médicas y departamentos administrativos, las áreas administrativas se cuenta con la Dirección Médica, la Dirección Financiera, Contabilidad, Gestión del Talento Humano, Gestión de Calidad, Sistemas, áreas que se encuentran integradas mediantes el sistema informático gerencial el mismo que fue adquirido en el año de 2005 y el que ha sufrido varios cambios, éste sistema se encuentra integrando todas la áreas de tal manera que la información esta entrelazada y en línea.

Cuenta con en el centro de cómputo con un servidor IBM con un sistema operativo CentOS sobre el cual está instalado la base de datos Oracle 9i Enterprise la

misma que cuenta con 148 usuarios activos en la BD[1]. Se encuentran conectados a la red 62 estaciones de trabajo las mismas que cuentan con las aplicaciones para el sistema informático desarrollado en Oracle Forms y Oracle Reports en la versión 6i.

Cuentan con un servidor de archivos sobre un clon que cuenta Windows Server 2003 de sistema operativo, en este servidor se encuentran alojados los archivos que generan los usuarios en sus estaciones de trabajo individuales

2.2.2. Centro de cómputo.- El Centro de computo o CPD[2] se denomina a un edificio, oficina o departamento de gran tamaño en el que se alojan varios equipos electrónicos los mismos que permiten el procesamiento, almacenamiento de grandes cantidades de información, de manera automatizada, al igual que se encarga de mantener el enlace con las estaciones de trabajo los mismos que consumen los servicios que este centro brinda, es decir que el CPD[1] se la parte central de una red ya que en éste lugar se encuentra toda la información de gran relevancia considerada por los altos ejecutivos de una empresa y los gerentes de la información que administran dicho centro.

El centro de cómputo también tiene por tarea el capacitar a los usuarios, realizar el mantenimiento de los equipos informáticos al igual que el realizar los estudios de factibilidad para el desarrollo de nuevos proyectos entre otras actividades.

La misión más importante que un centro de cómputo es el de garantizar que los servicios se encuentre disponibles y accesibles de acuerdo a las políticas preestablecidas.

De acuerdo con la importancia de la información las políticas de seguridad que se aplican al CPD[1] son controladas desde la parte física como la seguridad lógica.

[1]Base de Datos
[2]Centro de procesamiento de Datos

Por lo general los grandes servidores se concentran en salas denominadas “Cuarto Frio”, “Nevera”, “Site” entre otros, estos lugares tienen la peculiaridad que se encuentran aclimatados en base a un sistema de enfriamiento lo que permite que el lugar se encuentre a una temperatura de alrededor de 21 y 23 grados centígrados, con el fin de evitar problemas de malfuncionamiento y averías en los equipos electrónicos provocados por el sobrecalentamiento, para estos lugares las medidas de seguridad son estrictas, así como las medidas de extinción de incendios adecuadas para los equipos eléctricos tales como agua nebulizada o por gas INERGEN, dióxido de carbono o nitrógeno

2.2.3. Base de datos.- Una base de datos o banco de datos (en ocasiones abreviada con la sigla BD[2] o con la abreviatura b. d.) es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. En la actualidad, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital (electrónico), que ofrece un amplio rango de soluciones al problema de almacenar datos.

Existen SGBD[3] (Sistema Gestor de Base de Datos) en inglés, DBMA[4], son programas que brindan una interfaz entre la base de datos, el usuario y las aplicaciones las mismas que se encuentran diseñadas para comunicarse con la Base de Datos mediante lenguaje de consulta estructurada SQL[5] (Structured Query Language) que permiten gestionar la información manera rápida.

Las aplicaciones más usuales son para la gestión de empresas e instituciones públicas. También son ampliamente utilizadas en entornos científicos con el objeto de almacenar la información experimental, entre otras.

[3]Sistema Gestor de Base de Datos
[4] Data Base Mangement System
[5] Structured Query Language Lenguaje estructurado de consulta

2.2.3.1. Tipos de Base de Datos

Las bases de datos pueden clasificarse de varias maneras, de acuerdo al contexto que se esté manejando, la utilidad de las mismas o las necesidades que satisfagan.

Según la variabilidad de los datos almacenados

Bases de datos estáticas Son bases de datos solamente de lectura, la cual es utilizada principalmente para almacenar datos históricos que posteriormente se pueden utilizar para estudiar el comportamiento de un conjunto de datos a través del tiempo, realizar proyecciones y tomar decisiones.

Bases de datos dinámicas Estas bases de datos son donde la información almacenada se va modificando con el tiempo, en ésta base de datos nos permite realizar las operaciones de actualización, borrado y adición de datos, además de las operaciones fundamentales de consulta.

Bases de datos bibliográficas.- En esta base de datos se encuentra la información de manera descriptiva lo que corresponde a la fuente primaria de tal manera que al acceder a esta información nos permite acceder a los datos de gran volumen, como puede ser los datos de para ubicar un libro, película, etc.

Bases de datos de texto completo Esta base de datos se encarga o se utiliza para llevar a cabo el almacenamiento de las fuentes primarias, tales como el contenido de todas las ediciones de un periódico, revistas, etc.

Modelos de bases de datos A más de la clasificación antes mencionada por la funcionalidad de las bases de datos, éstas también se pueden clasificar de acuerdo a su modelo de administración de datos.

Un modelo de datos es básicamente un lenguaje utilizado para realizar una descripción de una base de datos al igual que como se van a relacionar cada una

de ellos con los demás que se encuentren conjuntamente almacenados, es decir las relaciones de integridad (las condiciones que los datos deben cumplir para reflejar correctamente la realidad deseada) de igual manera las manipulación de los datos (Adicionar, Eliminar, Editar y Consultar los datos de la base)

Dicho de otra manera o visto desde una manera más amplia podemos decir que el modelo de datos es la descripción de la realidad y cómo interactúan los datos entre sí.

Un modelo de datos generalmente se encuentra compuesto de dos lenguajes el DDL[6] (Data Definition Language) y el DML[7] (Data Manipulation Language). El DDL[6]o lenguaje de definición de datos su función es el de describir de una manera abstracta la estructura de los datos y las relaciones con sus correspondientes restricciones. El DML[7]o lenguaje de manipulación de datos se dedica a describir las operaciones para la manipulación de la información y a esta parte se la suele conocer como lenguaje de consulta.

Los modelos de datos no son cosas físicas: son abstracciones que permiten la implementación de un sistema eficiente de base de datos; por lo general se refieren a algoritmos, y conceptos matemáticos.

Los modelos frecuentemente utilizados en las bases de datos:

Bases de datos jerárquicas

Éstas son bases de datos que, como su nombre indica, almacenan su información en una estructura jerárquica. En este modelo los datos se organizan en una forma similar a un árbol (visto al revés), en donde un nodo padre de información puede tener varios hijos. El nodo que no tiene padres es llamado raíz, y a los nodos que no tienen hijos se los conoce como hojas.

[6] Data Definition Language
[7] Data Manipulation Language

Las bases de datos jerárquicas son especialmente útiles en el caso de aplicaciones que manejan un gran volumen de información y datos muy compartidos permitiendo crear estructuras estables y de gran rendimiento.

Una de las principales limitaciones de este modelo es su incapacidad de representar eficientemente la redundancia de datos.

Base de datos de red

Éste es un modelo ligeramente distinto del jerárquico; su diferencia fundamental es la modificación del concepto de nodo: se permite que un mismo nodo tenga varios padres (posibilidad no permitida en el modelo jerárquico).

Fue una gran mejora con respecto al modelo jerárquico, ya que ofrecía una solución eficiente al problema de redundancia de datos; pero, aun así, la dificultad que significa administrar la información en una base de datos de red ha significado que sea un modelo utilizado en su mayoría por programadores más que por usuarios finales.

Bases de datos transaccionales

Son bases de datos cuyo único fin es el envío y recepción de datos a grandes velocidades, estas bases son muy poco comunes y están dirigidas por lo general al entorno de análisis de calidad, datos de producción e industrial, es importante entender que su fin único es recolectar y recuperar los datos a la mayor velocidad posible, por lo tanto la redundancia y duplicación de información no es un problema como con las demás bases de datos, por lo general para poderlas aprovechar al máximo permiten algún tipo de conectividad a bases de datos relacionales.

Bases de datos relacionales

Éste es el modelo utilizado en la actualidad para modelar problemas reales y administrar datos dinámicamente. Tras ser postulados sus fundamentos en 1970 por Edgar Frank Codd, de los laboratorios IBM en San José (California), no tardó en consolidarse como un nuevo paradigma en los modelos de base de datos. Su idea fundamental es el uso de "relaciones". Estas relaciones podrían considerarse en forma lógica como conjuntos de datos llamados "tuplas". Pese a que ésta es la teoría de las bases de datos relacionales creadas por Codd, la mayoría de las veces se conceptualiza de una manera más fácil de imaginar. Esto es pensando en cada relación como si fuese una tabla que está compuesta por registros[8] (las filas de una tabla), que representarían las tuplas, y campos[9](las columnas de una tabla).

En este modelo, el lugar y la forma en que se almacenen los datos no tienen relevancia (a diferencia de otros modelos como el jerárquico y el de red). Esto tiene la considerable ventaja de que es más fácil de entender y de utilizar para un usuario esporádico de la base de datos. La información puede ser recuperada o almacenada mediante "consultas" que ofrecen una amplia flexibilidad y poder para administrar la información.

El lenguaje más habitual para construir las consultas a bases de datos relacionales es SQL[5], Structured Query Language o Lenguaje Estructurado de Consultas, un estándar implementado por los principales motores o sistemas de gestión de bases de datos relacionales.

Durante su diseño, una base de datos relacional pasa por un proceso al que se le conoce como normalización de una base de datos.

[8] Las filas de una tabla
[9] Las columnas de una tabla

Durante los años 80 la aparición de dBASE produjo una revolución en los lenguajes de programación y sistemas de administración de datos. Aunque nunca debe olvidarse que dBase no utilizaba SQL[5] como lenguaje base para su gestión.

Bases de datos multidimensionales

Son bases de datos ideadas para desarrollar aplicaciones muy concretas, como creación de Cubos OLAP[10]. Básicamente no se diferencian demasiado de las bases de datos relacionales (una tabla en una base de datos relacional podría serlo también en una base de datos multidimensional), la diferencia está más bien a nivel conceptual; en las bases de datos multidimensionales los campos[9] o atributos de una tabla pueden ser de dos tipos, o bien representan dimensiones de la tabla, o bien representan métricas que se desean estudiar.

Bases de datos orientadas a objetos

Este modelo, bastante reciente, y propio de los modelos informáticos orientados a objetos, trata de almacenar en la base de datos losobjetos completos (estado y comportamiento).

Una base de datos orientada a objetos es una base de datos que incorpora todos los conceptos importantes del paradigma de objetos:

- ✓ **Encapsulación -** Propiedad que permite ocultar la información al resto de los objetos, impidiendo así accesos incorrectos o conflictos.
- ✓ **Herencia -** Propiedad a través de la cual los objetos heredan comportamiento dentro de una jerarquía de clases.
- ✓ **Polimorfismo -** Propiedad de una operación mediante la cual puede ser aplicada a distintos tipos de objetos.

En bases de datos orientadas a objetos, los usuarios pueden definir operaciones sobre los datos como parte de la definición de la base de datos. Una operación

[10] On-Line Analytic Processing

(llamada función) se especifica en dos partes. La interfaz (o signatura) de una operación incluye el nombre de la operación y los tipos de datos de sus argumentos (o parámetros). La implementación (o método) de la operación se especifica separadamente y puede modificarse sin afectar la interfaz. Los programas de aplicación de los usuarios pueden operar sobre los datos invocando a dichas operaciones a través de sus nombres y argumentos, sea cual sea la forma en la que se han implementado. Esto podría denominarse independencia entre programas y operaciones.

Bases de datos documentales

Permiten la indexación a texto completo, y en líneas generales realizar búsquedas más potentes.

Bases de datos deductivas

Un sistema de base de datos deductiva, es un sistema de base de datos pero con la diferencia de que permite hacer deducciones a través de inferencias. Se basa principalmente en reglas y hechos que son almacenados en la base de datos. Las bases de datos deductivas son también llamadas bases de datos lógicas, a raíz de que se basa en lógica matemática. Este tipo de base de datos surge debido a las limitaciones de la Base de Datos Relacional de responder a consultas recursivas y de deducir relaciones indirectas de los datos almacenados en la base de datos.

2.2.4. Cuenta de usuario

En el contexto de la informática, un usuario es aquel que utiliza un sistema informático. Para que los usuarios puedan obtener seguridad, acceso al sistema, administración de recursos, etc, dichos usuarios deberán identificarse. Para poder identificarse, el usuario necesita una cuenta (una cuenta de usuario) y un usuario, la mayoría de casos se asocia a una contraseña. Los usuarios utilizan una interfaz

para acceder al sistema, el proceso de identificación es conocido como identificación de usuario o acceso del usuario al sistema (del inglés: "log in").

Los usuarios se caracterizan por ser el tipo de personas que utilizan un sistema sin la amplia experiencia necesaria que se requiere para entender al sistema (en oposición al técnico, hacker u otro perfil que sí se presupone conoce dicho sistema). En el contexto hacker, se les denomina usuarios reales. Véase también Usuario final.

Los usuarios de informática son muy similares a los usuarios en telecomunicaciones, pero con algunas pequeñas diferencias semánticas. La diferencia es comparable a la diferencia que existe entre un usuario final y los consumidores en la economía.

El nombre de usuario es un nombre único que se identifica a cada usuario (aunque en ocasiones existen alguna clase de usuarios 'invitado'). Los nombres de usuario se basan por lo general en cadenas cortas alfanuméricas. Dependiendo de las políticas o los servicios en particular, los nombre de usuario son elegidos ya sea por el usuario, o asignados por el administrador de sistemas.

Las opciones generalmente utilizadas para los nombres de usuarios pueden ser el nombre, las iniciales o alguna combinación con el nombre, apellido, iniciales o algunos números arbitrarios. Algunas veces los sistemas dictan los aspectos para elegir un nombre de usuario.

Por razones de seguridad, algunos sistemas exigen que el nombre de usuario contenga dígitos y/o símbolos (en vez de solo consistir de letras), aunque por lo general este requerimiento es más comúnmente asociado con las contraseñas.

Los aspectos referentes a las contraseñas se encuentran en el respectivo artículo.

Los nombres de usuario son ocasionalmente utilizados como el nombre del buzón en las direcciones de correo electrónico.

2.2.4.1. Usos

Una cuenta de usuario nos permite acceder a los servicios de un sistema. Por lo general nos autoriza el ingreso. Aunque, la autenticación no implica autorización automática.

Una vez que el usuario se ha autenticado, el sistema operativo asocia un identificador por ejemplo un entero para referirse a él, en vez de utilizar el nombre de usuario. A esto se le conoce como identificador de usuario (user id) en los sistemas operativos

En informática, un usuario es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona.

Un usuario generalmente se identifica frente al sistema o servicio utilizando un nombre de usuario y a veces una contraseña, este tipo es llamado usuario registrado. Por lo general un usuario se asocia a una única cuenta de usuario, en cambio, una persona puede llegar a tener múltiples cuentas en un mismo sistema o servicio (si eso está permitido).

Un usuario registrado accede a un servicio a través de un login luego de su autentificación.

Un usuario también puede ser anónimo si no posee una cuenta de usuario, por ejemplo, al navegar por un sitio web sin registrase el usuario puede considerarse parcialmente anónimo (parcialmente porque puede ser identificado por su dirección IP). La navegación anónima sólo puede lograrse utilizando un proxy anónimo (sólo es más seguro, no es 100% anónimo). También se puede acceder a un servicio de forma anónima, por lo general se poseen menos opciones y posibilidades que un usuario registrado. Los usuarios anónimos a veces son referidos simplemente como "invitados".

2.2.5. Seguridad Informática

La seguridad informática se orienta a la protección de la infraestructura de los centros de cómputo al igual que los datos basándose en reglas, estándares, protocolos, herramientas las mismas que permiten minimizar las posibilidades de que ocurra un acontecimiento no deseado para la seguridad de los equipos, infraestructura y datos de un centro de cómputo.

El brindar seguridad informática hace referencia a la custodia del software, base de datos, archivos, y a la información que la institución considera como un riesgo si llega a poseer otras personas ajenas a la institución a ésta información se la denomina confidencial o privilegiada.

La seguridad informática se ha convertido en uno de los elementos importantes dentro de las instituciones debiendo ser administrada bajo los criterios estipulados por los administradores teniendo como fin que los usuarios externos y no autorizados puedan acceder a la información sin la correspondiente autorización.

El asegurar el acceso oportuno a la información se denomina o se considera como otra función que persigue la seguridad informática al igual que la el correspondiente respaldo ante una perdida, daño ante atentados o desastres que puedan ocurrir en un momento dado.

Cada empresa automatizada tiene implementada su propia infraestructura computacional, área en la que se realiza la gestión y el almacenamiento de la información el propósito de implementar en ésta área seguridad informática es con el propósito de mantener los equipos funcionando correctamente y prevenir futuros daños mediante planes de contingencia previstos con anterioridad.

La información es gestionada por los usuarios mediante la estructura tecnológica por un medio de comunicación hacia este campo se orienta la seguridad informática estableciendo normas sobre el funcionamiento de los accesos al

sistema, tales como: horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuarios, etc. Es decir que se emplea todo lo necesario para que la información que se gestiona no sea errada ni sea susceptible de daños lo que daría paso a contratiempos por parte de los usuarios de la institución.

2.2.6. Seguridad en Base de datos Oracle

La base de datos Oracle tiene por características de seguridad el prevenir el acceso no autorizado a la base de datos, a objetos (tablas, vistas, índices, procedimientos, etc.) los cuales pertenecen a un usuario específico,

La seguridad implementada por Oracle se basa en privilegios los mismos que restringen el acceso a los datos u objetos de la Base de Datos. Un usuario puede acceder a un objeto solamente mediante privilegios previamente otorgados y a su vez los usuarios creados en la base de datos pueden generar privilegios a otros usuarios de acuerdo a su propio criterio, siempre que tengan esta facultad dentro del administrador de la Base de Datos.

La Base de Datos Oracle puede ser administrada bajo los siguientes parámetros:

- ✓ Usuarios y Esquemas
- ✓ Privilegios
- ✓ Roles
- ✓ Configuración del almacenamiento y cuotas
- ✓ Límites a los recursos
- ✓ Monitoreo

2.2.6.1. Usuarios y Esquemas.- Las diferentes Bases de Datos tienen sus propias listas de usuarios. Los usuarios dados de alta en el sistema tienen la

posibilidad de conectarse a través de una aplicación mediante un nombre de usuario y una contraseña que se encuentre habilitado en la base de datos, estos parámetros permite restringir el acceso no autorizado a la base de datos por usuarios que no están autorizados y registrados en la Base de Datos.

Dominio de Seguridad.- Se considera un dominio de seguridad al conjunto de elementos, a una política de seguridad al igual que el conjunto de actividades específicas tales como:

- ✓ Acciones (Privilegios o Roles) disponibles para el usuarios.
- ✓ Límites de espacio en el Tablespace (Son estructuras donde se almacenan los objetos del esquema de la base de datos, como tablas, índices, etc. con la peculiaridad de poderse repartir en varios ficheros) para los usuarios.
- ✓ Límites de utilización de los recursos del sistema para los usuarios.

2.2.6.2. Privilegios.- Se denomina privilegios a los permisos para ejecutar sentencias SQL[5] definidas sobre la Base de Datos.

Los privilegios de una base de datos Oracle los podemos separar en dos categorías distintas: Privilegios de sistema y Privilegios de objetos.

Privilegios de sistema.- Los usuarios pueden desempeñar mediante los privilegios del sistema acciones particulares dentro del sistema o una acción particular sobre un tipo determinado de objeto. Varios privilegios de sistema están disponibles solamente para administradores y desarrolladores de aplicaciones porque estos privilegios son muy potentes.

Privilegios de objetos.- Los usuarios pueden desempeñar acciones sobre un esquema específico mediante los privilegios de objetos, Los privilegios de objetos son asignados a usuarios finales, para que puedan usar una aplicación de la base de datos llevando a cabo tareas específicas.

Asignar Privilegios.- Los usuarios pueden recibir privilegios de dos maneras diferentes:

Privilegios asignados a los usuarios de manera explícita.

Privilegios asignados a roles (grupo de privilegios) y a su vez un rol puede ser asignado a un usuario o varios usuarios que realicen la misma actividad sobre de la Base de Datos, Debido a que los la administración de los roles es de manera más fácil o practica es mejor asignar los privilegios a los roles y a su vez los roles a los usuarios para una mejor administración.

2.2.6.3. Roles Los roles que provee Oracle es con el fin de permitir una administración más fácil y controlada de los privilegios. Los roles son agrupadores con nombre de privilegios, que pueden ser asignados a usuarios o a otros roles. Las siguientes propiedades de los roles permiten administrar los privilegios de una manera más fácil:

- ✓ R**educida asignación de privilegios:** En lugar de otorgar explícitamente el mismo conjunto de privilegios a muchos usuarios el administrador de la base de datos puede asignar los privilegios a un rol y éste a un grupo de usuarios.

- ✓ **Administración dinámica de los privilegios:** Cuando los privilegios de un grupo deben cambiar, solamente los privilegios del rol necesitan ser modificados. Los dominios de seguridad de todos los usuarios a los que asignó dicho rol.

- ✓ **Selectiva disponibilidad de los privilegios:** Los roles asignados a los usuarios pueden ser selectivamente activados o desactivados. Esto permite control específico de los privilegios de los usuarios en cualquier situación.

- ✓ **Consciencia de aplicación:** Una aplicación de la base de datos puede ser diseñada para habilitar o inhabilitar roles automáticamente cuando un usuario intenta usar la aplicación.

2.2.6.4. Configuración del almacenamiento y quotas Oracle provee medios para limitar el uso del espacio de disco asignado a la base de datos, de acuerdo a cada usuario; incluyendo los default tablespaces, temporary tablespaces y los tablespaces quotas.

Default Tablespace.- Cada usuario es asociado a un default tablespace. Cuando un usuario crea una tabla, índice, o cluster y no se especifica ningún tablespace que contenga físicamente al objeto, el default tablespace es utilizado si el usuario tiene privilegio para crear el objeto.

Temporay Tablespace.- Cada usuario tiene un temporary tablespace. Cuando un usuario ejecuta una sentencia SQL[5] que requiere la creación de objetos temporarios (por ejemplo un índice), se usa el temporary tablespace del usuario.

Tablespace Quotas.- Oracle puede limitar el espacio disponible de disco colectivo. Las quotas (límites de espacio) pueden ser configuradas para cada tablespace disponible para un usuario. Las tablespace quotas permiten un control selectivo sobre el espacio en disco que es consumido por cada objeto de cada esquema.

2.2.6.5. Límites a los recursos.- A cada usuario le es asignado un perfil que especifica las limitaciones sobre varios recursos del sistema disponibles para el usuario, incluyendo:

- ✓ El número de sesiones concurrentes que el usuario puede establecer
- ✓ El tiempo de CPU:
  - Disponible para la sesión de usuarios

- disponible para una simple llamada a Oracle realizada por una sentencia SQL[5]

✓ Cantidad de I/O:

- disponible para la sesión del usuario
- disponible para una simple llamada a Oracle realizada por una sentencia SQL[5]

✓ La cantidad de tiempo ocioso permitido para la sesión del usuario.

✓ La cantidad de tiempo de conexión permitido para la sesión del usuario.

✓ Restricciones en las contraseñas:

- Bloqueo de la cuenta después de una determinada cantidad de intentos de conexión fallidos.
- Expiración de las contraseñas y período de gracia.
- Reutilización de contraseñas y restricciones.

Se pueden crear diferentes perfiles y asignarse individualmente a cada usuario de la base de datos. A los usuarios que no se le ha asignado explícitamente un perfil, se les asigna el perfil por default. El límite en la utilización de recursos previene el consumo excesivo de los recursos globales del sistema de base de datos.

2.2.6.6. Monitoreo Oracle permite realizar un monitoreo selectivo de las acciones de los usuarios para ayudar en la investigación de usos maliciosos de la base de datos. El monitoreo puede realizarse a tres niveles distintos:

✓ **Monitoreo de sentencias:** Es el monitoreo de sentencias SQL[5] específicas sin atender concretamente a los objetos. Este tipo de monitoreo puede

hacerse para todos los usuarios del sistema o se puede enfocar sólo a algunos usuarios seleccionados.

- ✓ **Monitoreo de privilegios:** Es el monitoreo de los privilegios del sistema sin atender concretamente a los objetos. Este tipo de monitoreo puede hacerse para todos los usuarios del sistema o se puede enfocar sólo a algunos usuarios seleccionados.

- ✓ **Monitoreo de objetos**:Es el monitoreo de los accesos a esquemas específicos sin considerar el usuario. Monitorea las sentencias permitidas por los privilegios.

Para todos los tipos de monitoreo, Oracle permite el monitoreo selectivo de sentencias ejecutadas con éxito, sentencias ejecutadas sin éxito o ambas.

Los resultados del monitoreo son registrados en una tabla llamada “the audit trail” (la pista de auditoría).

2.2.7. Políticas de Seguridad

Las políticas de seguridad proveen una guía para el desarrollo de políticas de seguridad para operaciones de bases de datos, e incluye los siguientes temas:

- ✓ Política de Seguridad del Sistema
- ✓ Política de Seguridad de la Información
- ✓ Política de Seguridad del Usuario
- ✓ Política Administrativa de Contraseña
- ✓ Política de Auditoría

2.2.7.1. Política de Seguridad del sistema.- Aquí se describe aspectos de la política de seguridad de sistemas e incluye los siguientes temas:

- ✓ Mantenimiento de usuarios de base de datos
- ✓ Autentificación de usuarios
- ✓ Seguridad de Sistemas Operativos

Cada base de datos tiene uno o más administradores de seguridad quienes son responsables del mantenimiento de todos los aspectos de la política de seguridad. Si el sistema de bases de datos es pequeño, el administrador de bases de datos podría tener las responsabilidades del administrador de seguridad. Sin embargo, si el sistema de bases de datos es grande, una persona o grupos de personas especiales podrían tener responsabilidades limitadas de aquellas que corresponden a un administrador de seguridad.

Luego de decidir quién administrará la seguridad del sistema, se debe desarrollar una política de seguridad para cada base de datos. Una política de seguridad de base de datos debería incluir muchas sub-políticas, como se explica en las siguientes secciones.

Mantenimiento de usuarios de bases de datos.- La seguridad debería ser mantenida por el mantenimiento de los usuarios de bases de datos. Dependiendo del tamaño de un sistema de bases de datos y de la cantidad del trabajo requerido para administrar los usuarios de bases de datos, el administrador de seguridad debería ser el único usuario con los privilegios requeridos para crear, alterar o borrar un usuario de base de datos. Por otro lado, debería haber un número de administradores con privilegios para administrar los usuarios de bases de datos. Solo personas que gozan de confianza deberían tener privilegios totales para administrar los usuarios de bases de datos.

Autentificación de usuarios.- Los usuarios de bases de datos pueden ser autentificados (verificados como una persona correcta) por Oracle usando el sistema operativo de host, los servicios de red, o la base de datos. Generalmente

la autentificación de usuarios vía un sistema operativo host es preferida por las siguientes razones:

- ✓ Los usuarios pueden conectarse a Oracle más rápido y más convenientemente sin especificar nombre de usuario y contraseña.
- ✓ Control centralizado sobre la autorización de usuarios en el sistema operativo: Oracle no necesita almacenar o administrar los nombres de usuario y contraseñas si el sistema operativo y la base de datos se corresponden
- ✓ Las entradas de los usuarios en los audit trails de la base de datos y el sistema operativo se corresponden

La autentificación de usuarios por la base de datos es normalmente utilizada cuando el sistema operativo no puede soportar la autentificación de usuarios.

Seguridad de Sistemas Operativos.- Si es apropiado, los siguientes temas de seguridad deben ser considerados no sólo para un entorno de sistema operativo ejecutando Oracle sino también cualquier aplicación de bases de datos:

- ✓ Los administradores de bases de datos deben tener los privilegios del sistema operativo para crear o eliminar archivos.
- ✓ Los usuarios típicos de bases de datos no deberían tener los privilegios del sistema operativo para crear o eliminar archivos relacionados a la base de datos.

Si el sistema operativo identifica el rol de bases de datos para los usuarios, los administradores de seguridad deben tener los privilegios del sistema operativo para modificar el dominio de seguridad de las cuentas del sistema operativo.

2.2.7.2. Política de Seguridad de la Información.- La seguridad de datos incluye los mecanismos que controlan el acceso y el uso de la base de datos en el

nivel de objeto. Su política de seguridad de datos determina que usuarios tienen acceso a objetos de esquema específicos, y los tipos específicos de acciones permitidos para cada usuario sobre el objeto. También debería definir las acciones, para cualquiera, que sea auditado para cada objeto de esquema.

De cualquier forma, la seguridad de los datos debería estar basada sobre la sensibilidad de los datos. Si la información no es sensible, entonces la política de seguridad de datos puede ser más flexible. Sin embargo, si los datos son sensibles, una política de seguridad debe ser desarrollada para mantener un fuerte control sobre el acceso a los objetos.

2.2.7.3. Política de Seguridad de Usuarios.- Esta sección describe los aspectos de una política de seguridad de usuarios e incluye los siguientes temas:

- ✓ Seguridad del Usuario General
- ✓ Seguridad de Usuario-Final
- ✓ Seguridad de Administrador
- ✓ Seguridad de Desarrollador de Aplicaciones
- ✓ Seguridad de Administrador de Aplicaciones

Seguridad del Usuario General.- Para todos los tipos de usuarios de base de datos, considere los siguientes temas de seguridad de usuario general:

- ✓ Seguridad por contraseña
- ✓ Administración de privilegios

Seguridad por contraseña.- Si la autentificación de usuarios es administrada por la base de datos, los administradores de seguridad deberían desarrollar una política de seguridad por contraseña para mantener la seguridad de acceso a la base de datos. Por ejemplo, los usuarios de base de datos deberían ser advertidos

de cambiar su contraseña cada cierto período regular, y por supuesto, cuando sus contraseñas son reveladas a otros. Forzando a un usuario a modificar su contraseña en tales situaciones, los accesos a bases de datos sin autorización pueden ser reducidos.

Para proteger mejor la confidencialidad de su contraseña, Oracle puede ser configurado para utilizar contraseñas encriptadas para conexiones cliente/servidor y servidor/servidor.

Administración de privilegios.- Los administradores de seguridad deben considerar los temas relacionados a la administración de privilegios para todos los tipos de usuarios. Por ejemplo, en una base de datos con muchos usuarios, podría ser beneficioso utilizar roles para administrar los privilegios disponibles a usuarios. Por otro lado, en una base de datos con un número de usuarios reducido, podría ser más fácil otorgar privilegios explícitamente a los usuarios y anular el uso de roles.

Los administradores de seguridad que administran una base de datos con muchos usuarios, aplicaciones u objetos deberían tomar ventaja de los beneficios ofrecidos por los roles. Los roles simplifican en gran medida la tarea de la administración de privilegios en entornos complejos.

Seguridad de Usuario-Final.- Los administradores de la seguridad deben definir también una política para la seguridad de usuario-final. Si una base de datos es grande y con muchos usuarios, el administrador de seguridad puede decidir que grupos de usuarios pueden ser categorizados, crear roles de usuarios para esos grupos de usuarios, otorgar los privilegios necesarios o roles de aplicación para cada rol de usuario, y asignar los roles de usuarios a los usuarios. En excepciones, el administrador de seguridad debe también decidir que privilegios deben ser explícitamente otorgados a usuarios individuales.

Cuando es posible, utilizar roles en todas las situaciones posibles para crear privilegios usuario-final hacen su administración eficiente y simple.

Seguridad de Administrador.- Los administradores de seguridad deben tener una política de seguridad de administrador. Por ejemplo, cuando es una gran base de datos y existen diversos tipos de administradores de base de datos, el administrador de seguridad debe decidir cómo agrupar los privilegios administrativos relacionados a los diversos roles administrativos.

Los roles administrativos pueden entonces ser otorgados a los usuarios administradores apropiados. Por otro lado, cuando la base de datos es pequeña y tiene pocos administradores puede ser más conveniente crear un rol administrativo y otorgarlo a todos los administradores.

Protección para conexiones SYS y SYSTEM.- Luego de la creación de la base de datos, inmediatamente cambie la contraseña para los nombres de usuario administrativos SYS y SYSTEM para prevenir accesos no autorizados a la base de datos. Conectarse como SYS y SYSTEM da al usuario todos los privilegios para modificar la base de datos de distintas formas. Por lo tanto, los privilegios para estos nombres de usuario son extremadamente sensibles, y deben estar disponibles sólo para los administradores de bases de datos seleccionados.

Protección para conexiones Administrador.- Sólo los administradores de bases de datos deben tener la capacidad para conectarse a la base de datos con los privilegios de administrador. Conectarse como SYSDBA da al usuario privilegios sin restricción para hacer cualquier cosa sobre la base de datos (tales como encender, apagar y recuperar) o los objetos dentro de la base de datos (tales como crear, eliminar, y borrar).

Seguridad de Desarrollador de Aplicaciones.- Los administradores de seguridad deben definir una política especial de seguridad para los desarrolladores de aplicaciones que usen base de datos. Un administrador de

seguridad solo puede otorgar privilegios, los necesarios para crear los objetos que necesiten los desarrolladores, a los administradores de bases de datos y ellos se encargaran de recibir los pedidos de creación de objetos de parte de los desarrolladores.

Desarrolladores de Aplicaciones y sus privilegios.- Los desarrolladores de bases de datos son exclusivamente usuarios de ésta y requieren un grupo de privilegios para poder cumplir con sus trabajos. A diferencia de los usuarios finales, los desarrolladores necesitan privilegios de sistema, como por ejemplo para crear una tabla, crear un procedimiento, etc. Sin embargo, solo específicos privilegios van a otorgarse a los desarrolladores, así se podrá restringir sus accesos en la base de datos.

Desarrollo de Aplicaciones Libres vs. Desarrollo de Aplicaciones Controladas.- El administrador de base de datos puede definir las siguientes opciones cuando determine que privilegios deben ser otorgados a los desarrolladores:

Libre Desarrollo Un desarrollador de aplicaciones está autorizado a crear nuevos esquemas de objetos, incluyendo tablas, índices, procedimientos, paquetes, etc. Esta opción permite desarrollar una aplicación independiente de los otros objetos.

Desarrollo Controlado Un desarrollador no está autorizado a crear nuevos esquemas de objetos. Todas las tablas, índices, procedimientos, etc., requeridos son creados por el administrador de base de datos, por un pedido del desarrollador. Esta opción permite al administrador de base de datos tener completamente controlado el espacio usado de la misma y el camino de acceso a la información en ella.

No obstante, algunos sistemas de base de datos usan solo una de esas opciones, otros sistemas pueden combinar esas opciones. Por ejemplo, los desarrolladores

pueden ser autorizados para crear nuevos procedimientos y paquetes almacenados, pero no están autorizados para crear tablas o índices.

Para que un administrador de seguridad tome alguna decisión con respecto a este tema debe basarse en lo siguiente:

- ✓ El control deseado sobre el espacio a utilizar de la base de datos
- ✓ El control deseado sobre las rutas de acceso a los esquemas de los objetos
- ✓ La base de datos usada para desarrollar aplicaciones, si una base de datos de prueba es usada para el desarrollo de aplicaciones, una política más liberal de desarrollo será implementada.

Roles y privilegios para los desarrolladores.- Los administradores de seguridad pueden crear roles para manejar los privilegios requeridos por los desarrolladores. Por ejemplo, el típico rol llamado APPLICATION_DEVELOPER puede incluir los privilegios de sistemas para utilizar CREATE TABLE, CREATE VIEW y CREATE PROCEDURE.

Los administradores de seguridad considerarán lo siguiente cuando definan roles para los desarrolladores:

- ✓ Los privilegios de sistema para utilizar CREATE son usualmente otorgados a los desarrolladores, entonces ellos pueden crear sus propios objetos. Sin embargo, CREATE ANY, el cual permite al usuario crear un objeto en cualquier campo de acción del usuario, no es usualmente otorgado a los desarrolladores. Esto restringe la creación de nuevos objetos sólo para las cuentas de usuario de los desarrolladores.
- ✓ Es poco frecuente asignar privilegios sobre objetos a los roles usados por los desarrolladores de aplicaciones. Es impráctico, esto restringe sus posibilidades de uso en la creación de otros objetos. Es más práctico

permitir a los desarrolladores crear sus propios objetos para propósitos de desarrollo.

Restricciones de Espacio impuestas sobre los desarrolladores.- Como el privilegio de crear objetos, que se le otorga a los desarrolladores, forma parte del proceso de desarrollo de aplicaciones, los administradores de seguridad deben controlar cual y cuanto espacio va a ser usado por cada desarrollador en la base de datos. Por ejemplo, como un administrador de seguridad, debería fijar o restringir los siguientes límites para cada desarrollador:

- ✓ El Tablespace en los cuales los desarrolladores pueden crear tablas o índices.
- ✓ La quota por cada Tablespace accesible por los desarrolladores.

Seguridad de Administrador de Aplicaciones.- En grandes sistemas de bases de datos con muchas aplicaciones (por ejemplo, precompiladores y aplicaciones de formularios) podría tener un administrador de aplicaciones. Este es responsable de los siguientes tipos de tareas:

- ✓ Creación de roles para aplicaciones y manejo de privilegios para cada rol de las aplicaciones.
- ✓ Creación y manejo de objetos usados por una aplicación en la base de datos.
- ✓ Mantenimiento y actualización del código de las aplicaciones y de los procedimientos de Oracle.

Frecuentemente, un administrador de aplicaciones es también el desarrollador que diseñó dicha aplicación. Sin embargo, esos trabajos pueden no ser las responsabilidades del desarrollador y se le asignará a otro individuo familiarizado con la aplicación de la base de datos.

2.2.7.4. Política administrativa de Contraseña.- La seguridad de los sistemas de base de datos depende de no divulgar las contraseñas en ningún momento. No obstante, son vulnerables al robo, falsificación y abuso. Para permitir un mayor control en la seguridad sobre las bases de datos, la política administrativa de contraseñas de Oracle es controlada por DBAs.

Esta sección describe los siguientes aspectos de la administración de contraseñas en Oracle:

- ✓ Cierre de cuenta
- ✓ Expiración de las contraseñas
- ✓ Verificación en la complejidad de contraseñas

Cierre de Cuenta.- Cuando un usuario excede un determinado número de intentos de accesos fallidos, el server automáticamente cierra la cuenta del usuario. DBA especifica el número permitido de accesos fallidos usando la sentencia CREATE PROFILE. También especifica el período de tiempo que la cuenta quedará cerrada.

Si el DBA no especifica el tiempo que tardará en habilitarse la cuenta nuevamente, el sistema toma un tiempo por default; y si el tiempo estipulado es ilimitado, el encargado del sistema de seguridad deberá directamente habilitar la cuenta. De esta manera, el período de tiempo que una cuenta permanece cerrada depende de cómo la DBA configura los recursos asignados al usuario.

El encargado de seguridad también puede directamente cerrar cuentas de usuarios. Cuando esto ocurre sólo el encargado de seguridad puede habilitarla nuevamente.

Expiración de las contraseñas.- El DBA usa la sentencia CREATE PROFILE para especificar un máximo de tiempo de vida de las contraseñas. Pasado este tiempo

la contraseña expira y el usuario deberá cambiarla. También puede especificar un período de gracia usando la misma sentencia.

Los usuarios ingresarán el período de gracia sobre el primer intento de login, a una cuenta de la base de datos, después de que su contraseña haya expirado. Durante el período de gracia, aparecerá un mensaje de advertencia cada vez que el usuario intente entrar en su cuenta, y continuará apareciendo hasta que expire el período de gracia. Si la contraseña no es modificada dentro de dicho período, la cuenta expirará y ningún intento de acceso será permitido hasta que no se modifique la contraseña.

El encargado de la seguridad puede también expirar directamente la cuenta. Esto es particularmente útil para generar nuevas cuentas.

Verificación en la complejidad de contraseñas.- La rutina de verificación de complejidad de contraseñas en Oracle puede ser especificada usando PL/SQL script, el cual fija los parámetros de default.

La rutina de verificación de la complejidad de las contraseñas representa los siguientes puntos:

- ✓ La contraseña tiene una longitud mínima de 4 posiciones
- ✓ Debe ser distinta que el user-id
- ✓ Tiene al menos un número, una letra y un punto
- ✓ No usar palabras simples tales como welcome, account, database o user
- ✓ La contraseña actual difiere de la contraseña anterior al menos en 3 letras

Oracle recomienda no cambiar las contraseñas usando la sentencia ALTER USER porque no soporta enteramente la función de verificación de contraseñas. En

cambio, si podría usar las herramientas que provee Oracle como SQL*Plus o Enterprise Manager para cambiar las contraseñas.

DBA (Database Access) puede mejorar las rutinas de verificación de complejidad de las contraseñas o crear sus propias rutinas de verificación de contraseña usando PL/SQL.

2.2.7.5. La Política de Auditoria.- Los administradores de Seguridad deben establecer una política para el procedimiento de auditoria de cada base de datos. Cuando es necesaria una auditoria el administrador de seguridad debe decidir a qué nivel de detalle se realizará la auditoría de la base de datos.

Una vez detectado alguna actividad de origen sospechosa a través del sistema general de auditoria, se realizará una auditoría más específica.

Trusted ORACLE.- Es un sistema de administración de la seguridad de bases de datos. Fue diseñado para proveer el más alto nivel de capacidades para la administración de la seguridad requerido por organizaciones que procesan información sensitiva. Trusted Oracle es compatible con todos los productos Oracle.

Además, Trusted Oracle implementa Mandatory Access Control (MAC) (control de acceso obligatorio). Mandatory Access Control es un medio para restringir el acceso a la información basado en etiquetas o rótulos. La etiqueta de un usuario indica a qué información le está permitido acceder a un usuario y con qué tipo de acceso (lectura o escritura). La etiqueta de un objeto indica la sensibilidad de la información que el objeto contiene.

Copia de seguridad y recuperación de la base de datos.- En cada sistema de base de datos siempre existe la posibilidad de una falla del sistema o de hardware. Si una falla ocurre y afecta la base de datos esta debe ser recuperada.

Los objetivos después de la falla son asegurar que los efectos de todas las transacciones realizadas se reflejen en la base de datos recuperada y retornar a la operación normal tan rápido como sea posible mientras se aísla a los usuarios.

Tipos de falla.- Varias circunstancias pueden detener la operación de una base de datos Oracle.

Los tipos de falla más comunes son:

Errores de usuario.- Los errores de usuario pueden requerir, para ser recuperados, de una base de datos en un punto anterior en el tiempo al que ocurrió el error.

Para permitir la recuperación a partir de los errores de usuario y acomodar otros requisitos únicos de recuperación, Oracle provee una recuperación exacta en el tiempo.

Fallas de sentencias y procesos.- Las fallas de sentencias ocurren cuando hay una falla lógica en el manejo de una sentencia en un programa Oracle.

Cuando ocurre una falla de sentencia los efectos de las sentencias se deshacen automáticamente por Oracle y se devuelve el control al usuario.

Una falla de proceso es una falla en un proceso de usuario accediendo a Oracle, tales como una desconexión o finalización de un proceso en forma anormal.

El proceso de usuario fallido no puede continuar trabajando, aunque Oracle y otro proceso de usuario puedan. El proceso subordinado de Oracle PMON detecta automáticamente los procesos de usuario fallidos o es informado de este hecho por SQL[5] Net. PMON resuelve el problema realizando una regresión de las transacciones realizadas y liberando los recursos que estaban tomados por el proceso fallido.

Falla de una copia de programa en memoria.- Una falla de una copia de programa en memoria puede resultar por un problema de hardware como la salida de energía o un problema de software como la caída del sistema operativo.

Cuando ocurre una falla de este tipo la información de los buffers del área global del sistema no se escribe en los archivos. Esta falla requiere recuperar la copia del programa en la memoria

La recuperación de la instancia se lleva a cabo automáticamente por Oracle cuando la instancia se reinicializa.

El Redo log se usa para recuperar los datos en los buffers del SGA.

Falla en disco.- La falla en disco es un problema físico cuando se lee o escribe un archivo en disco.

La recuperación del medio restablece los archivos de la base de datos con la información correspondiente al instante más reciente antes de la falla, incluyendo la información que se perdió a causa de la falla. Se requiere lo siguiente: copia de seguridad de los archivos de la base de datos

Si algunos archivos de datos se dañan, en una falla de disco, pero la mayor parte de la base de datos está intacta, la base de datos puede permanecer abierta mientras la “tablespaces” requeridas se recupera individualmente.

Por consiguiente las porciones no dañadas de una base de datos están disponibles para su uso normal mientras se recuperan las porciones dañadas

Estructuras utilizadas para la recuperación.- Oracle utiliza diversas estructuras para proveer una recuperación completa a causa de una falla de una copia del programa en memoria del disco: el redo log, segmentos de rollbak, un archivo de control y copia de seguridad de la base de datos necesarias.

El Redo Log.- El Redo Log es un conjunto de archivos que protegen la información de la base de datos alterada que aún no ha sido escrita en los archivos.

El Redo Log puede consistir en 2 partes:

El Redo Log en línea (online).- Registra todos los cambios hechos a la base de datos. Cuando se envía una transacción en la base de datos, se guarda en forma temporal la entrada correspondiente del Redo log en los buffers del SGA, que luego el proceso subordinado LGWR escribe en un archivo Redo log en línea.

El Redo Log almacenado (offline).- Se almacenan mediante archivos.

Archivos de control.- Los archivos de control de una base de datos mantienen, entre otras cosas información sobre la estructura de los archivos de una base de datos y el número de secuencia del log actual que está siendo escrito por LGWR (Es el único proceso que escribe en los ficheros de redo log y el único que lee directamente los buffers de redo log durante el funcionamiento normal de la BD).

Durante los procedimientos normales de recuperación.

Segmentos de regresión (rollback segments).- Los segmentos de regresión graban información usada por distintas funciones de Oracle.

Durante la recuperación de la base de datos, después que todos los cambios grabados en el Redo log han sido aplicados. Oracle utiliza información de los segmentos rollback para deshacer cualquier transacción realizada. Debido a que los segmentos rollback se almacenan en los buffers de la base de datos, esta importante información de recuperación es automáticamente protegida por el redo log.

Copias de Seguridad de la Base de Datos.- Debido a que uno o más archivos pueden ser físicamente dañados como consecuencia de una falla del disco, la

recuperación del medio requiere restauración de los archivos dañados desde el backup más reciente.

Hay varias formas de hacer copias de seguridad de los archivos de una base de datos:

Copia de seguridad completa de una base de datos.- Es una copia de seguridad de todos los archivos de datos, archivos redo log en línea, y el archivo de control.

Las copias de seguridad completas se realizan cuando se cierra la base de datos y queda inhabilitada para su uso.

Copias de seguridad parciales.- Es una copia de una parte de la base datos. La copia de seguridad de un tablespace individual o la copia de seguridad de un archivo de control son ejemplos de backups parciales.

Pasos básicos de recuperación.- Debido a la forma en que la información de los buffers se graba en los archivos puede ocurrir que en un momento dado:

- ✓ Un archivo contenga datos modificados por transacciones no ejecutadas
- ✓ Un archivo no contenga algunos datos modificados por transacciones ejecutadas.

Para solucionar esta situación, Oracle siempre utiliza dos pasos separados durante la recuperación de una falla de un medio o una falla de una copia de un programa en memoria:

Avance (Rolling Forward).- Consiste en aplicar a los archivos de datos todos los cambios grabados en el Redo Log, llevando (adelantando) los archivos de datos al punto de tiempo requerido.

Si todo la información del Redo Log está en línea, Oracle ejecuta este paso de recuperación de manera automáticamente se inicia la base de datos. Después de realizado este paso los archivos de datos contienen todos los cambios realizados por transacciones ejecutados y por transacciones no ejecutadas, grabados en el Redo Log.

Retroceso (Rolling Back).- Se utilizan los segmentos de retroceso (Rollback Segments) para identificar las transacciones que nunca se ejecutaron, pero que están grabadas en el Redo Log. Oracle realiza este paso automáticamente.

El administrador de la Recuperación.- Es una herramienta de Oracle que lleva a cabo las operaciones referidas a las copias de seguridad y a la recuperación de la base de datos.

Este mantiene un catálogo de recuperación, el cual contiene información sobre las copias de seguridad de archivos y de los Redo Logs offline.

2.2.8. Vulnerabilidades Físicas A menudo suelen relacionarse aspectos de seguridad física, con la primera etapa en la historia de la computación.

A pesar de los muchos avances en aquellos aspectos relacionados con la seguridad lógica, la seguridad física continua siendo hoy día, un factor fundamental de la estrategia global de toda organización.

La seguridad física continúa siendo tan relevante hoy día como lo era hace treinta años.

Aún sigue siendo necesario proteger el cuarto de servidores, limitando el acceso al mismo e instalando los cerramientos apropiados.

Un aspecto interesante de la evolución en la seguridad física, se encuentra relacionado con la complejidad que esta reviste en la actualidad, en contraposición a la revestida en décadas anteriores, donde gran parte del problema pasaba por

proteger el sitio donde se albergaba el mainframe (Una computadora que es capaz de compartir los recursos con muchas otras computadoras de menor capacidad).

Recientemente, el crecimiento de la computación portable, ha expandido la necesidad de direccionar la seguridad física más allá de los límites tradicionales, convirtiendo este punto en un aspecto sumamente delicado.

La seguridad física ha requerido un cuidado especial en los últimos años, principalmente debido a la amenaza terrorista

En la actualidad, varias son las iniciativas del gobierno y del sector privado, respecto de la protección de la infraestructura crítica de los países.

Las amenazas a la infraestructura se han vuelto en muchos casos globales y pueden materializarse en diversas formas.

Es importante notar que las amenazas a la infraestructura tienen múltiples efectos, incluyendo el riesgo para los sistemas de información.

La seguridad física provee protección para los edificios, estructuras, vehículos conteniendo sistemas de información y cualquier otro componente de red. De acuerdo a sus características, los sistemas son referidos como estáticos, móviles o portables.

- ✓ Sistemas Estáticos (Static Systems)

  Son instalados sobre estructuras en ubicaciones fijas.

- ✓ Sistemas Móviles (Mobile Systems)

  Son instalados en vehículos o sitios que cumplen la función de estructura móvil.

- ✓ Sistemas Portables (Portable Systems)

Pueden ser operados en cualquier parte (edificios, vehículos o en lugares abiertos)

Una característica distintiva de la seguridad física, es que esta representa el tipo más obvio de seguridad.

Esto se debe a que en la mayoría de los casos esta es visible. Las personas pueden ver cerraduras, paneles de alarma y guardias de seguridad.

Debido a que tanto los empleados como las personas ajenas a la organización pueden ver estos controles, los mismos pueden dar una señal de la postura de seguridad tomada por la organización.

Un posible intruso, que obtiene una primera impresión a partir de los dispositivos de seguridad que puede “ver”, probablemente sospeche que será necesario trabajar arduamente a fin de saltear tales protecciones y ganar acceso al edificio. (Disuasión)

Si bien es cierto que los controles lógicos ayudan a proteger los recursos de la organización, ellos no pueden detener a quienes pueden tener acceso físico a los mismos.

En base a los datos expuesto la Clínica Humanitaria tiene la necesidad de implementar en su centro de cómputo niveles de seguridad los mismos que le permitirán mantener niveles de seguridad con el fin de precautelar la información que se alberga en dicho centro, teniendo en cuenta que la información es el bien más preciado de toda institución es necesario que ésta esté a buen recaudo pero para ello es necesario conocer cuáles son las limitaciones y los peligros a los que se encuentra expuesta ésta información para tomar las correspondientes acciones preventivas y correctivas para el centro de cómputo lo que repercutirá en la institución.

CAPITULO III

3. METODOLOGÍA

3.2. METODOLOGIA DE ANALISIS DE RIESGO

3.2.1. Estudio inicial

Es el establecer los colaboradores, determinar el lugar informático en el que se va a llevar a cabo el estudio, con el fin de conocer el área es necesario diseñar una Lista de verificación para obtener información de importancia del centro lo que nos permitirá realizar una evaluación inicial, verificar los manuales de políticas y reglamentos.

3.2.2. Procedimientos y técnicas de auditoria.- Existen objetivos de control y procedimientos de auditoria que después de evaluar los riesgos es necesario identificar las fortalezas y debilidades en los controles existentes basados en la información recopilada para posteriormente generar el correspondiente informe el mismo que debe ser redactado de manera objetiva para la gerencia, la misma que debe tener la disponibilidad para implementar los correctivos necesarios al igual que mantener las revisiones periódicas de los seguimientos emprendidos.

3.2.3. Evaluación de Riesgo.- La evaluación de riesgos determina las vulnerabilidades amenazas y riesgos para generar un plan de controles que contemplen los criterios de un centro de cómputo seguro mediante los parámetros de disponibilidad, confidencialidad e integridad de la información, teniendo en cuenta los siguientes puntos:

- ✓ La probabilidad de amenaza
- ✓ El impacto sobre el centro en base a los parámetros de disponibilidad, confidencialidad e integridad de la información.

3.2.4. Determinación de la probabilidad.- Es necesario tomar en cuenta los siguientes parámetros para determinar la probabilidad que ocurra un evento

- ✓ Origen de la Amenaza
- ✓ Causa de la vulnerabilidad.

Se deben clasificar las probabilidades de que una vulnerabilidad potencial sea explotada por una fuente de amenaza en Grave, Alto, Medio y Nulo.

NIVEL	DEFINICIÓN	Mínimo de probabilidad que suceda
Grave	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo.	2 veces al año.
Alto	La amenaza está fundamentada y es posible.	1 vez al año.
Medio	La amenaza es posible.	0,5 veces al año.
Nulo	La amenaza no posee la suficiente motivación y capacidad.	0,25 veces al año.

Fig1. Cuadro de Nivel de impacto de las vulnerabilidades.

3.2.5. Numero de ocurrencias del evento en un periodo.- Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de información, modificación de datos, utilizamos información obtenida de ciertas publicaciones tecnológicas con relación similar a los eventos que se desea estudiar. De esta manera se define una escala en la cual, una amenaza grave está

considerada una probabilidad que suceda al menos dos veces al año, amenaza de categoría Alto que suceda al menos una vez al año, una amenaza de categoría Medio una probabilidad de 0,5 veces al año y por último para una amenaza de categoría Nulo una probabilidad de 0,25 veces al año.

3.2.6. Identificación de Vulnerabilidades.- Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se utilizan herramientas como listas de verificación y herramientas de software que determinen las vulnerabilidades.

3.2.7. Análisis del impacto y el factor de riesgo.- El próximo paso en la metodología que estamos describiendo, es poder determinar el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, para ello se deben considerar los siguientes aspectos

- ✓ Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.
- ✓ La importancia crítica de los datos y el sistema (importancia a la organización).
- ✓ Sensibilidad de los datos y el sistema.

3.2.8. Identificación de Controles.- En esta fase se evaluarán las conclusiones de la valoración y la matriz de riesgo con el fin de identificar los controles que mitiguen los riesgos encontrados.

3.2.9. Definición de Políticas.- Las Políticas de seguridad dependen de la cultura de la organización. Por esta razón las políticas y procedimientos deben estar hechos a la medida, según los requerimientos específicos de cada organización. Para la definición de las políticas y procedimientos se realiza un proceso de

validación en conjunto con la organización con el fin de generar políticas y procedimientos que se ajusten a esta. Como punto de partida para la definición de las políticas se tendrá como referencia el análisis de riesgo realizado.

3.2.10. Alcance de las Políticas

Seguridad en la Organización

- ✓ Roles y Responsabilidades de Seguridad de la Información
- ✓ Políticas para el manejo de la información.

Clasificación de la Información

- ✓ Importancia de la información según la organización

Administración de las operaciones de cómputo y comunicaciones

- ✓ Políticas sobre el uso del correo electrónico
- ✓ Políticas sobre el uso de clave de acceso.
- ✓ Políticas sobre el uso de recursos.

3.2.11. Definición de estándares.- Es la definición cuantitativa o cualitativa de un valor o parámetro determinado que puede estar incluido en una política o procedimiento, Algunos de los principales estándares a definir son:

- ✓ Longitudes de contraseñas.
- ✓ Histórico de contraseñas,
- ✓ Eventos a registrar.

3.3. Análisis de vulnerabilidades Físicas del CPD[1]

3.3.1. Control de acceso físico al CPD[1]

Para mantener la seguridad de un CPD[1] es necesario comprender que éste lugar es en donde se encuentran los datos más valiosos de una institución se debe considerar que la seguridad física es de vital importancia para este lugar ya que, el no restringir los accesos al CPD[1]se está exponiendo los datos y la información más vulnerable a que sea susceptible de sustracción, alteración, modificación, etc. Es necesario mantener un control de entrada y salida del personal, al igual que de los equipos y sus componentes, en la Clínica se cuenta con varios métodos de seguridad aplicadas como:

3.3.1.1. Ubicación del CPD[1].- Es recomendable que la ubicación sea entre la primera o segunda planta del edificio, para evitar los riesgos de las plantas altas y bajas (inundaciones, goteras etc.), que su ubicación no esté señalizada, que no tenga ventanas etc.

La ubicación del CPD[1]en la Clínica Humanitaria se encuentra en la segunda planta, el lugar no cuenta con señalización que indique en donde se encuentra dicho centro, El cuarto cuenta con un sistema de enfriamiento y no cuenta con ventanas es decir que no incurre con las normas específicas para la implantación de un CPD[1].

ANÁLISIS DE VULNERABILIDAD POR UBICACIÓN DE CPD				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	**Alto**	**Medio**	**Nulo**
Riesgo de Inundación por goteras				X
Riesgo de sabotaje por estar visible				X

La ubicación del CPD está Señalizada				X

Fig2. Análisis de vulnerabilidad por ubicación de CPD

3.3.1.2. Suelo falso o techo falso

De acuerdo a las recomendaciones para un CPD[1]dice que debe existir un suelo o techo falso por donde se distribuye el cableado, el mismo que debe ser de material no inflamable debe mantener las distancias respecto del suelo real. De igual manera se debe mantener un aseo en dicho lugares, se debe tener detectores de humedad, un sistema de detección de incendios etc.

El CPD[1]cuenta con un techo falso, pero a su vez éste no cumple con las especificaciones técnicas en la que se solicita que sea de material no inflamable, no se cuenta con detector de humedad para este lugar a pesar que sobre este cuarto se encuentra una estructura de hormigón armado lo que no permitirá que se filtre humedad por causa de goteras y de igual manera se cuenta con un sistema de circulación de aire para evitar que las corrientes de aire generen humedad, El centro cuenta con un extintor de incendio el mismo que es de CO2 el recomendado para equipos electrónicos, el mantener un extintor de incendios no significa que este asegurado al existir un siniestro de incendio ya que para su acción necesita contar con un sistema automático de detección de incendios.

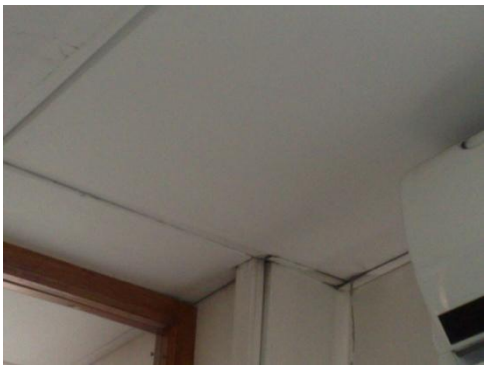


Fig3. Techo falso del CPD.

Análisis de vulnerabilidad por Suelo falso o Techo falso				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Debe disponer de un suelo o techo falso			**X**	
El suelo falso o techo falso sirve para distribuir el cableado			**X**	
El suelo falso o techo falso es de material no inflamable		**X**		
Se debe mantener un aseo en el suelo falso o techo falso lugares			**X**	
Se debe tener detectores de humedad en el suelo falso o techo falso			**X**	
Se debe tener sistema de detección de incendios	**X**			

Fig4. Análisis de vulnerabilidad por Suelo falso o Techo falso

3.3.1.3. Dispositivo Biométrico

La Biometría, esta tecnología está basada en el reconocimiento de características físicas e intransferibles de los seres humanos, tales características como la huella digital, estos sistemas biométricos utilizan dos dispositivos, un software de captura y un dispositivo biométrico (lector), es necesario aclarar que la huella digital no es una imagen sino un sistema complejo en el que se comparan diversos patrones, esta tecnología se utiliza para brindar un acceso seguro a equipos de computación

o redes informáticas, protección de información al igual que para llevar el control de horarios y acceso físico de cierto personal en áreas restringidas**.**

La ventaja principal de esta tecnología es la seguridad debido a que los sistemas de contraseñas o tarjetas pueden ser hurtadas, de ésta manera se garantiza el acceso a una PC o una sala restringida teniendo en cuenta que para hacerlo no depende de algo que se necesite conocer o algo adicional que tengamos, sino que, todo lo contrario depende de lo que somos y en lo que se basó para tomar como nuestra identificación.

Esta tecnología funciona de la siguiente manera, cuando la huella digital es el medio de identificación que se ha dispuesto, el dispositivo biométrico captura la huella y el software capta los puntos característicos de la huella lo procesa y lo transforma en un resultado matemático por medio de algoritmos que no pueden ser llevados en inversa, por esta razón los sistemas biométricos son considerados como de alta seguridad, el resultado al proceso matemático aplicado a la huella que se autenticó es comparado con la información antes almacenada en una base de datos segura la misma que servirá para permitir o denegar el acceso, al igual que o a su vez para registrará el momento del acceso.

La clínica humanitaria cuenta con un sistema de acceso biométrico, el mismo que se encarga de registrar el acceso del personal a la institución con la finalidad de mantener un control en el departamento de Gestión del Factor Humano sin embargo este sistema no se encuentra empleado para el acceso al Centro de cómputo.

Fig5. Acceso al CPD.

ANÁLISIS DE VULNERABILIDAD POR DISPOSITIVO BIOMÉTRICO				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Se utiliza la tecnología de dispositivos biométricos como seguridad del CPD	X			

Fig6. Análisis de vulnerabilidad por Dispositivo Biométrico

3.3.1.4. Procedimiento de autorización de acceso al CPD[1]

La autorización al centro de cómputo se debe establecer a través de un procedimiento por medio del cual se especifique los requerimientos para dicho acceso.

Es necesario generar un listado de autorización el mismo que debe contener la información esencial, de tal manera que el administrador del centro o quien se encuentre a cargo de la seguridad del CPD[1]pueda conocer y ubicar a dicha persona para realizar las labores que se encuentren descritas en el documento de autorización, con la finalidad de que el personal no acceda a información que no es necesaria y a su vez que ésta información no sea susceptible de hurto o de alteraciones éste documento debe contener la firma de quien autoriza o solicita dicho acceso éste documento debe contener la siguiente información:

Nombre, cargo, número de cédula o pasaporte de cada una de las personas que conforman el Listado.

Existe explícitamente un documento en la institución la misma que determina las obligaciones de los encargados del centro de cómputo en la que dice: que el administrador y su asistente son los responsables y quienes autorizan el acceso al

centro de cómputo por ser ellos quienes tienen el criterio de seguridad. Es decir que el criterio para permitir el acceso ya sea de manera lógica como de manera física se encuentra en manos de los encargados del CPD[1], sin embargo vía e-mail se encuentra registrado las solicitudes de acceso al nuevo personal que se incorpora a la institución y que requiere el acceso al sistema informático, de igual manera con el fin de actualizar los usuarios del sistema se envía vía e-mail los egresos del personal, es decir cuando un empleado ha dejado de laborar en la institución.

ANÁLISIS DE VULNERABILIDAD POR AUTORIZACIÓN DE ACCESO				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Existe un procedimiento de autorización de acceso al CPD.			X	
El procedimiento de autorización de acceso se encuentra accesible para los administradores.		X		
Existe detallado un listado de autorizaciones de acceso al CPD	X			
Está determinada las labores de la persona a quien se autoriza el ingreso al CPD	X			
Los documentos se encuentran registrados con las debidas firmas de autorización de acceso al CPD		X		

Fig7. Análisis de vulnerabilidad por autorización de acceso

3.3.1.5. Sistemas de seguridad y vigilancia mediante cámaras

Dentro de la tecnología de seguridad se ha implementado de manera eficaz y con grandes avances las cámaras de seguridad teniendo como ventaja el ejercer una vigilancia preventiva mediante el registro visual de cada suceso que registran las diferentes cámaras que se llegan a disponer en un determinado lugar. El uso de los equipos de videograbación va dirigido a asegurar el amplio espectro de lugares en los que la seguridad necesita de un gran apoyo como son dichas cámaras. Los lugares en los que se emplean van desde Empresas de diversos tipos, Centros Comerciales, Aeropuertos, Entidades Bancarias, Vías públicas, etc.

Al tener una o a su vez un grupo de cámaras conectadas hasta un servidor en donde se registran cada una de las imágenes que son capturadas por dichas cámaras se lo denomina CCTV (Closed Circuit Television), no todos los circuitos cerrados cuentan con un ordenador de almacenamiento de los datos registrados, ya que también existen CCTV que no necesitan almacenar la información almacenada. Este circuito cerrado puede contar con uno o varios monitores desde los cuales se vigila, se denomina circuito cerrado debido que, todos los componentes se encuentran interconectados. Además, a diferencia de la televisión convencional, este sistema está diseñado para una cantidad limitada de usuarios.

En la actualidad las cámaras permiten ser controladas remotamente desde un lugar de monitorización en el que se controla su panorámica (Es el amplio horizonte visual que presenta una imagen), inclinación y zoom.

Las cámaras de la actualidad incluyen visión nocturna, proceso asistidos por un ordenador y detección de movimiento que facilita al sistema estar en modo de alerta cuando se realiza un movimiento frente a la cámara.

Una cámara que tiene como función el de activarse al detectar movimientos se utiliza en los sistemas que lo controlan ya que estos equipos se encuentran

registrando el movimiento mientras se encuentren encendidos, su función es el de comparar con una imagen congelada, al momento que esta imagen ha cambiado el ordenador al que se encuentra conectado empieza a registrar los eventos que dicha cámara envía hasta dicho equipo, ésta función permite que en el ordenador se optimice el espacio de almacenamiento para grabar solamente cuando exista movimiento.

La Clínica Humanitaria cuenta con un CCTV el mismo que se encuentra distribuido por la clínica con 16 cámaras las mismas que su información se almacena en el servidor de cámaras, cada cámara cuenta con la función de registrar ya sea cuando hay iluminación o al no existir es decir equipos con visión nocturna y a colores, el sistema de almacenamiento es administrado mediante un software llamado “GEOVISION” éste software se encarga de almacenar solamente cuando detecta movimiento ya que las cámaras en todo momento se encuentran enviando información el inconveniente detectado es que tiene un margen de respuesta después de registrar el movimiento.

La información que se encuentra almacenada en el ordenador es usada solamente para confirmación o verificación, teniendo acceso los administradores y la dirección médica, ésta información tiene un tiempo de almacenamiento de hace un mes atrás, para acceder a esta información se lo hace remotamente mediante la aplicación GEOVISION para cliente el mismo que otorga permisos para configuración o para eliminación de datos mediante autenticación.

El uso de esta herramienta como seguridad es correcta pero el uso no es el adecuado ya que se ha concebido a ésta tecnología para confirmación y no para detección ya que no se está monitoreando constantemente y no existe el lugar, el personal y el equipo para realizar la correspondiente monitorización.

Fig8. Cámara de vigilancia de acceso al CPD.

ANÁLISIS DE VULNERABILIDAD FÍSICA POR VIGILANCIA MEDIANTE CÁMARAS				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
La cámara de seguridad se usa para vigilancia preventiva	**X**			
Las imágenes proyectadas por las cámaras de seguridad se encuentran almacenadas				**X**
Cuenta con monitorización las cámaras de seguridad		**X**		
El Espectro que cubre las cámaras de seguridad son la correcta			**X**	
Puede ser controladas las cámaras de seguridad remotamente			**X**	
Las cámaras de seguridad incluyen				**X**

visión nocturna				
La cámara de seguridad registra la información al detectar movimiento				X
El tiempo de espera entre el momento que se genera el movimiento y el registro en el ordenador			X	

Fig9. Análisis de vulnerabilidad física por vigilancia mediante cámaras

3.3.1.6. Climatización del centro de cómputo

La climatización es un proceso de tratamiento que se da al aire de un determinado lugar con el propósito de mantener condiciones ambientales adecuadas, controlando temperatura, humedad, calidad y distribución del aire en un determinado ambiente, el objetivo de realizar este proceso es el de satisfacer las necesidades para un determinado proceso o producto electrónico.

Un CPD[1] debe mantener condiciones ambientales adecuadas para los equipos ya que de esta manera se garantiza la integridad de la información y la confiabilidad de las operaciones de los equipos por periodos más largos, En la Clínica Humanitaria se encuentra instalado un sistema de climatización independiente, el mismo que permite mantener una temperatura de 21º C. y con una humedad promedio de 5%. El área que se climatiza es de 10m2, es el lugar en el que se encuentran los diferentes servidores de la institución.

Fig10. Climatizador del CPD.

Análisis de vulnerabilidad Física Climatización del centro de cómputo				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
La temperatura del CPD se mantiene en un rango de 21°C y 23°C				**X**
Existe un control de humedad del CPD	**X**			
La instalación del Climatizador se realizó mediante un estudio adecuado.	**X**			

Fig11. Análisis de vulnerabilidad Física Climatización del centro de cómputo

3.4. Análisis de vulnerabilidades Lógicas cuando se accede a la BD

3.4.1. Acceso Lógico al centro de cómputo cuando se accede a la BD del sistema Informático

3.4.1.1. Privilegios para los usuarios en BD

Privilegios de sistema.- Los Privilegios de sistema permiten a los usuarios desempeñar una acción particular dentro del sistema o sobre un tipo determinado de objeto. Por ejemplo, el privilegio para crear un Tablespace o para borrar filas de una tabla en la base de datos, son privilegios de sistema.

Muchos privilegios de sistema están disponibles solamente para administradores y desarrolladores de aplicaciones porque estos privilegios son muy poderosos.

Privilegios de objetos.- Los privilegios de objetos permiten a los usuarios desempeñar acciones sobre un esquema específico. Por ejemplo, el privilegio para borrar filas de una tabla específica es un privilegio de objetos.

Los privilegios de objetos son asignados a usuarios finales, entonces ellos pueden usar una aplicación de la base de datos para llevar a cabo tareas específicas.

Asignar privilegios.- Un usuario puede recibir un privilegio de dos formas distintas:

- ✓ Los privilegios pueden ser asignados a los usuarios explícitamente.
- ✓ Los privilegios pueden ser asignados a roles (grupo de privilegios), y después el rol puede ser signado a uno o más usuarios.

Debido a que los roles permiten una mejor y más fácil administración de los privilegios, éstos normalmente son asignados a roles y no a usuarios específicos.

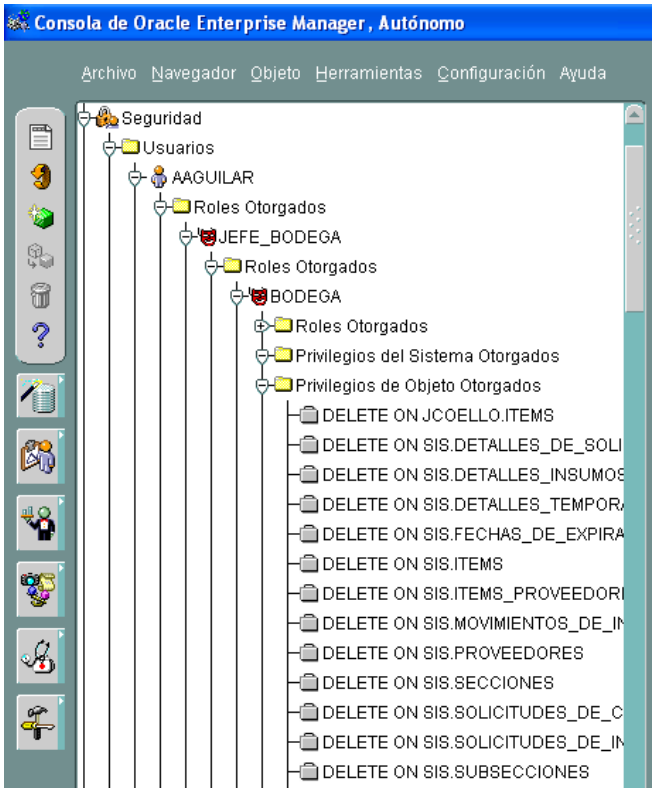


Fig12. Usuario y Privilegios otorgados en la BD.

ANÁLISIS DE VULNERABILIDAD DE ACCESO LÓGICO A LA BD MEDIANTE PRIVILEGIOS				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Los privilegios hacia los usuarios comunes son controlados por el Administrador del CPD			**X**	
Los privilegios se encuentran otorgados en base a roles				**X**
Existen roles generados en base a los perfiles.				**X**

Fig13. Análisis de vulnerabilidad de acceso Lógico a la BD mediante privilegios

3.4.1.2. Programas de control de acceso.- Los programas administradores de BD son los que gestionan desde las credenciales de los usuarios hasta el grado de privilegios que tiene un usuario hacia los recursos que estén expuesto en la red para el correspondiente consumo de quien solicite, de igual manera el administrador debe llevar un control de mantenimiento sobre los eventos o suceso que se generen en la Base de Datos llamados Log's (Registro oficial de eventos durante un rango de tiempo en particular.). Este administrador permite mantener un control de seguridad sobre credenciales y privilegios de una manera gráfica para su administración adecuada.

Definición de usuarios.- Pararealizar la definición de usuarios comunes se debe identificar cuáles son las tareas que van a realizar estos usuarios ya que no podrán tener los mismos privilegios que tiene un administrador de sistema un

programador o el gerente de la empresa por ésta razón el administrador de la BD permite generar tipos o los conocidos roles que son los que agrupan a cada uno de los privilegios para diferentes grupos es decir que para cada uno de los cargos antes mencionados tendremos un grupo de privilegios que se encuentran enmarcados bajo un solo nombre lo que permite una mejor administración y asignación para los usuarios.

Para generar los roles es necesario que se encuentren claramente identificado cuales son las tareas específicas de los usuarios de acuerdo a su perfil laboral lo que permitirá realizar un rol apegado al trabajo específico del usuario.

El software de la Clínica Humanitaria al ser un software comercial es decir que fue adquirido, y no desarrollado específicamente por dicha institución, los usuarios y roles han sido generados de acuerdo a las actividades que deben realizarse en el sistema informático, es decir que al adquirir el sistema medico informático los usuarios empezaron a tomar ciertas actividades nuevas y algunas a dejar de realizarlas ya que estaban asignadas a otras áreas o departamentos según el software, es por eso que los roles fueron generados sin basarse en los perfiles de los usuarios de la clínica y a su vez ha sido lo contrario, en base al sistema se han ido generando los perfiles de los diferentes cargos en los que influyen el sistema informático de manera directa.

ANÁLISIS DE VULNERABILIDAD DE ACCESO LÓGICO A LA BD MEDIANTE PROGRAMAS DE CONTROL DE ACCESO				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Se realiza control de credenciales				**X**

Se realiza el control de Log's de la BD			X	
Existe un procedimiento para realizar el proceso de monitoreo mediante un programa de control hacia la BD.		X		
El programa permite gestionar nuevos usuarios al igual que eliminar usuarios de la BD				X
Para generar un nuevo usuario, se encuentre detallado el perfil que va a cumplir.				X
Se encuentra documentado las solicitudes de los nuevos usuarios con los respectivos perfiles				X
Se encuentra documentados los usuarios que has sido eliminados de la BD				X

Fig14. Análisis de vulnerabilidad de acceso Lógico a la BD mediante programas de control de acceso.

3.4.1.3. Inyección SQL[5].- Se conoce como inyección SQL[5] el método de introducir código SQL[5] mediante una aplicación que tiene acceso a la base de datos la misma que no cuenta con las medidas adecuadas de seguridad frente a una consulta a realizar contra una Base de Datos.

Cuando la plataforma de base de datos falla para desinfectar las entradas, los atacantes son capaces de ejecutar las inyecciones SQL[5] de tal manera que

permite elevar los privilegios del atacante y obtener acceso a una amplia gama de funcionalidades.

Muchos de los proveedores han dado a conocer soluciones para evitar estos problemas, pero no servirá de mucho si los parches no se aplican o no se toman los correctivos correspondientes.

Este proceso de ataque se realizó en las aplicaciones de la institución dando como resultado que esta vulnerabilidad se encuentra corregida debido a las proceso de seguridad que se establecieron al momento de generar el programa por parte de los comercializadores del software medico informático.

ANÁLISIS DE VULNERABILIDAD DE ACCESO LÓGICO A LA BD POR CONTROL DE ACCESO POR INYECCIÓN SQL				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Pruebas de inyección SQL[5]				**X**
La existencia de registros de pruebas de inyección SQL[5]a la BD[1]		**X**		
Correctivos con relación a los hallazgos encontrados		**X**		

Fig15 Análisis de vulnerabilidad de acceso lógico a la BD por control de acceso por inyección SQL[5]

3.4.1.4. Identificación y autenticación de usuarios.- El identificar se denomina al proceso de diferenciar a una persona de otra, el autenticar es validar a través de algún método que la persona que dice ser sea la correcta.

El llegar a determinar una manera adecuada para el control de identificación y autenticación no es muy fácil o a su vez tienen un costo muy alto. Los modelos más generalmente usados se basan en técnicas tales como:

Lo que el usuario sabe.- Generalmente las claves de acceso que pueden utilizarse acceso a una Base de Datos. Es el método comúnmente usado. La manera de brindar características de seguridad es el de mantener un período de expiración de la clave la misma que no puede repetirse con las ultimas diez utilizadas o el número que el administrados decida de acuerdo al grado de seguridad que se dese brindar a nuestra base de datos.

El tipo de contraseña también es otro control que se adiciona a la seguridad implementada al usuario, se asigna un número de caracteres mínimos para la contraseña al igual que se obliga que sea de tipo alfanumérico lo que permite que se realice por lo menos una combinación para la creación de claves si a esto se añade la restricción del uso de nombres, apellidos, fecha de nacimiento o datos que pertenezcan a la información personal del usuario se estaría fortaleciendo este sistema de seguridad.

Algo específico del usuario.- Cada uno de los usuarios tienen características corporales únicas e intransferibles lo que permite que se pueda aplicar una seguridad más óptima sabiendo que realmente es el usuario que tiene los permisos para alguna actividad específica podríamos citar las características faciales, huellas dactilares, voz, etc.

Estos controles son los más automatizados dentro de esta clasificación. Los controles biométricos ya fueron descriptos en detalle anteriormente.

Hay una gran variedad de controles de este tipo, generalmente basados en las siguientes características del usuario:

- ✓ Huellas dactilares

- ✓ Patrones de la retina
- ✓ Geometría de la mano
- ✓ Dinámica de la firma
- ✓ Patrones de la voz

La seguridad aplicada para el acceso lógico por parte del usuario a la BD de la Clínica Humanitaria es el uso de usuario y contraseña, el sistema tiene la opción de permitir realizar cambios de contraseña sin límite de tiempo superior o inferior para la contraseña nueva, esto quiere decir que los usuarios tienen total libertad de realizar cambios en la contraseña las veces que el usuario desee, sin embargo existen usuarios que tienen su clave de acceso con un mínimo de tres caracteres y no se ha cambiado desde que se les ha otorgado el acceso al sistema informático es decir que alguna personas no han cambiado su clave por más de un año atrás, esto quiere decir que no se está cumpliendo con los parámetros de seguridad que se deberían los mismos que permitirán mantener un grado de seguridad adecuado a la información que se genera por parte de los usuarios.

ANALISIS DE VULNERABILIDAD DE ACCESO LOGICO A LA BD POR IDENTIFICACIÓN Y AUTENTICACION DE USUARIOS				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Los usuarios se autentica mediante claves de acceso				**X**
Las claves de acceso se encuentran administradas mediante una BD				**X**

Las claves tiene estipulado un período de expiración de la clave		**X**		
La clave otorgada es susceptible de cambio por parte del usuario				**X**
Esta registradas las ultimas diez contraseñas utilizadas por el usuario	**X**			
El número de caracteres y tipo de caracteres para la contraseña es controlado		**X**		

fig16. Análisis de vulnerabilidad de acceso lógico a la BD por identificación y autenticación de usuarios.

3.5. Matriz de vulnerabilidades encontradas

MATRIZ VULNERAVILIDADES FISICAS DETECTADAS EN EL CPD DE LA CLINICA HUMANITARIA PABLO JARAMILLO C			
DESCRIPCION	**NIVEL VULNERABILIDAD**		
	Grave	**Alto**	**Medio**
Se debe tener sistema de detección de incendios	**X**		
Se utiliza la tecnología de dispositivos biométricos como seguridad del CPD	**X**		
Existe detallado un listado de autorizaciones de acceso al CPD	**X**		
Está determinada las labores de la persona a quien se autoriza el ingreso al CPD	**X**		
La cámara de seguridad se usa para vigilancia preventiva	**X**		
Existe un control de humedad del CPD	**X**		
La instalación del Climatizador se realizó mediante un estudio adecuado.	**X**		

Fig17. Matriz vulnerabilidades físicas con nivel “Grave” detectadas en el CPD de la Clínica Humanitaria Pablo Jaramillo C

.

MATRIZ VULNERAVILIDADES FISICAS DETECTADAS EN EL CPD DE LA CLINICA HUMANITARIA PABLO JARAMILLO C			
DESCRIPCION	**NIVEL VULNERABILIDAD**		
	Grave	**Alto**	**Medio**
El procedimiento de autorización de acceso se encuentra accesible para los administradores.		**X**	
El suelo falso o techo falso es de material no inflamable		**X**	
Los documentos se encuentran registrados con las debidas firmas de autorización de acceso al CPD		**X**	
Cuenta con monitorización las cámaras de seguridad		**X**	

Fig18. Matriz vulnerabilidades físicas con nivel “Alto” detectadas en el CPD de la Clínica Humanitaria.

MATRIZ VULNERAVILIDADES FISICAS DETECTADAS EN EL CPD DE LA CLINICA HUMANITARIA PABLO JARAMILLO C			
DESCRIPCION	**NIVEL VULNERABILIDAD**		
	Grave	**Alto**	**Medio**
Debe disponer de un suelo o techo falso			**X**
El suelo falso o techo falso sirve para distribuir el cableado			**X**
Se debe mantener un aseo en el suelo falso o techo falso lugares			**X**
Se debe tener detectores de humedad en el suelo falso o techo falso			**X**
Existe un procedimiento de autorización de acceso al CPD.			**X**
El Espectro que cubre las cámaras de seguridad son la correcta			**X**
Puede ser controladas las cámaras de seguridad remotamente			**X**
El tiempo de espera entre el momento que se genera el movimiento y el registro en la pc ordenador			**X**

Fig19. Matriz vulnerabilidades físicas con nivel “Medio” detectadas en el CPD de la Clínica Humanitaria.

MATRIZ VULNERAVILIDADES LOGICAS DETECTADAS EN EL CPD DE LA CLINICA HUMANITARIA PABLO JARAMILLO C			
DESCRIPCION	**NIVEL VULNERABILIDAD**		
	Grave	**Alto**	**Medio**
Esta registradas las ultimas diez contraseñas utilizadas por el usuario	**X**		
Existe un procedimiento para realizar el proceso de monitoreo mediante un programa de control hacia la BD.		**X**	
La existencia de registros de pruebas de inyección SQL[5]a la BD[1]		**X**	
Correctivos con relación a los hallazgos encontrados		**X**	
Las claves tiene estipulado un período de expiración de la clave		**X**	
El número de caracteres y tipo de caracteres para la contraseña es controlado		**X**	
Los privilegios hacia los usuarios comunes son controlados por el Administrador del CPD			**X**
Se realiza el control de Log's[11] de la BD			**X**

Fig20. Matriz vulnerabilidades lógicas con detectadas en el CPD de la Clínica Humanitaria.

[11] Un log es un registro oficial de eventos durante un rango de tiempo en particular

3.6. **Análisis de las vulnerabilidades encontradas**

Las vulnerabilidades de la matriz que se encuentra detallada ha sido realizada en base al Cuadro de Nivel de impacto de las vulnerabilidades Fig1. En el que se indica los niveles de vulnerabilidades físicas y lógicas. Las vulnerabilidades encontradas han sido calificadas de acuerdo al impacto que tiene en la Clínica Humanitaria y a su vez en base a la metodología propuesta. Las vulnerabilidades de Nivel Grave necesitan ser corregidas o se consideran de gran amenaza o que tiene un alto impacto en el CPD, las vulnerabilidades de nivel alto, medio se encuentran de alguna manera controladas debido a que existen controles que se llevan a cabo sobre ellas de tal forma que su impacto esta mitigado gracias a las medidas que se han implementado.

3.6.1. Análisis de cada una de las vulnerabilidades con calificación de "Grave"

3.6.2. Se debe tener sistema de detección de incendios.- El CPD de la clínica no cuenta con un sistema automático de control de incendios lo que permitiría que en un siniestro de incendio produjera severos daños en cuanto a los equipos y datos. Cabe recalcar que el departamento cuenta con un extintor de incendios apropiado para equipos electrónicos, este extintor es de CO2 pero necesita de la intervención de una persona al no contar con un personal que se encuentre en vigilancia directa del CPD esto se considera una vulnerabilidad de alto impacto.

3.6.3. Se utiliza la tecnología de dispositivos biométricos como seguridad del CPD.- De acuerdo con el análisis de la tecnología de equipos de seguridad biométrica, un lugar se encuentra con un sistema de seguridad alto sin embargo mediante políticas bien aplicadas se pueden llevar a cabo una seguridad sobre lugares críticos.

Así podemos decir que en la Clínica Humanitaria se aplican políticas de seguridad las mismas que han permitido prescindir de esta tecnología por dos razones el costo y porque las políticas se encuentran en auge y cumpliéndose.

3.6.3.1. Resumen de Política de seguridad de la Clínica Humanitaria

El equipo de seguridad contratado para la Clínica Humanitaria estará a cargo de la seguridad de las instalaciones de la Clínica, debiendo conocer a cada miembro que se encuentra laborando en la institución deberá apoyarse en el listado de personal entregado por parte del departamento de Gestión del Factor Humano. El listado cuenta con los nombres, horas de trabajo y el cargo que ocupa cada empleado de la institución.

Si el personal de la institución desea ingresar a su lugar de trabajo en horas que no se encuentran descritas en el documento, deberá presentar la correspondiente autorización en el caso de no tenerla el personal de seguridad deberá solicitar el permiso vía telefónica al inmediato superior del personal que desea ingresar y registrar dicho ingreso.

En base a ésta política quedaría cubierta la vulnerabilidad antes detectada y considerada como de alto riesgo.

3.6.4. Existe detallado un listado de autorizaciones de acceso al CPD.- El CPD no cuenta con un listado de personas con autorización de acceso lo que permite que se realice cualquier acceso sin tomar las consideraciones de seguridad. Es decir que cualquier persona accede al CPD desde el personal de limpieza que deber realizar el aseo de dicha área de manera eventual. Si bien está descrito que en la política de seguridad de acceso a la Clínica el momento que se accede a la misma y al departamento administrativo se encuentra en contacto con el departamento de Sistemas ya que se encuentra en un mismo ambiente no así el cuarto frio que se encuentra con una cerradura y la llave de acceso la tiene los administradores del CPD.

3.6.5. Está determinada las labores de la persona a quien se autoriza el ingreso al CPD.- Las actividades que realizan las personas que acceden al CPD no se encuentran detallados como se mencionó anteriormente no se cuenta con un listado en el que se pueda verificar al personal autorizado a acceder al CPD sin embargo se detalla según la política de cargos para el personal de acuerdo al departamento.

3.6.5.1. Resumen de política para los administradores de CPD.- Los administradores del CPD se encuentran a cargo del acceso físico y lógico al centro de cómputo. Cada acceso se deberá realizar bajo los criterios propios de cada administrador y bajo la total responsabilidad al momento de autorizar dicho acceso.

De acuerdo a esta política interna los administradores del CPD tienen la total potestad para autorizar o denegar los accesos al centro de cómputo. A sabiendas que la responsabilidad del control y permisos recae sobre ellos.

3.6.6. La cámara de seguridad se usa para vigilancia preventiva.- Cada una de las cámaras que se encuentran instaladas en la Clínica su información se registra o se almacena en el ordenador sin embargo no existe un monitor[12], por lo contrario esta información es de confirmación es decir que después que se ha generado un siniestro solamente se confirma mediante los registro que se encuentran almacenados en el ordenador.

3.6.7. Existe un control de humedad del CPD.- En el CPD al contar con una sistema de climatización es necesario contar con sistema que vigile la humedad ya que debido a los cambios de temperatura pueden producir humedad y ésta puede llegar a los sistemas electrónicos causando serios daños, a pesar que el climatizador brinda una humedad aproximada del 5% eso no se encuentra registrado ni comprobada.

[12] Persona designada para revisar los sucesos mediante las cámaras de video vigilancia.

3.6.8. La instalación del Climatizador se realizó mediante un estudio adecuado.- No se evidencia registro de estudio previo a la instalación del climatizador ya que la instalación del mismo debe ser en base a estándares y normas las mismas que garantizan que el uso del mismo va a ser favorable para el CPD, el no haber realizado un estudio y no haber aplicado normas estandarizadas puede llevar problemas con el funcionamiento electrónico o que no esté realizando la función adecuada para la que fue requerida en el CPD.

3.6.9. Están registradas las ultimas diez contraseñas utilizadas por el usuario.- Una de las seguridades a nivel de usuario es el que cada una de las contraseñas puedan ser modificadas sin embargo estas no deben repetirse por lo menos con las últimas diez contraseñas, esto garantiza que si una contraseña de un usuario fue revelada anteriormente y cambio no tenga la posibilidad de volver a ingresar la misma.

CAPITULO IV

4. DESARROLLO

4.2. Políticas en base a las vulnerabilidades relevantes detectadas

Aclaración: De acuerdo a la propuesta en al ante proyecto se encuentra detallado los objetivos tres y cuatro en los que se detalla lo siguiente:

- ✓ Generar políticas de acceso lógico al sistema médico informático de acuerdo a cada uno de los roles de los usuarios.
- ✓ Establecer políticas que permitan gestionar los rangos de seguridad de acceso físico al centro de cómputo por parte del o los administradores de dicho centro.

El cumplimiento de éstos objetivos se encuentran detallados en conjunto con las definiciones de políticas que se detallan a continuación.

4.2.1. DEFINICION DE POLITICAS

A la política se la define con reglas generales de comportamiento generadas para el correcto funcionamiento de los procesos dentro de una institución, teniendo que para la rama informática las políticas permiten mantener seguridad sobre los activos informáticos de la institución.

Las políticas que una institución implementa son de tipo particular y dependen de la cultura organizacional que se mantiene, es decir que las políticas se deben hacer a medida de cada institución de acuerdo a los requerimientos específicos.

4.2.2. Propuesta de políticas a implementarse en la Clínica Humanitaria

CLINICA HUMANITARIA

FUNDACION PABLO JARAMILLO C

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
1. Se debe tener sistema de detección de incendios	Grave

Objetivo:

Con el fin de precautelar los equipos del CPD y considerando que en ellos se alberga los datos, de igual manera considerando que ésta información es de uso general, permanente e imprescindible para la institución es necesario considerar la implementación para el CPD la siguiente política la misma que permitirá gestionar la seguridad frente a las vulnerabilidades contra incendios determinadas en el análisis de vulnerabilidades físicas del CPD.

Política:

a. Los administradores del CPD que estén a cargo deberán llevar el control periódico de cada uno de las instalaciones tanto eléctricas como de ventilación y control de temperatura de acuerdo con los estándares para el correcto funcionamiento de un CPD.

b. Los daños que se determinen al realizar la inspección al CPD se debe comunicar a los superiores con el fin de tomar las acciones correctivas de manera rápida y eficiente.

c. Para acceder al CPD durante las horas en las que no se encuentra el administrador del centro de cómputo el personal de seguridad deberá contar con los permisos correspondientes otorgados por las

autoridades superiores de informática para permitir dicho acceso, de igual manera el personal de seguridad deberá registrar la hora de ingreso como la de salida y su correspondiente actividad que realizó.

d. Cada una de las revisiones se debe documentar y detallar los hallazgos que se haya determinado en el proceso de control del CPD.

e. Al presentarse situaciones de emergencia o de situaciones de urgencia, el acceso al CPD estará sujeto a las especificadas por las autoridades superiores del CPD.

Efecto de incumplimiento:

El no aplicar cada una de los puntos detallados anteriormente permitirá que se pueda suscitar un evento no deseado en el CPD el mismo que conlleva a que se provoque desde la pérdida de los datos a un siniestro de incendio.

CLINICA HUMANITARIA

FUNDACION PABLO JARAMILLO C

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
1. Se utiliza la tecnología de dispositivos biométricos como seguridad del CPD	Grave

Objetivo:

Con el fin de evitar el acceso al CPD de personas ajenas al departamento y evitar daños provocados en equipos los mismos que conlleven a perdida de información, modificación, alteración, y otros actos que atenten con el buen funcionamiento de los equipos y programas del CPD es necesario tener en cuenta las siguientes políticas:

Política:

a. El acceso al CPD debe ser registrado y autorizado por la máxima autoridad el mismo que deberá registrar de manera detallada la fecha de acceso, la actividad a realizar y las correspondientes observaciones que se hayan generado en el tiempo de permanencia del personal.

b. Cada acceso al CPD debe ser por una actividad o necesidad específica y que requiera el acceso físico de tal manera que no se pueda realizar de manera remota.

c. Cada aGcceso será archivado de manera física con la correspondiente firma de responsabilidad de quien autoriza dicho acceso, al igual que la rúbrica del personal que ha obtenido el permiso para acceder al CPD.

d. Para acceder al CPD durante las horas no laborables por parte del personal del departamento de cómputo el personal de seguridad general de la institución debe contar con la debida autorización para que pueda ingresar, éste ingreso debe ser registrado con la correspondiente hora de ingreso como la de salida, quien realizo la autorización y su correspondiente actividad que realizó.

e. Las autorizaciones deben ser de manera física (Papel escrito, o verbal) o lógica (Mediante correo electrónico)

f. Cuando no se cuente con las autorizaciones antes mencionadas y sea necesario el acceso del personal al CPD el personal de seguridad debe contactarse con los superiores de dicho personal los mismos que autoricen el acceso, el personal de seguridad deberá registrar cada uno de los sucesos

Efecto de incumplimiento:

El incumplimiento de éstas políticas permitirá que el acceso al CPD no sea controlado y que sea vulnerable a saboteos por parte de personal mal intencionado o con poca experiencia en el manejo y uso de los equipos del CPD.

CLINICA HUMANITARIA

FUNDACION PABLO JARAMILLO C

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
1. Existe detallado un listado de autorizaciones de acceso al CPD 2. Está determinada las labores de la persona a quien se autoriza el ingreso al CPD 3. Está determinada las labores de la persona a quien se autoriza el ingreso al CPD	Grave

Objetivo:

Con el fin de precautelar la manipulación errada de los equipos e instalaciones del CPD al momento de permitir el acceso, es necesario aplicar las siguientes políticas.

Política:

a. El acceso al CPD debe ser autorizado por la máxima autoridad del departamento.

b. Se debe registrar el acceso al igual que la actividad a realizar por la persona autorizada, siempre debe estar bajo la supervisión de una persona del departamento que cuente con las destrezas y conocimientos para llevar a cabo la supervisión de acuerdo con las normas y procedimientos del CPD los mismos que puede detallarse de manera explícita o implícita.

Efecto de incumplimiento:

El no cumplir con estas políticas permitirá que se cometan errores y posible mal funcionamientos de los equipos o instalaciones que fueron manipuladas sin el conocimiento adecuado.

CLINICA HUMANITARIA

FUNDACION PABLO JARAMILLO C

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
1. La cámara de seguridad se usa para vigilancia preventiva	Grave

Objetivo:

El mantener el CPD bajo una correcta y permanente vigilancia permitirá evitar siniestros no controlados o previstos.

Política:

a. Las cámaras deben ser monitoreadas periódicamente por el personal de seguridad de la institución con el fin de prevenir que sucesos siniestros puedan llegar a ser incontrolables o irreversibles.

b. El personal de seguridad tiene la obligación de monitorear las cámaras y al detectar alguna anomalía comunicar a las personas correspondientes y tomar las acciones para corregir o eliminar los problemas detectados.

Efecto de incumplimiento:

El no cumplir con esta política permitirá que no se pueda detectar problemas generados en el momento y por ende no controlar a tiempo lo que conlleva a que se pueda volver un problema incontrolable o irreparable.

CLINICA HUMANITARIA

FUNDACION PABLO JARAMILLO C

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
1. Existe un control de humedad del CPD 2. La instalación del Climatizador se realizó mediante un estudio adecuado.	Grave

Objetivo:

Con el fin de precautelar la información y que las nuevas instalaciones tanto que afecten de manera directa o indirecta en el procesamiento de los datos se debe realizar un estudio previo de impactos y evaluación de los mismos antes de implementar al CPD.

Política:

a. La administración del CPD deberá emitir las normas y procedimientos que correspondan para realizar las instalaciones de nuevos componentes basados en estudios de factibilidad y evaluación de impactos para el CPD.

b. Los equipos instalados deben contar con la aprobación para la instalación de dicho equipo de manera documentada al igual que el estudio que sustente que el equipo es el idóneo para cubrir las

necesidades del CPD

c. Los estudios deberán realizarse con la colaboración de personal tanto de la empresa como externo y sus resultados deben ser notificados y conocidos por los altos mandos de la institución.

Efecto de incumplimiento:

El no cumplir con estas políticas dará origen a realizar las implementaciones basadas en conocimientos empíricos y más no técnicos permitiendo que se generen errores tanto lógicos como físicos a corto o largo plazo.

CLINICA HUMANITARIA

FUNDACION PABLO JARAMILLO C

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
1. Esta registradas las ultimas diez contraseñas utilizadas por el usuario	Grave

Objetivo:

Con el fin de precautelar la información que se alberga en la BD por parte de los usuarios debido al uso incorrecto de sus contraseñas es necesario aplicar las siguientes políticas que permitirán mantener un mejor control sobre las claves de acceso al sistema por parte de los usuarios.

Política:

a. Los administradores deben generar las normas y los procedimientos que permitan gestionar las claves seguras por parte de los usuarios que tengan permisos para acceder al sistema informático de la institución.

b. Los administradores deben fijar un tiempo de validez de las claves de acceso para los usuarios con el fin de que se encuentren en periodo de renovación.

c. Los administradores deben implementar los correspondientes procesos

sobre la generación de claves seguras, tomando las consideraciones y estándares adecuados para conseguir dicho objetivo.

d. Los administradores deben mantener y transmitir la cultura de generar claves seguras para los nuevos usuarios del sistema informático al igual que refrescar los conocimientos de los usuarios antiguos.

e. Los administradores deben implementar los proceso que permitan controlar las últimas claves registradas, de tal manera que sean inutilizables en las nueva clave que se desee ingresar, el número de claves a recordar debe ser tomada con el mejor criterio por parte del administrador a cargo de realizar este procedimiento, los usuarios no podrán ingresar al sistema una vez que haya expirado su clave y no se haya realizado la modificación.

Efecto de incumplimiento:

El incumplir con esta política permitirá mantener una vulnerabilidad lógica la misma que puede ser explotada por personas con conocimiento y a su vez sufrir ataques que pueden tener consecuencias no deseadas.

CLINICA HUMANITARIA

FUNDACION PABLO JARAMILLO C

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
Política para gestionar los privilegios de acceso a la BD a los usuarios del sistema informático.	

Objetivo:

Con el fin de mantener la integridad, confidencialidad y disponibilidad de la información que está almacenada en el CPD es necesario aplicar las siguientes políticas

Política:

a. El administrador a cargo del CPD debe generar las normas y procedimientos mediante los cuales permitan otorgar a los usuarios los roles sobre la BD de tal manera que se asignen de manera acorde a las normas que se encuentren redactadas.

b. El administrador encargado de otorgar los roles a los usuarios sobre la BD deben conocer el perfil de los usuarios a los cuales va a asignar los permisos de acceso

c. Cada usuario debe poseer los permisos que necesite en el momento que se encuentre desarrollando las actividades a él encomendadas, es decir que cuando el usuario deje de hacer actividades ajenas al trabajo

cotidiano es responsabilidad del administrador el quitar los permisos que no sean necesarios.

d. Los usuarios serán modificados los roles otorgados solamente cuando sea presentada la correspondiente solicitud para dicho proceso y sea aceptada por el administrador del CPD, la solicitud deberá ser registrada y almacenada.

e. Las solicitudes de cambios en los roles de los usuarios deberán ser claros y específicos teniendo en cuenta los siguientes requerimientos:

- ✓ Nombres
- ✓ Cargo
- ✓ Fecha de inicio en las nuevas actividades
- ✓ Fecha de culminación de las actividades
- ✓ Firma de responsabilidad de quien solicita
- ✓ Firma de responsabilidad de quien aprueba

f. Esta información será administrada y agregada de acuerdo a los requerimientos del administrador del CPD.

Efecto de incumplimiento:

El incumplir con esta política permitirá que los usuarios que hayan sido otorgados permisos de acceso a la BD puedan seguir accediendo a información que no necesiten para sus labores cotidianas

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.2. Conclusiones

En base del análisis de las vulnerabilidades determinadas y las políticas generadas para el CPD de la Clínica Humanitaria Pablo Jaramillo C. podemos decir:

La Institución al ser una clínica materno infantil ha prestado atención de manera muy dedicada a la infraestructura y atención al paciente tanto a nivel de salud como de gestión, no así, con la infraestructura y las seguridades para el CPD por lo que son llamados a gestionar los administradores, para que se implementen las seguridades adecuadas en dicho centro.

El CPD a pesar de encontrarse en un cuarto con seguridad, el monitoreo se realiza desde los equipos de los administradores, estos debería contar con las seguridades lógicas para los equipos ya que comparten el lugar con el departamento de Contabilidad y su acceso es libre.

Debido a la falta de interés en la seguridad del CPD por parte de los altos mandos no se ha llegado a implementar las correspondientes seguridades en el mismo y por ende no se han realizado los respectivos estudios para la implementación y adecuación del centro.

Pese a contar con la tecnología implementada para video vigilancia,dicha tecnología no es aprovechada para uso preventivo, al contrario es usada para corroborar un suceso que se haya dado, es decir que no se está cumpliendo con el objetivo de dicha tecnología que es de prevención.

Los usuarios no cuentan con los conocimientos y la cultura adecuados para gestionar claves de alta seguridad, razón por la cual las claves de acceso son consideradas de una seguridad baja.

Los accesos a la BD del sistema informático no cuentan con un procedimiento que permita al encargado guiarse o revisar mediante un documento elaborado, de igual manera no se cuenta con un soporte para revisar si los roles ya asignados a los usuarios son los correctos de acuerdo a sus labores que realizan.

5.3. Recomendaciones

Se recomienda que el CPD no se encuentre ubicado junto al departamento de Contabilidad ya que no permite llevar un adecuado control de acceso al CPD.

Es necesario implementar un procedimiento para la implementación de nuevos componentes para el CPD en el que conste la solicitud de un análisis o estudio sobre el impacto y su idoneidad.

Es necesario designar al personal adecuado para el monitoreo de cámaras que se encuentran dispuestas en la institución de tal manera que se convierta en una tecnología de seguridad preventiva.

Se debe tener precaución con las personas que son autorizas para el acceso al CPD, para realizar tareas no técnicas (Limpieza, Mantenimiento, etc.) las mismas que al no poseer los conocimientos adecuados pueden ocasionar serios daños en los equipos.

Se debería tener o acondicionar un ambiente o área de visitas para el área de Contabilidad y el área de Sistemas o separar estas dos áreas.

Se debe generar un manual de proceso y procedimientos para las actividades del CPD el mismo que permita a cada uno de las personas que laboran conocer y consultar las actividades que realizan soportado en un manual.

El proceso y procedimientos que se encuentran generados deben ser revisados y actualizados con el fin de que se encuentren acorde a la realidad.

Las políticas deben ser sujetas a revisiones periódicas y a modificaciones para que se pueda cumplir con el objetivo que se el de mantener la seguridad y los buenos manejos del CPD.

BIBLIOGRAFÍA

(Autor Luis Mendizabal) Copiado el 25/8/2011

http://www.slideshare.net/lmendi/redes-y-seguridad-infomatica

(Autor: Mario Farías-Elinos) Copiado el 25/8/2011

Url:http://seguridad.cudi.edu.mx/congresos/2001/pronad/seg_pronad.pdf

(Universidad del valle de México) Copiado el 25/8/2011

http://www.uvmnet.edu/normatividad/reglamentos/ca-r01-1.doc

Manual de Oracle.

(Autor: alegsa.com.ar) Copiado el 25/8/2011

http://www.alegsa.com.ar/Dic/software.php

(Autor: Wikipedia.org) Copiado el 25/8/2011

http://es.wikipedia.org/wiki/M%C3%A9todo_cualitativo

(Emagister.com) Copiado el 25/8/2011

http://www.wikilearning.com/apuntes/la_encuesta-concepto_de_encuesta/14756-1

Herald Ware Mendoza Copiado el 5/9/2011

http://elprofejorge.blogdiario.com/img/acc.pdf

Anexos

Resultados del análisis de vulnerabilidades realizado en el CPD de la Clínica Humanitaria Pablo Jaramillo C.

CLINICA HUMANITARIA

FUNDACION PABLO JARAMILLO C.

DIRECCION MEDICA

ANALISIS DE VULNERABILIDADES FISICAS Y DE ACCESO LOGICO AL CENTRO DE COMPUTO DE LA CLINICA HUMANITARIA FUNDACION PABLO JARAMILLO C.

Desarrollado por:

Miguel Juela León
TECNÓLOGO ANALISTA DE SISTEMAS
Cuenca, Noviembre de 2011

INTRODUCCIÓN

Cada día los centros de cómputo de las empresas son objetos de ataques ya sea desde dentro o desde fuera de ellas la razón especial es porque en estos lugares se alberga los datos de las empresas, considerando que la información de una empresa es una activo intangible, es por eso que se vuelve cada vez más importante mantener un riguroso control sobre los accesos a los datos al igual que el monitoreo permanente del comportamiento de dicho centro.

Los encargados de brindar la seguridad debida son los administradores del centro de cómputo o a su vez en centros más grandes existen ya las áreas encargadas de seguridad, las mismas que no necesariamente pertenecen al centro de cómputo sino más bien son áreas separadas y con gran injerencia sobre los departamentos, la función de este es el de mantener la seguridad y a su vez de fomentar los buenos principios de seguridad sobre la información por parte de los usuarios.

OBJETIVOS

Objetivo General.-Análisis de vulnerabilidades físicas y de acceso lógico al centro de cómputo de la Clínica Humanitaria Fundación Pablo Jaramillo C, cuando se accede a la BD del Sistema Informático

Objetivos específicos

- ✓ Investigar al acceso físico y lógico al centro de cómputo cuando se accede a la BD del Sistema Informático.
- ✓ Generar políticas de acceso lógico al sistema médico informático de acuerdo a cada uno de los roles de los usuarios.
- ✓ Establecer políticas que permitan gestionar los rangos de seguridad de acceso físico al centro de cómputo por parte del o los administradores de dicho centro

METODOLOGÍA

Estudio inicial Es el establecer los colaboradores, determinar el lugar informático en el que se va a llevar a cabo el estudio, con el fin de conocer el área es necesario diseñar una Lista de verificación para obtener información de importancia del centro lo que nos permitirá realizar una evaluación inicial, verificar los manuales de políticas y reglamentos.

Procedimientos y técnicas de auditoria.- Existen objetivos de control y procedimientos de auditoria que después de evaluar los riesgos es necesario identificar las fortalezas y debilidades en los controles existentes basados en la información recopilada para posteriormente generar el correspondiente informe el mismo que debe ser redactado de manera objetiva para la gerencia, la misma que debe tener la disponibilidad para implementar los correctivos necesarios al igual que mantener las revisiones periódicas de los seguimientos emprendidos.

Evaluación de Riesgo.- La evaluación de riesgos determina las vulnerabilidades amenazas y riesgos para generar un plan de controles que contemplen los criterios de un centro de cómputo seguro mediante los parámetros de disponibilidad, confidencialidad e integridad de la información, teniendo en cuenta los siguientes puntos:

- ✓ La probabilidad de amenaza
- ✓ El impacto sobre el centro en base a los parámetros de disponibilidad, confidencialidad e integridad de la información.

Determinación de la probabilidad.- Es necesario tomar en cuenta los siguientes parámetros para determinar la probabilidad que ocurra un evento

- ✓ Origen de la Amenaza
- ✓ Causa de la vulnerabilidad.

Se deben clasificar las probabilidades de que una vulnerabilidad potencial sea explotada por una fuente de amenaza en Grave, Alto, Medio y Nulo.

NIVEL	DEFINICIÓN	Mínimo de probabilidad que suceda
Grave	La amenaza está altamente motivada y es suficientemente capaz de llevarse a cabo.	2 veces al año.
Alto	La amenaza está fundamentada y es posible.	1 vez al año.
Medio	La amenaza es posible.	0,5 veces al año.
Nulo	La amenaza no posee la suficiente motivación y capacidad.	0,25 veces al año.

Numero de ocurrencias del evento en un periodo.- Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de información, modificación de datos, utilizamos información obtenida de ciertas publicaciones tecnológicas con relación similar a los eventos que se desea estudiar. De esta manera se define una escala en la cual, una amenaza grave está considerada una probabilidad que suceda al menos dos veces al año, amenaza de categoría Alto que suceda al menos una vez al año, una amenaza de categoría Medio una probabilidad de 0,5 veces al año y por último para una amenaza de categoría Nulo una probabilidad de 0,25 veces al año.

Identificación de Vulnerabilidades.- Para la identificación de vulnerabilidades sobre la plataforma de tecnología, se utilizan herramientas como listas de verificación y herramientas de software que determinen las vulnerabilidades.

Análisis del impacto y el factor de riesgo.- El próximo paso en la metodología que estamos describiendo, es poder determinar el impacto adverso para la organización, como resultado de la explotación por parte de una amenaza de una determinada vulnerabilidad, para ello se deben considerar los siguientes aspectos

- ✓ Consecuencias de tipo financiero, es decir pérdidas causadas sobre un activo físico o lógico determinado y las consecuencias que este activo no funcione, y afecte la operación de la compañía.
- ✓ La importancia crítica de los datos y el sistema (importancia a la organización).
- ✓ Sensibilidad de los datos y el sistema.

Identificación de Controles.- En esta fase se evaluarán las conclusiones de la valoración y la matriz de riesgo con el fin de identificar los controles que mitiguen los riesgos encontrados.

Definición de Políticas.- Las Políticas de seguridad dependen de la cultura de la organización. Por esta razón las políticas y procedimientos deben estar hechos a la medida, según los requerimientos específicos de cada organización. Para la definición de las políticas y procedimientos se realiza un proceso de validación en conjunto con la organización con el fin de generar políticas y procedimientos que se ajusten a esta. Como punto de partida para la definición de las políticas se tendrá como referencia el análisis de riesgo realizado.

Alcance de las Políticas

Seguridad en la Organización

- ✓ Roles y Responsabilidades de Seguridad de la Información
- ✓ Políticas para el manejo de la información.

Clasificación de la Información

- ✓ Importancia de la información según la organización

Administración de las operaciones de cómputo y comunicaciones

- ✓ Políticas sobre el uso del correo electrónico
- ✓ Políticas sobre el uso de clave de acceso.
- ✓ Políticas sobre el uso de recursos.

Definición de estándares.- Es la definición cuantitativa o cualitativa de un valor o parámetro determinado que puede estar incluido en una política o procedimiento, Algunos de los principales estándares a definir son:

- ✓ Longitudes de contraseñas.
- ✓ Histórico de contraseñas,
- ✓ Eventos a registrar.

HALLAZGOS EN EL ANALISIS

CONTROL DE ACCESO FISICO AL CPD

Para mantener la seguridad de un CPD es necesario comprender que éste lugar es en donde se encuentran los datos más valiosos de una institución se debe considerar que la seguridad física es de vital importancia para este lugar ya que, el no restringir los accesos al CPD se está exponiendo los datos y la información más vulnerable a que sea susceptible de sustracción, alteración, modificación, etc. Es necesario mantener un control de entrada y salida del personal, al igual que de los equipos y sus componentes, en la Clínica se cuenta con varios métodos de seguridad aplicadas como:

Ubicación del CPD.- Es recomendable que la ubicación sea entre la primera o segunda planta del edificio, para evitar los riesgos de las plantas altas y bajas (inundaciones, goteras etc.), que su ubicación no esté señalizada, que no tenga ventanas etc.

La ubicación del CPD[1]en la Clínica Humanitaria se encuentra en la segunda planta, el lugar no cuenta con señalización que indique en donde se encuentra dicho centro, El cuarto cuenta con un sistema de enfriamiento y no cuenta con ventanas es decir que no incurre con las normas específicas para la implantación de un CPD.

ANÁLISIS DE VULNERABILIDAD POR UBICACIÓN DE CPD				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	**Alto**	**Medio**	**Nulo**
Riesgo de Inundación por goteras				X
Riesgo de sabotaje por estar visible				X
La ubicación del CPD está Señalizada				X

SUELO FALSO O TECHO FALSO

De acuerdo a las recomendaciones para un CPD dice que debe existir un suelo o techo falso por donde se distribuye el cableado, el mismo que debe ser de material no inflamable debe mantener las distancias respecto del suelo real. De igual manera se debe mantener un aseo en dicho lugares, se debe tener detectores de humedad, un sistema de detección de incendios etc.

El CPD cuenta con un techo falso, pero a su vez éste no cumple con las especificaciones técnicas en la que se solicita que sea de material no inflamable, no se cuenta con detector de humedad para este lugar a pesar que sobre este cuarto se encuentra una estructura de hormigón armado lo que no permitirá que se filtre humedad por causa de goteras y de igual manera se cuenta con un sistema de circulación de aire para evitar que las corrientes de aire generen humedad, El centro cuenta con un extintor de incendio el mismo que es de CO2 el recomendado para equipos electrónicos, el mantener un extintor de incendios no significa que este asegurado al existir un siniestro de incendio ya que para su acción necesita contar con un sistema automático de detección de incendios.

Análisis de vulnerabilidad por Suelo falso o Techo falso				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Debe disponer de un suelo o techo falso			**X**	
El suelo falso o techo falso sirve para distribuir el cableado			**X**	
El suelo falso o techo falso es de material no inflamable		**X**		
Se debe mantener un aseo en el suelo falso o techo falso lugares			**X**	
Se debe tener detectores de humedad en el suelo falso o techo falso			**X**	
Se debe tener sistema de detección de incendios	**X**			

Análisis de la vulnerabilidad con nivel Grave.- El CPD de la clínica no cuenta con un sistema automático de control de incendios lo que permitiría que en un siniestro de incendio produjera severos daños en cuanto a los equipos y datos. Cabe recalcar que el departamento cuenta con un extintor de incendios apropiado para equipos electrónicos, este extintor es de CO2 pero necesita de la intervención de una persona al no contar con un personal que se encuentre en vigilancia directa del CPD esto se considera una vulnerabilidad de alto impacto.

DISPOSITIVO BIOMETRICO

La Biometría, esta tecnología está basada en el reconocimiento de características físicas e intransferibles de los seres humanos, tales características como la huella digital, estos sistemas biométricos utilizan dos dispositivos, un software de captura y un dispositivo biométrico (lector), es necesario aclarar que la huella digital no es una imagen sino un sistema complejo en el que se comparan diversos patrones, esta tecnología se utiliza para brindar un acceso seguro a equipos de computación o redes informáticas, protección de información al igual que para llevar el control de horarios y acceso físico de cierto personal en áreas restringidas**.**

La ventaja principal de esta tecnología es la seguridad debido a que los sistemas de contraseñas o tarjetas pueden ser hurtadas, de ésta manera se garantiza el acceso a una PC o una sala restringida teniendo en cuenta que para hacerlo no depende de algo que se necesite conocer o algo adicional que tengamos, sino que, todo lo contrario depende de lo que somos y en lo que se basó para tomar como nuestra identificación.

Esta tecnología funciona de la siguiente manera, cuando la huella digital es el medio de identificación que se ha dispuesto, el dispositivo biométrico captura la huella y el software capta los puntos característicos de la huella lo procesa y lo transforma en un resultado matemático por medio de algoritmos que no pueden ser llevados en inversa, por esta razón los sistemas biométricos son considerados como de alta seguridad, el resultado al proceso matemático aplicado a la huella que se autenticó es comparado con la información antes

almacenada en una base de datos segura la misma que servirá para permitir o denegar el acceso, al igual que o a su vez para registrará el momento del acceso.

La clínica humanitaria cuenta con un sistema de acceso biométrico, el mismo que se encarga de registrar el acceso del personal a la institución con la finalidad de mantener un control en el departamento de Gestión del Factor Humano sin embargo este sistema no se encuentra empleado para el acceso al Centro de cómputo.

ANÁLISIS DE VULNERABILIDAD POR DISPOSITIVO BIOMÉTRICO				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Se utiliza la tecnología de dispositivos biométricos como seguridad del CPD	X			

Análisis de la vulnerabilidad con nivel Grave.- De acuerdo con el análisis de la tecnología de equipos de seguridad biométrica, un lugar se encuentra con un sistema de seguridad alto, sin embargo mediante políticas bien aplicadas se pueden mantener una seguridad sobre lugares críticos.

Así podemos decir que en la Clínica Humanitaria se aplican políticas de seguridad las mismas que han permitido prescindir de esta tecnología por dos razones el costo y porque las políticas se encuentran en auge y aplicándose.

RESUMEN DE POLITICA DE SEGURIDAD DE LA CLINICA HUMANITARIA

"El equipo de seguridad contratado para la Clínica Humanitaria estará a cargo de la seguridad de las instalaciones de la Clínica, debiendo conocer a cada miembro que se encuentra laborando en la institución deberá apoyarse en el listado de personal entregado por parte del departamento de Gestión del Factor Humano. El listado cuenta con los nombres, horas de trabajo y el cargo que ocupa cada empleado de la institución.

Si el personal de la institución desea ingresar a su lugar de trabajo en horas que no se encuentran descritas en el documento, deberá presentar la correspondiente autorización en el caso de no tenerla el personal de seguridad deberá solicitar el permiso vía telefónica al inmediato superior del personal que desea ingresar y registrar dicho ingreso."

En base a ésta política quedaría cubierta la vulnerabilidad antes detectada y considerada como de alto riesgo.

PROCEDIMIENTO DE AUTORIZACION DE ACCESO AL CPD

La autorización al centro de cómputo se debe establecer a través de un procedimiento por medio del cual se especifique los requerimientos para dicho acceso.

Es necesario generar un listado de autorización el mismo que debe contener la información esencial, de tal manera que el administrador del centro o quien se encuentre a cargo de la seguridad del CPD[1]pueda conocer y ubicar a dicha persona para realizar las labores que se encuentren descritas en el documento de autorización, con la finalidad de que el personal no acceda a información que no es necesaria y a su vez que ésta información no sea susceptible de hurto o de alteraciones éste documento debe contener la firma de quien autoriza o solicita dicho acceso éste documento debe contener la siguiente información:

Nombre, cargo, número de cédula o pasaporte de cada una de las personas que conforman el Listado.

Existe explícitamente un documento en la institución la misma que determina las obligaciones de los encargados del centro de cómputo en la que dice: que el administrador y su asistente son los responsables y quienes autorizan el acceso al centro de cómputo por ser ellos quienes tienen el criterio de seguridad. Es decir que el criterio para permitir el acceso ya sea de manera lógica como de manera física se encuentra en manos de los encargados del CPD[1], sin embargo vía e-mail se encuentra registrado las solicitudes de acceso al nuevo personal que se incorpora a la institución y que requiere el acceso al sistema informático, de igual manera con el fin de actualizar los usuarios del sistema se envía vía e-mail los egresos del personal, es decir cuando un empleado ha dejado de laborar en la institución.

ANÁLISIS DE VULNERABILIDAD POR AUTORIZACIÓN DE ACCESO				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Existe un procedimiento de autorización de acceso al CPD.			X	
El procedimiento de autorización de acceso se encuentra accesible para los administradores.		X		
Existe detallado un listado de autorizaciones de acceso al CPD	X			
Está determinada las labores de la persona a	X			

quien se autoriza el ingreso al CPD				
Los documentos se encuentran registrados con las debidas firmas de autorización de acceso al CPD		X		

Análisis de las vulnerabilidades encontradas con nivel Grave

Existe detallado un listado de autorizaciones de acceso al CPD.- El CPD no cuenta con un listado de personas con autorización de acceso lo que permite que se realice cualquier acceso sin tomar las consideraciones de seguridad. Es decir que cualquier persona accede al CPD desde el personal de limpieza que deber realizar el aseo de dicha área de manera eventual. Si bien está descrito que en la política de seguridad de acceso a la Clínica el momento que se accede a la misma y al departamento administrativo se encuentra en contacto con el departamento de Sistemas ya que se encuentra en un mismo ambiente no así el cuarto frio que se encuentra con una cerradura y la llave de acceso la tiene los administradores del CPD.

Está determinada las labores de la persona a quien se autoriza el ingreso al CPD.- Las actividades que realizan las personas que acceden al CPD no se encuentran detallados como se mencionó anteriormente no se cuenta con un listado en el que se pueda verificar al personal autorizado a acceder al CPD sin embargo se detalla según la política de cargos para el personal de acuerdo al departamento.

Resumen de política para los administradores de CPD.- Los administradores del CPD se encuentran a cargo del acceso físico y lógico al centro de cómputo. Cada acceso se deberá realizar bajo los criterios propios de cada administrador y bajo la total responsabilidad al momento de autorizar dicho acceso.

De acuerdo a esta política interna los administradores del CPD tienen la total potestad para autorizar o denegar los accesos al centro de cómputo. A sabiendas que la responsabilidad del control y permisos recae sobre ellos.

SISTEMAS DE SEGURIDAD Y VIGILANCIA MEDIANTE CÁMARAS

Dentro de la tecnología de seguridad se ha implementado de manera eficaz y con grandes avances las cámaras de seguridad teniendo como ventaja el ejercer una vigilancia preventiva mediante el registro visual de cada suceso que registran las diferentes cámaras que se llegan a disponer en un determinado lugar. El uso de los equipos de videograbación va dirigido a asegurar el amplio espectro de lugares en los que la seguridad necesita de un gran apoyo como son dichas cámaras. Los lugares en los que se emplean van desde Empresas de diversos tipos, Centros Comerciales, Aeropuertos, Entidades Bancarias, Vías públicas, etc.

Al tener una o a su vez un grupo de cámaras conectadas hasta un servidor en donde se registran cada una de las imágenes que son capturadas por dichas cámaras se lo denomina CCTV (Closed Circuit Television), no todos los circuitos cerrados cuentan con un ordenador de almacenamiento de los datos registrados, ya que también existen CCTV que no necesitan almacenar la información almacenada. Este circuito cerrado puede contar con uno o varios monitores desde los cuales se vigila, se denomina circuito cerrado debido que, todos los componentes se encuentran interconectados. Además, a diferencia de la televisión convencional, este sistema está diseñado para una cantidad limitada de usuarios.

En la actualidad las cámaras permiten ser controladas remotamente desde un lugar de monitorización en el que se controla su panorámica (Es el amplio horizonte visual que presenta una imagen), inclinación y zoom.

Las cámaras de la actualidad incluyen visión nocturna, proceso asistidos por un ordenador y detección de movimiento que facilita al sistema estar en modo de alerta cuando se realiza un movimiento frente a la cámara.

Una cámara que tiene como función el de activarse al detectar movimientos se utiliza en los sistemas que lo controlan ya que estos equipos se encuentran registrando el movimiento mientras se encuentren encendidos, su función es el de comparar con una imagen congelada, al momento que esta imagen ha cambiado el ordenador al que se encuentra conectado empieza a registrar los eventos que dicha cámara envía hasta dicho equipo, ésta

función permite que en el ordenador se optimice el espacio de almacenamiento para grabar solamente cuando exista movimiento.

La Clínica Humanitaria cuenta con un CCTV el mismo que se encuentra distribuido por la clínica con 16 cámaras las mismas que su información se almacena en el servidor de cámaras, cada cámara cuenta con la función de registrar ya sea cuando hay iluminación o al no existir es decir equipos con visión nocturna y a colores, el sistema de almacenamiento es administrado mediante un software llamado "GEOVISION" éste software se encarga de almacenar solamente cuando detecta movimiento ya que las cámaras en todo momento se encuentran enviando información el inconveniente detectado es que tiene un margen de respuesta después de registrar el movimiento.

La información que se encuentra almacenada en el ordenador es usada solamente para confirmación o verificación, teniendo acceso los administradores y la dirección médica, ésta información tiene un tiempo de almacenamiento de hace un mes atrás, para acceder a esta información se lo hace remotamente mediante la aplicación GEOVISION para cliente el mismo que otorga permisos para configuración o para eliminación de datos mediante autenticación.

El uso de esta herramienta como seguridad es correcta pero el uso no es el adecuado ya que se ha concebido a ésta tecnología para confirmación y no para detección ya que no se está monitoreando constantemente y no existe el lugar, el personal y el equipo para realizar la correspondiente monitorización.

ANÁLISIS DE VULNERABILIDAD FÍSICA POR VIGILANCIA MEDIANTE CÁMARAS				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
La cámara de seguridad se usa para vigilancia preventiva	**X**			
Las imágenes proyectadas por las cámaras de seguridad se encuentran almacenadas				**X**
Cuenta con monitorización las cámaras de seguridad		**X**		
El Espectro que cubre las cámaras de seguridad son la correcta			**X**	
Puede ser controladas las cámaras de seguridad remotamente			**X**	
Las cámaras de seguridad incluyen visión nocturna				**X**
La cámara de seguridad registra la información al detectar movimiento				**X**
El tiempo de espera entre el momento que se genera el movimiento y el registro en el ordenador			**X**	

Análisis a las vulnerabilidades encontradas de nivel Grave

La cámara de seguridad se usa para vigilancia preventiva.- Cada una de las cámaras que se encuentran instaladas en la Clínica su información se registra o se almacena en el ordenador sin embargo no existe un monitor, por lo contrario esta información es de confirmación es decir que después que se ha generado un siniestro solamente se confirma mediante los registro que se encuentran almacenados en el ordenador.

CLIMATIZACIÓN DEL CENTRO DE CÓMPUTO

La climatización es un proceso de tratamiento que se da al aire de un determinado lugar con el propósito de mantener condiciones ambientales adecuadas, controlando temperatura, humedad, calidad y distribución del aire en un determinado ambiente, el objetivo de realizar este proceso es el de satisfacer las necesidades para un determinado proceso o producto electrónico.

Un CPD debe mantener condiciones ambientales adecuadas para los equipos ya que de esta manera se garantiza la integridad de la información y la confiabilidad de las operaciones de los equipos por periodos más largos, En la Clínica Humanitaria se encuentra instalado un sistema de climatización independiente, el mismo que permite mantener una temperatura de 21º C. y con una humedad promedio de 5%. El área que se climatiza es de 10m2, es el lugar en el que se encuentran los diferentes servidores de la institución.

Análisis de vulnerabilidad Física Climatización del centro de cómputo				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
La temperatura del CPD se mantiene en un rango de 21°C y 23°C				**X**
Existe un control de humedad del CPD	**X**			
La instalación del Climatizador se realizó mediante un estudio adecuado.	**X**			

Análisis a las vulnerabilidades encontradas de nivel Grave

Existe un control de humedad del CPD.- En el CPD al contar con una sistema de climatización es necesario contar con sistema que vigile la humedad ya que debido a los cambios de temperatura pueden producir humedad y ésta puede llegar a los sistemas electrónicos causando serios daños, a pesar que el climatizador brinda una humedad aproximada del 5% eso no se encuentra registrado ni comprobada.

La instalación del Climatizador se realizó mediante un estudio adecuado.- No se evidencia registro de estudio previo a la instalación del climatizador ya que la instalación del mismo debe ser en base a estándares y normas las mismas que garantizan que el uso del mismo va a ser favorable para el CPD, el no haber realizado un estudio y no haber aplicado normas estandarizadas puede llevar problemas con el funcionamiento electrónico o que no esté realizando la función adecuada para la que fue requerida en el CPD.

PRIVILEGIOS PARA LOS USUARIOS EN BD

Privilegios de sistema.- Los Privilegios de sistema permiten a los usuarios desempeñar una acción particular dentro del sistema o sobre un tipo determinado de objeto. Por ejemplo, el

privilegio para crear un Tablespace o para borrar filas de una tabla en la base de datos, son privilegios de sistema.

Muchos privilegios de sistema están disponibles solamente para administradores y desarrolladores de aplicaciones porque estos privilegios son muy poderosos.

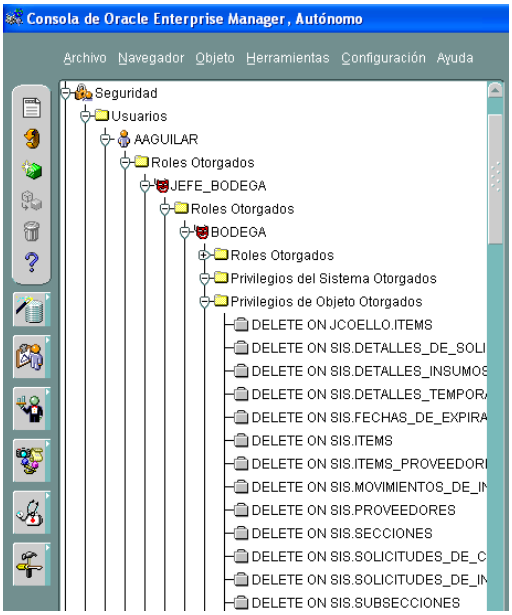
Privilegios de objetos.- Los privilegios de objetos permiten a los usuarios desempeñar acciones sobre un esquema específico. Por ejemplo, el privilegio para borrar filas de una tabla específica es un privilegio de objetos.

Los privilegios de objetos son asignados a usuarios finales, entonces ellos pueden usar una aplicación de la base de datos para llevar a cabo tareas específicas.

Asignar privilegios.- Un usuario puede recibir un privilegio de dos formas distintas:

- ✓ Los privilegios pueden ser asignados a los usuarios explícitamente.
- ✓ Los privilegios pueden ser asignados a roles (grupo de privilegios), y después el rol puede ser signado a uno o más usuarios.

Debido a que los roles permiten una mejor y más fácil administración de los privilegios, éstos normalmente son asignados a roles y no a usuarios específicos.



ANÁLISIS DE VULNERABILIDAD DE ACCESO LÓGICO A LA BD MEDIANTE PRIVILEGIOS				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Los privilegios hacia los usuarios comunes son controlados por el Administrador del CPD			**X**	
Los privilegios se encuentran otorgados en base a roles				**X**
Existen roles generados en base a los perfiles.				**X**

PROGRAMAS DE CONTROL DE ACCESO

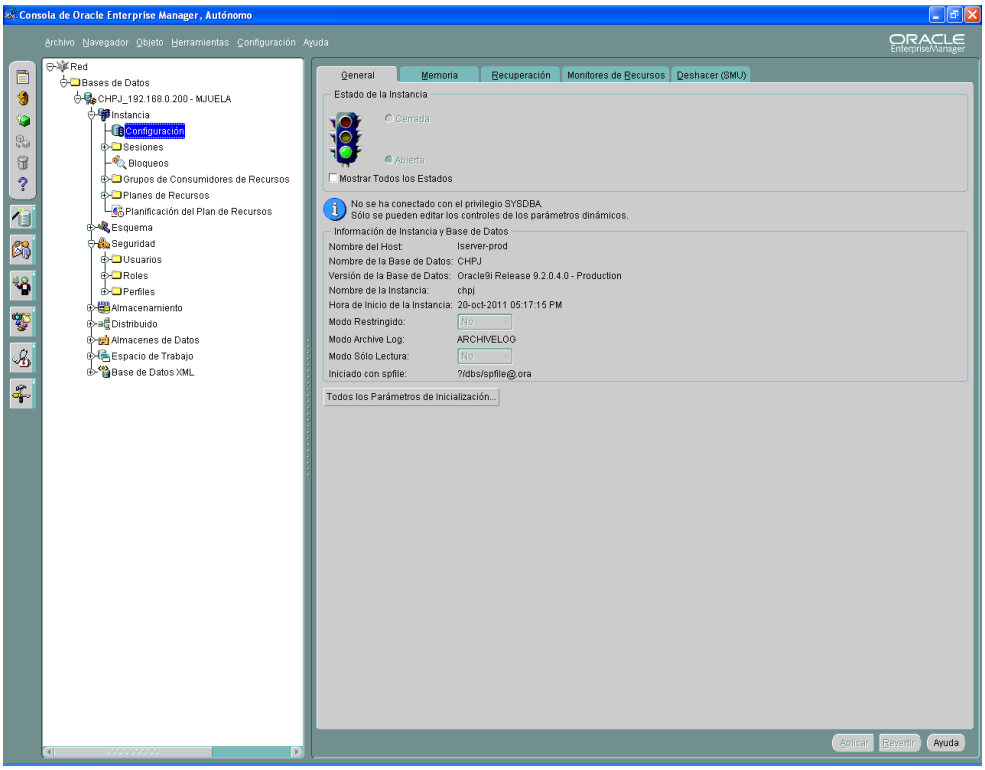
Los programas administradores de BD son los que gestionan desde las credenciales de los usuarios hasta el grado de privilegios que tiene un usuario hacia los recursos que estén expuesto en la red para el correspondiente consumo de quien solicite, de igual manera el administrador debe llevar un control de mantenimiento sobre los eventos o suceso que se generen en la Base de Datos llamados Log's (Registro oficial de eventos durante un rango de tiempo en particular.). Este administrador permite mantener un control de seguridad sobre credenciales y privilegios de una manera gráfica para su administración adecuada.

Definición de usuarios.- Pararealizar la definición de usuarios comunes se debe identificar cuáles son las tareas que van a realizar estos usuarios ya que no podrán tener los mismos privilegios que tiene un administrador de sistema un programador o el gerente de la empresa por ésta razón el administrador de la BD permite generar tipos o los conocidos roles que son los que agrupan a cada uno de los privilegios para diferentes grupos es decir que para cada uno de los cargos antes mencionados tendremos un grupo de privilegios que

se encuentran enmarcados bajo un solo nombre lo que permite una mejor administración y asignación para los usuarios.

Para generar los roles es necesario que se encuentren claramente identificado cuales son las tareas específicas de los usuarios de acuerdo a su perfil laboral lo que permitirá realizar un rol apegado al trabajo específico del usuario.

El software de la Clínica Humanitaria al ser un software comercial es decir que fue adquirido, y no desarrollado específicamente por dicha institución, los usuarios y roles han sido generados de acuerdo a las actividades que deben realizarse en el sistema informático, es decir que al adquirir el sistema medico informático los usuarios empezaron a tomar ciertas actividades nuevas y algunas a dejar de realizarlas ya que estaban asignadas a otras áreas o departamentos según el software, es por eso que los roles fueron generados sin basarse en los perfiles de los usuarios de la clínica y a su vez ha sido lo contrario, en base al sistema se han ido generando los perfiles de los diferentes cargos en los que influyen el sistema informático de manera directa.



ANÁLISIS DE VULNERABILIDAD DE ACCESO LÓGICO A LA BD MEDIANTE PROGRAMAS DE CONTROL DE ACCESO				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Se realiza control de credenciales				**X**
Se realiza el control de Log's de la BD			**X**	
Existe un procedimiento para realizar el proceso de monitoreo mediante un programa de control hacia la BD.		**X**		
El programa permite gestionar nuevos usuarios al igual que eliminar usuarios de la BD				**X**
Para generar un nuevo usuario, se encuentre detallado el perfil que va a cumplir.				**X**
Se encuentra documentado las solicitudes de los nuevos usuarios con los respectivos perfiles				**X**
Se encuentra documentados los usuarios que has sido eliminados de la BD				**X**

INYECCION SQL

Se conoce como inyección SQL el método de introducir código SQL[5] mediante una aplicación que tiene acceso a la base de datos la misma que no cuenta con las medidas adecuadas de seguridad frente a una consulta a realizar contra una Base de Datos.

Cuando la plataforma de base de datos falla para desinfectar las entradas, los atacantes son capaces de ejecutar las inyecciones SQL[5] de tal manera que permite elevar los privilegios del atacante y obtener acceso a una amplia gama de funcionalidades.

Muchos de los proveedores han dado a conocer soluciones para evitar estos problemas, pero no servirá de mucho si los parches no se aplican o no se toman los correctivos correspondientes.

Este proceso de ataque se realizó en las aplicaciones de la institución dando como resultado que esta vulnerabilidad se encuentra corregida debido a las proceso de seguridad que se establecieron al momento de generar el programa por parte de los comercializadores del software medico informático.

ANÁLISIS DE VULNERABILIDAD DE ACCESO LÓGICO A LA BD POR CONTROL DE ACCESO POR INYECCIÓN SQL				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Pruebas de inyección SQL[5]				**X**
La existencia de registros de pruebas de inyección SQL[5]a la BD[1]		**X**		
Correctivos con relación a los hallazgos encontrados		**X**		

IDENTIFICACION Y AUTENTICACION DE USUARIOS

El identificar se denomina al proceso de diferenciar a una persona de otra, el autenticar es validar a través de algún método que la persona que dice ser sea la correcta.

El llegar a determinar una manera adecuada para el control de identificación y autenticación no es muy fácil o a su vez tienen un costo muy alto. Los modelos más generalmente usados se basan en técnicas tales como:

Lo que el usuario sabe.- Generalmente las claves de acceso que pueden utilizarse acceso a una Base de Datos. Es el método comúnmente usado. La manera de brindar características de seguridad es el de mantener un período de expiración de la clave la misma que no puede repetirse con las ultimas diez utilizadas o el número que el administrados decida de acuerdo al grado de seguridad que se dese brindar a nuestra base de datos.

El tipo de contraseña también es otro control que se adiciona a la seguridad implementada al usuario, se asigna un número de caracteres mínimos para la contraseña al igual que se obliga que sea de tipo alfanumérico lo que permite que se realice por lo menos una combinación para la creación de claves si a esto se añade la restricción del uso de nombres, apellidos, fecha de nacimiento o datos que pertenezcan a la información personal del usuario se estaría fortaleciendo este sistema de seguridad.

Algo específico del usuario.- Cada uno de los usuarios tienen características corporales únicas e intransferibles lo que permite que se pueda aplicar una seguridad más óptima sabiendo que realmente es el usuario que tiene los permisos para alguna actividad específica podríamos citar las características faciales, huellas dactilares, voz, etc.

Estos controles son los más automatizados dentro de esta clasificación. Los controles biométricos ya fueron descriptos en detalle anteriormente.

Hay una gran variedad de controles de este tipo, generalmente basados en las siguientes características del usuario:

- ✓ Huellas dactilares

- ✓ Patrones de la retina
- ✓ Geometría de la mano
- ✓ Dinámica de la firma
- ✓ Patrones de la voz

La seguridad aplicada para el acceso lógico por parte del usuario a la BD de la Clínica Humanitaria es el uso de usuario y contraseña, el sistema tiene la opción de permitir realizar cambios de contraseña sin límite de tiempo superior o inferior para la contraseña nueva, esto quiere decir que los usuarios tienen total libertad de realizar cambios en la contraseña las veces que el usuario desee, sin embargo existen usuarios que tienen su clave de acceso con un mínimo de tres caracteres y no se ha cambiado desde que se les ha otorgado el acceso al sistema informático es decir que alguna personas no han cambiado su clave por más de un año atrás, esto quiere decir que no se está cumpliendo con los parámetros de seguridad que se deberían los mismos que permitirán mantener un grado de seguridad adecuado a la información que se genera por parte de los usuarios.

ANALISIS DE VULNERABILIDAD DE ACCESO LOGICO A LA BD POR IDENTIFICACIÓN Y AUTENTICACION DE USUARIOS				
Descripción de la vulnerabilidad	**Nivel de Vulnerabilidad**			
	Grave	Alto	Medio	Nulo
Los usuarios se autentica mediante claves de acceso				**X**

Las claves de acceso se encuentran administradas mediante una BD				**X**
Las claves tiene estipulado un período de expiración de la clave		**X**		
La clave otorgada es susceptible de cambio por parte del usuario				**X**
Esta registradas las ultimas diez contraseñas utilizadas por el usuario	**X**			
El número de caracteres y tipo de caracteres para la contraseña es controlado		**X**		

Análisis a las vulnerabilidades encontradas de nivel Grave

Están registradas las ultimas diez contraseñas utilizadas por el usuario.- Una de las seguridades a nivel de usuario es el que cada una de las contraseñas puedan ser modificadas sin embargo estas no deben repetirse por lo menos con las últimas diez contraseñas, esto garantiza que si una contraseña de un usuario fue revelada anteriormente y cambio no tenga la posibilidad de volver a ingresar la misma.

ANALISIS DE LAS VULNERABILIDADES ENCONTRADAS

Las vulnerabilidades de la matriz que se encuentra detallada han sido realizadas en base al Cuadro de Nivel de impacto de las vulnerabilidades Fig1. En el que se indica los niveles de vulnerabilidades físicas y lógicas. Las vulnerabilidades encontradas han sido calificadas de acuerdo al impacto que tiene en la Clínica Humanitaria y a su vez en base a la metodología propuesta. Las vulnerabilidades de Nivel Grave necesitan ser corregidas o se consideran de gran amenaza o que tiene un alto impacto en el CPD, las vulnerabilidades de nivel alto, medio se encuentran de alguna manera controladas debido a que existen controles que se llevan a cabo sobre ellas de tal forma que su impacto esta mitigado gracias a las medidas que se han implementado.

DEFINICION DE POLITICAS

A la política se la define con reglas generales de comportamiento generadas para el correcto funcionamiento de los procesos dentro de una institución, teniendo que para la rama informática las políticas permiten mantener seguridad sobre los activos informáticos de la institución.

Las políticas que una institución implementa son de tipo particular y dependen de la cultura organizacional que se mantiene, es decir que las políticas se deben hacer a medida de cada institución de acuerdo a los requerimientos específicos.

CLINICA HUMANITARIA
FUNDACION PABLO JARAMILLO C.

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
2. Se debe tener sistema de detección de incendios	Grave

Objetivo:

Con el fin de precautelar los equipos del CPD y considerando que en ellos se alberga los datos, de igual manera considerando que ésta información es de uso general, permanente e imprescindible para la institución es necesario considerar la implementación para el CPD la siguiente política la misma que permitirá gestionar la seguridad frente a las vulnerabilidades contra incendios determinadas en el análisis de vulnerabilidades físicas del CPD.

Política:

f. Los administradores del CPD que estén a cargo deberán llevar el control periódico de cada uno de las instalaciones tanto eléctricas como de ventilación y control de temperatura de acuerdo con los estándares para el correcto funcionamiento de un CPD.

g. Los daños que se determinen al realizar la inspección al CPD se debe comunicar a los superiores con el fin de tomar las acciones correctivas de manera rápida y eficiente.

h. Para acceder al CPD durante las horas en las que no se encuentra el administrador del centro de cómputo el personal de seguridad deberá contar con los permisos correspondientes otorgados por las autoridades superiores de informática para permitir dicho acceso, de igual manera el personal de seguridad deberá registrar la hora de ingreso como la de salida y su correspondiente actividad que realizó.

i. Cada una de las revisiones se debe documentar y detallar los hallazgos que se haya determinado en el proceso de control del CPD.

j. Al presentarse situaciones de emergencia o de situaciones de urgencia, el acceso al CPD estará sujeto a las especificadas por las autoridades superiores del CPD.

Efecto de incumplimiento:

El no aplicar cada una de los puntos detallados anteriormente permitirá que se pueda suscitar un evento no deseado en el CPD el mismo que conlleva a que se provoque desde la pérdida de los datos a un siniestro de incendio.

CLINICA HUMANITARIA
FUNDACION PABLO JARAMILLO C.

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
2. Se utiliza la tecnología de dispositivos biométricos como seguridad del CPD	Grave

Objetivo:

Con el fin de evitar el acceso al CPD de personas ajenas al departamento y evitar daños provocados en equipos los mismos que conlleven a perdida de información, modificación, alteración, y otros actos que atenten con el buen funcionamiento de los equipos y programas del CPD es necesario tener en cuenta las siguientes políticas:

Política:

g. El acceso al CPD debe ser registrado y autorizado por la máxima autoridad el mismo que deberá registrar de manera detallada la fecha de acceso, la actividad a realizar y las correspondientes observaciones que se hayan generado en el tiempo de permanencia del personal.

h. Cada acceso al CPD debe ser por una actividad o necesidad específica y que requiera el acceso físico de tal manera que no se pueda realizar de manera remota.

i. Cada acceso será archivado de manera física con la correspondiente firma de responsabilidad de quien autoriza dicho acceso, al igual que la rúbrica del personal que ha obtenido el permiso para acceder al CPD.

j. Para acceder al CPD durante las horas no laborables por parte del personal del

departamento de cómputo el personal de seguridad general de la institución debe contar con la debida autorización para que pueda ingresar, éste ingreso debe ser registrado con la correspondiente hora de ingreso como la de salida, quien realizo la autorización y su correspondiente actividad que realizó.

k. Las autorizaciones deben ser de manera física (Papel escrito, o verbal) o lógica (Mediante correo electrónico)

l. Cuando no se cuente con las autorizaciones antes mencionadas y sea necesario el acceso del personal al CPD el personal de seguridad debe contactarse con los superiores de dicho personal los mismos que autoricen el acceso, el personal de seguridad deberá registrar cada uno de los sucesos

Efecto de incumplimiento:

El incumplimiento de éstas políticas permitirá que el acceso al CPD no sea controlado y que sea vulnerable a saboteos por parte de personal mal intencionado o con poca experiencia en el manejo y uso de los equipos del CPD.

CLINICA HUMANITARIA
FUNDACION PABLO JARAMILLO C.

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
4. Existe detallado un listado de autorizaciones de acceso al CPD 5. Está determinada las labores de la persona a quien se autoriza el ingreso al CPD 6. Está determinada las labores de la persona a quien se autoriza el ingreso al CPD	Grave

Objetivo:

Con el fin de precautelar la manipulación errada de los equipos e instalaciones del CPD al momento de permitir el acceso, es necesario aplicar las siguientes políticas.

Política:

c. El acceso al CPD debe ser autorizado por la máxima autoridad del departamento.

d. Se debe registrar el acceso al igual que la actividad a realizar por la persona autorizada, siempre debe estar bajo la supervisión de una persona del departamento que cuente con las destrezas y conocimientos para llevar a cabo la supervisión de acuerdo con las normas y procedimientos del CPD los mismos que puede detallarse de manera explícita o implícita.

Efecto de incumplimiento:

El no cumplir con estas políticas permitirá que se cometan errores y posible mal funcionamientos de los equipos o instalaciones que fueron manipuladas sin el conocimiento adecuado.

CLINICA HUMANITARIA
FUNDACION PABLO JARAMILLO C.

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
2. La cámara de seguridad se usa para vigilancia preventiva	Grave

Objetivo:

El mantener el CPD bajo una correcta y permanente vigilancia permitirá evitar siniestros no controlados o previstos.

Política:

c. Las cámaras deben ser monitoreadas periódicamente por el personal de seguridad de la institución con el fin de prevenir que sucesos siniestros puedan llegar a ser incontrolables o irreversibles.

d. El personal de seguridad tiene la obligación de monitorear las cámaras y al detectar alguna anomalía comunicar a las personas correspondientes y tomar las acciones para corregir o eliminar los problemas detectados.

Efecto de incumplimiento:

El no cumplir con esta política permitirá que no se pueda detectar problemas generados en el momento y por ende no controlar a tiempo lo que conlleva a que se pueda volver un problema incontrolable o irreparable.

CLINICA HUMANITARIA
FUNDACION PABLO JARAMILLO C.

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
3. Existe un control de humedad del CPD 4. La instalación del Climatizador se realizó mediante un estudio adecuado.	Grave

Objetivo:

Con el fin de precautelar la información y que las nuevas instalaciones tanto que afecten de manera directa o indirecta en el procesamiento de los datos se debe realizar un estudio previo de impactos y evaluación de los mismos antes de implementar al CPD.

Política:

d. La administración del CPD deberá emitir las normas y procedimientos que correspondan para realizar las instalaciones de nuevos componentes basados en estudios de factibilidad y evaluación de impactos para el CPD.

e. Los equipos instalados deben contar con la aprobación para la instalación de dicho equipo de manera documentada al igual que el estudio que sustente que el equipo es el idóneo para cubrir las necesidades del CPD

f. Los estudios deberán realizarse con la colaboración de personal tanto de la empresa como externo y sus resultados deben ser notificados y conocidos por los altos mandos de la institución.

Efecto de incumplimiento:

El no cumplir con estas políticas dará origen a realizar las implementaciones basadas en conocimientos empíricos y más no técnicos permitiendo que se generen errores tanto lógicos como físicos a corto o largo plazo.

CLINICA HUMANITARIA
FUNDACION PABLO JARAMILLO C.

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
2. Esta registradas las ultimas diez contraseñas utilizadas por el usuario	Grave

Objetivo:

Con el fin de precautelar la información que se alberga en la BD por parte de los usuarios debido al uso incorrecto de sus contraseñas es necesario aplicar las siguientes políticas que permitirán mantener un mejor control sobre las claves de acceso al sistema por parte de los usuarios.

Política:

f. Los administradores deben generar las normas y los procedimientos que permitan gestionar las claves seguras por parte de los usuarios que tengan permisos para acceder al sistema informático de la institución.

g. Los administradores deben fijar un tiempo de validez de las claves de acceso para los usuarios con el fin de que se encuentren en periodo de renovación.

h. Los administradores deben implementar los correspondientes procesos sobre la generación de claves seguras, tomando las consideraciones y estándares adecuados para conseguir dicho objetivo.

i. Los administradores deben mantener y transmitir la cultura de generar claves seguras para los nuevos usuarios del sistema informático al igual que refrescar los conocimientos de los usuarios antiguos.

j. Los administradores deben implementar los proceso que permitan controlar las

últimas claves registradas, de tal manera que sean inutilizables en las nueva clave que se desee ingresar, el número de claves a recordar debe ser tomada con el mejor criterio por parte del administrador a cargo de realizar este procedimiento, los usuarios no podrán ingresar al sistema una vez que haya expirado su clave y no se haya realizado la modificación.

Efecto de incumplimiento:

El incumplir con esta política permitirá mantener una vulnerabilidad lógica la misma que puede ser explotada por personas con conocimiento y a su vez sufrir ataques que pueden tener consecuencias no deseadas.

CLINICA HUMANITARIA
FUNDACION PABLO JARAMILLO C.

Política a implementarse en el CPD

Vulnerabilidad encontrada:	**Nivel:**
Política para gestionar los privilegios de acceso a la BD a los usuarios del sistema informático.	

Objetivo:

Con el fin de mantener la integridad, confidencialidad y disponibilidad de la información que está almacenada en el CPD es necesario aplicar las siguientes políticas

Política:

g. El administrador a cargo del CPD debe generar las normas y procedimientos mediante los cuales permitan otorgar a los usuarios los roles sobre la BD de tal manera que se asignen de manera acorde a las normas que se encuentren redactadas.

h. El administrador encargado de otorgar los roles a los usuarios sobre la BD deben conocer el perfil de los usuarios a los cuales va a asignar los permisos de acceso

i. Cada usuario debe poseer los permisos que necesite en el momento que se encuentre desarrollando las actividades a él encomendadas, es decir que cuando el usuario deje de hacer actividades ajenas al trabajo cotidiano es responsabilidad del administrador el quitar los permisos que no sean necesarios.

j. Los usuarios serán modificados los roles otorgados solamente cuando sea presentada la correspondiente solicitud para dicho proceso y sea aceptada por

el administrador del CPD, la solicitud deberá ser registrada y almacenada.

k. Las solicitudes de cambios en los roles de los usuarios deberán ser claros y específicos teniendo en cuenta los siguientes requerimientos:

- ✓ Nombres
- ✓ Cargo
- ✓ Fecha de inicio en las nuevas actividades
- ✓ Fecha de culminación de las actividades
- ✓ Firma de responsabilidad de quien solicita
- ✓ Firma de responsabilidad de quien aprueba

l. Esta información será administrada y agregada de acuerdo a los requerimientos del administrador del CPD.

Efecto de incumplimiento:

El incumplir con esta política permitirá que los usuarios que hayan sido otorgados permisos de acceso a la BD puedan seguir accediendo a información que no necesiten para sus labores cotidianas

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

En base del análisis de las vulnerabilidades determinadas y las políticas generadas para el CPD de la Clínica Humanitaria Pablo Jaramillo C. podemos decir:

La Institución al ser una clínica materno infantil ha prestado atención de manera muy dedicada a la infraestructura y atención al paciente tanto a nivel de salud como de gestión, no así, con la infraestructura y las seguridades para el CPD por lo que son llamados a gestionar los administradores, para que se implementen las seguridades adecuadas en dicho centro.

El CPD a pesar de encontrarse en un cuarto con seguridad, el monitoreo se realiza desde los equipos de los administradores, estos debería contar con las seguridades lógicas para los equipos ya que comparten el lugar con el departamento de Contabilidad y su acceso es libre.

Debido a la falta de interés en la seguridad del CPD por parte de los altos mandos no se ha llegado a implementar las correspondientes seguridades en el mismo y por ende no se han realizado los respectivos estudios para la implementación y adecuación del centro.

Pese a contar con la tecnología implementada para video vigilancia, dicha tecnología no es aprovechada para uso preventivo, al contrario es usada para corroborar un suceso que se haya dado, es decir que no se está cumpliendo con el objetivo de dicha tecnología que es de prevención.

Los usuarios no cuentan con los conocimientos y la cultura adecuados para gestionar claves de alta seguridad, razón por la cual las claves de acceso son consideradas de una seguridad baja.

Los accesos a la BD del sistema informático no cuentan con un procedimiento que permita al encargado guiarse o revisar mediante un documento elaborado, de igual manera no se cuenta con un soporte para revisar si los roles ya asignados a los usuarios son los correctos de acuerdo a sus labores que realizan.

Recomendaciones:

Se recomienda que el CPD no se encuentre ubicado junto al departamento de Contabilidad ya que no permite llevar un adecuado control de acceso al CPD.

Es necesario implementar un procedimiento para la implementación de nuevos componentes para el CPD en el que conste la solicitud de un análisis o estudio sobre el impacto y su idoneidad.

Es necesario designar al personal adecuado para el monitoreo de cámaras que se encuentran dispuestas en la institución de tal manera que se convierta en una tecnología de seguridad preventiva.

Se debe tener precaución con las personas que son autorizas para el acceso al CPD, para realizar tareas no técnicas (Limpieza, Mantenimiento, etc.) las mismas que al no poseer los conocimientos adecuados pueden ocasionar serios daños en los equipos.

Se debería tener o acondicionar un ambiente o área de visitas para el área de Contabilidad y el área de Sistemas o separar estas dos áreas.

Se debe generar un manual de proceso y procedimientos para las actividades del CPD el mismo que permita a cada uno de las personas que laboran conocer y consultar las actividades que realizan soportado en un manual.

El proceso y procedimientos que se encuentran generados deben ser revisados y actualizados con el fin de que se encuentren acorde a la realidad.

Las políticas deben ser sujetas a revisiones periódicas y a modificaciones para que se pueda cumplir con el objetivo que se el de mantener la seguridad y los buenos manejos del CPD.

DOCUMENTO DE ENTREGA RECEPCIÓN DE INFORME.

La información antes detallada es de propiedad única de la Clínica Humanitaria por lo que sus datos y hallazgos pertenecen a esta institución de salud y no podrá ser divulgada, publicada o vendida.

Entregado por:

_____

INGENIERO MIGUEL JUELA LEÓN.
ANALISTA DE VULNERABILIDADES

Recibido por:

_____

DOCTOR. MARCELO AGUILAR MOSCOSO
DIRECTOR MEDICO DE LA CLINICA HUMANITARIA.

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: ING. TANNIA MAYORGA
PARA: MSC. LUIS ANDRÉS CHÁVEZ ING.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 30 de Noviembre 2011.

Por medio de la presente certifico que el pregradista Miguel Trinidad Juela León con CI No.0103363693 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **ANALISIS DE VULNERABILIDADES FISICAS Y DE ACCESO LOGICO AL CENTRO DE COMPUTO DE LA CLINICA HUMANITARIA FUNDACION PABLO JARAMILLO C.**, del título de ingenieros en sistemas informáticos

Atentamente

_____
ING. TANNIA MAYORGA

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: ING. PABLO OCHOA
PARA: MSC. LUIS ANDRÉS CHÁVEZ ING.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 30 de Noviembre 2011.

Por medio de la presente certifico que el pregradista Miguel Trinidad Juela León con CI No.0103363693 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **ANALISIS DE VULNERABILIDADES FISICAS Y DE ACCESO LOGICO AL CENTRO DE COMPUTO DE LA CLINICA HUMANITARIA FUNDACION PABLO JARAMILLO C.**, del título de ingenieros en sistemas informáticos

Atentamente

_____
ING. PABLO OCHOA

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: ING. JUAN PEREZ
PARA: MSC. LUIS ANDRÉS CHÁVEZ ING.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 30 de Noviembre 2011.

Por medio de la presente certifico que el pregradista Miguel Trinidad Juela León con CI No.0103363693 han realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **ANALISIS DE VULNERABILIDADES FISICAS Y DE ACCESO LOGICO AL CENTRO DE COMPUTO DE LA CLINICA HUMANITARIA FUNDACION PABLO JARAMILLO C.**, del título de ingenieros en sistemas informáticos

Atentamente

_____
ING. JUAN PEREZ