ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Centro de Educación Continua

DIPLOMADO EN AUDITORÍA INFORMÁTICA

PROMOCIÓN V

PROYECTO

"Auditoría de Aplicación y Base de Datos"

AUTORES:

Ing. Marcos Delgado

Ing. Oscar Avilés

Año

2011

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

PROMOCIÓN V

PROYECTO

"Auditoría de Aplicación y Base de Datos"

AUTORES

Ing. Marcos Delgado

Ing. Oscar Avilés

AÑO

2011

INDICE

PROYECTO

Objetivo del Proyecto

El objetivo del proyecto, es realizar un trabajo de auditoría de bases de datos y aplicativo del Sistema de Visitas Médica, evaluando los controles generales sobre la base de datos y los controles de aplicación que se utilizan y verificando que los controles encontrados son los suficientes para asegurar la integridad, confiabilidad y disponibilidad de datos.

Alcance del Proyecto

El alcance del proyecto, es evaluar si se ha implementado políticas y procedimientos que existan en la empresa sobre el control de base de dato y aplicación del Sistema de Visitas Médica, para garantizar de manera razonable la integridad, confidencialidad y disponibilidad de la información.

Para esto, se realiza entrevistas con el personal de la Dirección de Sistemas para conocer los procesos y revisar de ser necesario asuntos específicos en el Sistema Medico.

Metodología

Se utilizará como referencia COBIT 4.1, como también las GTAG, en detalle la metodología es la siguiente:

- Levantamiento de Información.
- Evaluación de Riesgos.
- Elaborar Programa de Auditoría.
- Ejecutar Programa de Auditoría.
- Elaborar borrador de Informe de Auditoría.
- Presentar borrador de Informe de Auditoría a los Auditados.
- Presentación de Informe de Auditoría.

Equipo de Trabajo

El trabajo de Auditoría será realizado por los Ingenieros. Marcos Delgado Andrade y Oscar Avilés Ronquillo.

Observaciones Adicionales

El trabajo fue realizado con un acceso a lo información restringido, todo lo que tenemos documentado es en base a entrevistas.

PLAN Y PROGRAMA

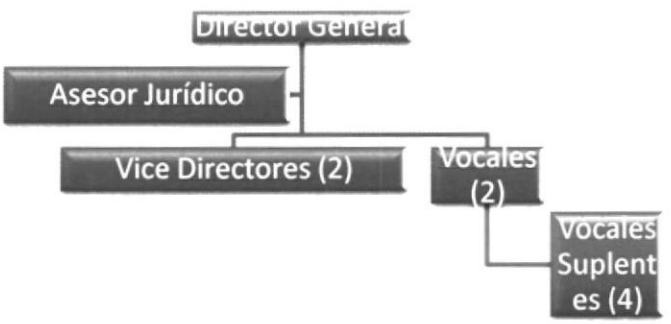
Investigación preliminar

La empresa, Fundación Medica fue fundada en 1888 por un grupo de filántropos liderado por Francisco Campos Coello, a quienes les preocupaban las condiciones de vida de los habitantes menos favorecidos de Guayaquil, ciudad que alberga el 27% de la población del Ecuador.

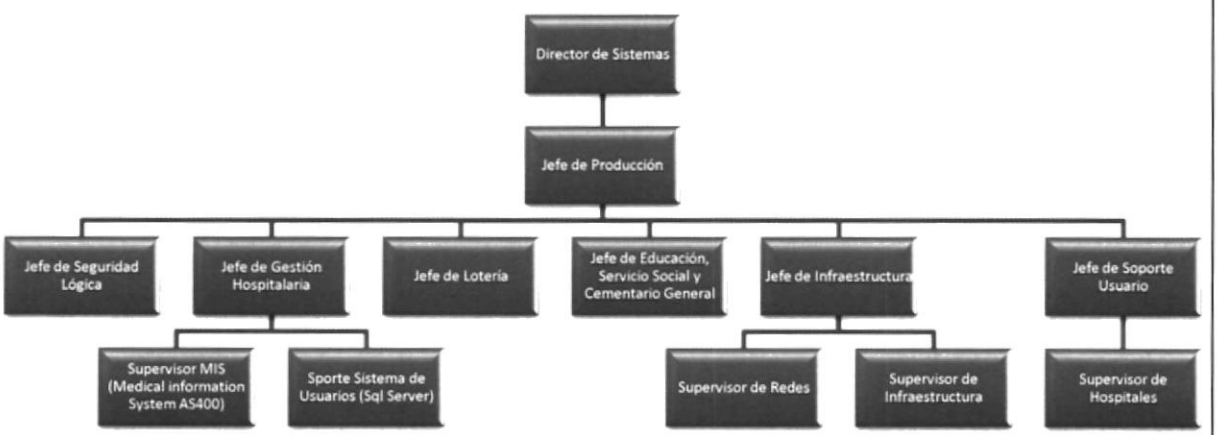
Los Servicios ofrecidos son Salud, Educación, Servicio Social, Cementerio General

La empresa FM está organizada de la siguiente manera:

- Comité Ejecutivo



- Funcionarios
- Administradores
- Directores Técnicos
- Sistemas



A continuación, se presenta un resumen del inventario de las tecnologías de la información de la Empresa FM.

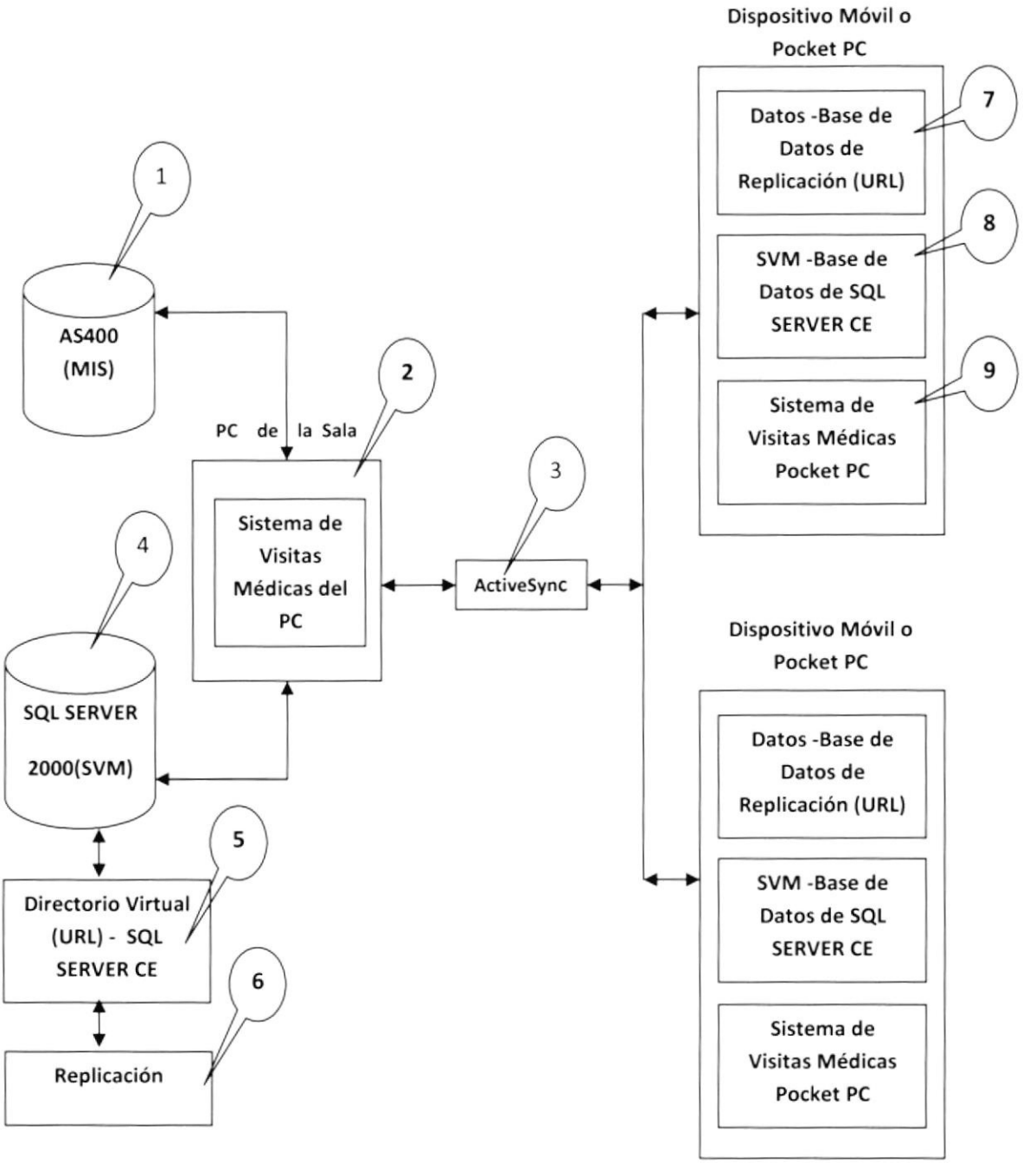
Activo de Información	Descripción	Importancia
Sistemas de Información		
SGC	Sistema Gerencial de Costo	Alta
SCP	Sistema de Control de Presupuesto	Alta
MIS	Medical Information System.	Media
Adams	Sistema para la Administración del Recurso Humano.	Media
SAC	Sistema Administrativo de Compra	Alta
SVM	Sistema de Vistas Medicas	Media
SCA	Sistema de Contabilización Automática	Alta
PRI	Programa de Incidentes y requerimientos	Baja
Tecnología de Información		
Servidores (10)	Base de Datos, Aplicaciones, Internet, Antivirus, Correo, BSC, Relojes Biométricos.	Alta
Enlaces	A bases de datos, internet, video conferencia, otros.	Alta
Computadores (225)	Para el uso de Trabajadores	Alta
Redes (Física e inalámbricas)	Comunicación	Alta

Los sistemas son desarrollados por la Dirección de Sistemas, utilizando con herramientas de desarrollo: VB, VB .Net y base de datos DB2, SQLServer, Informix.

El sistema MIS, es uno de los sistema más importante de la empresa, ya que el mismo soporta las operaciones. En dicho sistema, se registran proceso clínico y administrativo.

Los otros sistemas que tienen una importancia alta, dependen de la información que se genera el MIS. A continuación, se observa una gráfica del cómo el sistema médico interactúa con el sistema MIS, a través de los dispositivos móviles.

A continuación la arquitectura del Sistema de Visitas Médica:



ESPECIFICACIONES TÉCNICAS DEL SISTEMA MEDICO

1.- Base de datos AS400 → Sistema de Información Médica (**MIS**)

2.- PC de la Sala → Contiene el Sistema de Visitas Médica del PC

3.- ActiveSync → Es un programa instalado en el PC de la Sala que permite crear una **relación de sincronización** entre el dispositivo móvil y su PC mediante un cable a través del puerto USB.

4.- SQL Server 2000 → Contiene Base de Datos del Sistema de Vistas Médica.

5.- Directorio Virtual → Es necesario crearlo para accesar a los datos. A continuación una lista de los directorios virtuales por **Especialidad** y **Sala**.

6.- Replicación → Permite la copia de objetos de la base de datos y distribución de la información creando un vinculo entre ambas bases de datos para que exista consistencia.

Usando replicación se puede distribuir los datos a diferentes locaciones, utilizando usuarios remotos o móviles (**Pocket PC**), conectados a una Red Local o por Internet.

El tipo de replicación que utilizamos es **Merge** o replicación por **Mezcla.** Este es el método que utilizamos en los Dispositivos Móviles o Pocket PC. Consiste en que el **Servidor** envía una petición a los **subscriptores** (Pocket PC) y a continuación por petición del subscriptor cada vez que se realicen cambios en la publicación (alguno de los artículos o tablas de esta) del servidor, se envían al subscriptor UNICAMENTE los cambios que se han efectuado realizado a demanda.

7.- Base de datos de Replicación → El Dispositivo Móvil o **Pocket PC** contiene la Base de datos de replicación **Datos.sdf** que permite intercambiar la información del **Servidor** a las **Pocket PC de la Sala**.

8.- Base de datos de SQL Server CE → El Dispositivo Móvil o **Pocket PC** contiene la Base de datos **SVM.sdf**, esta tiene la información que está en Producción de un centro de costo o Salas.

Evaluación de Riesgos

1. **Objetivo**

   El objetivo de la Evaluación de Riesgos, es identificar los riesgos detectados durante el levantamiento de información; valorar el impacto sobre los objetivos y continuidad del negocio y orientar la auditoria hacia los riesgos más importantes.

2. **Calificación del riesgo**

   Para determinar si un riesgo identificado es alto, medio o bajo, se utilizan los siguientes criterios:

   - *Probabilidad:*

     Se refiere a la probabilidad de ocurrencia de la explotación de la vulnerabilidad respecto del riesgo.

   - *Impacto:*

     Se refiere al impacto que tiene el riesgo, sobre el logro de objetivos y la continuidad del negocio. Se obtiene multiplicando la frecuencia y la materialidad. A continuación, se presenta los rangos de impacto, para calificar los riesgos:

Nivel	Rango
Alto	6 - 9
Medio	3 - 5
Bajo	1 - 2

Matriz de Evaluación de Riesgos

Administración de Usuario y Perfiles

Objetivo de Control	Afecta	Riesgos	Probabilidad	Impacto	Riesgo
Correcta administración de usuarios	Base de Datos **SVM** Aplicación PC **SVM**	Exposición al mal uso de los bienes informáticos, lo cual puede ocasionar problemas a los servicios y operaciones de la organización.	2	6	ALTO
	Base de Datos **SVM** Aplicación PC **SVM**	Usuarios asignados a varios roles permitiendo el acceso a la información libremente.	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Asignación no documentada y descontrolada de los roles de los usuarios.	2	6	ALTO
	Base de Datos **SVM** Aplicación PC **SVM**	Existencia de cuentas de usuarios activas de personal que no labora actualmente para la organización.	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Cuentas no usadas por periodos largos se mantiene activas	2	3	MEDIO
Correcta administración de los perfiles de usuario	Base de Datos **SVM** Aplicación PC **SVM**	Perfiles de usuarios no compatibles con el manual de funciones del personal	3	3	ALTO
	Base de Datos **SVM** Aplicación PC **SVM**	Perfiles de usuarios asignados a personal no adecuado	1	1	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Acceso y manipulación de información por personal no autorizado	1	1	BAJO

Administración de Accesos de Usuarios & Datos

Objetivo de Control	Afecta	Riesgos	Probabilidad	Impacto	Riesgo
Correcta administración de Usuarios y datos	Base de Datos **SVM** Aplicación PC **SVM**	Acceso al aplicativo y base de datos con cuentas de personal que ya no labora en la organización	3	3	MEDIO
	Base de Datos **SVM** Aplicación PC **SVM**	Privilegios de administración de la base de datos o administración de accesos al aplicativo estén asignados a personal no autorizado	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Existencias de falencias en la seguridad de los sistemas y bases de datos, sin las acciones correctivas correspondientes	6	9	ALTO
	Base de Datos **SVM** Aplicación PC **SVM**	Desconocimiento de las gerencias de las falencias de seguridad que permitan el análisis respectivo para gestionar las acciones correctivas	2	6	ALTO
	Base de Datos **SVM**	Asignación de cuentas genéricas de operación de base de datos a usuarios que no autorizados	1	2	BAJO
	Base de Datos **SVM**	Cuentas genéricas con accesos privilegiados sin restricciones periódicas	1	2	BAJO
	Base de Datos **SVM**	Cuentas por default de la base de datos de producción asignadas a personal de desarrollo	1	2	BAJO

Administración de contraseña

Objetivo de Control	Afecta	Riesgos	Probabilidad	Impacto	Riesgo
Administración segura de Contraseñas	Base de Datos **SVM** Aplicación PC **SVM**	Violaciones de acceso por contraseñas asociadas a cosas personales del personal	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Uso repetitivos de claves al renovarlas por parte de los usuarios	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Acceso no autorizados a cuentas de usuarios por un usuario no propietario de la cuenta	3	9	ALTO

Administración de Cambios

Objetivo de Control	Afecta	Riesgos	Probabilidad	Impacto	Riesgo
Administración de Cambios	Base de Datos **SVM** Aplicación PC **SVM**	Procesos operativos no autorizados	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Cambios en los procesos operacionales no documentados ni autorizados	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Modificaciones en la estructura de base de datos o en la aplicación (desarrollo), en el ambiente de producción	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Modificaciones pasadas a producción sin las respectivas autorizaciones y no documentadas	3	5	MEDIO
	Base de Datos **SVM** Aplicación PC **SVM**	Pases a producción sin responsabilidades definidas en casos de fallos en producción	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Errores en producción por cambios emergentes o no emergentes, sin la debida documentación para poder implementar las acciones correctivas de forma ágil	2	2	BAJO
	Base de Datos **SVM**	Actualizaciones de seguridad no instaladas	1	2	BAJO

Procedimientos & Programas

Objetivo de Control	Afecta	Riesgos	Probabilidad	Impacto	Riesgo
Seguridad, Respaldo y Recuperación	ORGANIZACIÓN	Acceso por personal no autorizado al centro de computo	1	2	BAJO
	ORGANIZACIÓN	Uso indebido de los activos físicos del centro de computo	1	2	BAJO
	Base de Datos **SVM** Aplicación PC **SVM**	Caída prolongada de los servicios soportados por el servidor de aplicación y Base de datos	3	3	MEDIO
	Base de Datos **SVM** Aplicación PC **SVM**	Dependencia total en una persona para la solución de calidad de servicios informáticos	3	5	MEDIO
	Base de Datos **SVM**	Respaldos incompletos de información	1	2	BAJO
	Base de Datos **SVM**	Inexistencia de respaldos en momentos críticos	1	2	BAJO
	Base de Datos **SVM**	Respaldos no utilizables por daños físicos del medio de almacenamiento	1	2	BAJO
	Base de Datos **SVM**	Recuperación de datos en tiempos demasiado largos	3	5	MEDIO
	Base de Datos **SVM**	Imposibilidad de recuperación de datos	3	5	MEDIO

Aplicaciones visuales - Integraciones

Objetivo de Control	Afecta	Riesgos	Probabilidad	Impacto	Riesgo
Administración de Conexiones del aplicativo SVM PC y dispositivo móvil	Aplicación PC **SVM**	Los información de los pacientes no puedan ser cargados en la base de datos del SVM desde el MIS y viceversa	3	6	ALTO
	Aplicación PC **SVM** Aplicación Móvil **SVM**	La información de los pacientes no pueda ser cargada desde la base de datos SVM en los dispositivos móviles y viceversa	3	6	ALTO
	Aplicación Móvil **SVM**	Robo o daño del dispositivo móvil. Lentitud del dispositivo móvil. No existe Servidor de Contingencia	3	9	ALTO

Tipo y Cantidad de Riesgos Encontrados

Evaluación de Riesgos	Cantidad de Riesgos
Altos	9
Medios	7
Bajos	21

AUDITORIA

Objetivos de Auditoría

Determinar la existencia de controles en base a los riesgos con calificación alta resultantes de la evaluación de riesgos ejecutada que afectan la base de datos y aplicativo SVM, para determinar que la información se mantiene integra, confiable y disponible. Asegurando que la manipulación de la información de los pacientes cumple con los criterios importantes de la información.

Áreas o componentes a auditar

Se auditará la base de datos SVM que soporta el aplicativo SVM, al aplicativo SVM y el entorno informático en el que operan.

Alcance de la Auditoría

El alcance de la presente auditoría, es verificar si se han implementado los controles necesarios en la gestión del aplicativo SVM y la base de datos que soporta el aplicativo, de manera tal, que garanticen de manera razonable la integridad, confidencialidad y disponibilidad de la información.

Para lo cual, se realizaran reuniones con el personal del Departamento de TI para conocer los procesos que llevan a cabo, se les solicitara documentación de dichos procesos, y de ameritar el caso, se revisara asuntos específicos en el Sistema de Visita Médica y la base de datos.

Herramientas

Los programas a utilizar para la presente auditoría son:

- Word 2007/2010: Procesador de Texto.
- Excel 2007/2010: Hoja de Cálculo.
- MIS : Sistema de Información Médica
- SVM : Sistema de Visitas Médicas.
- SQL 2000 : Consultas a la Base de Datos

PROGRAMA DE AUDITORIA

En base a los riesgos calificados como altos en la ejecución de la Evaluación de Riegos, el objetivo es evaluar los controles generales implementados en la gestión de las tecnologías de la información de la Empresa, para verificar si se garantiza de manera razonable la integridad, confidencialidad y disponibilidad de la información. Se toma como marco las guías GTAGs.

Administración de Usuarios y Perfiles

Objetivo de Control	Riesgo	Nivel de Riesgo	Actividad de Control	Procedimiento de Auditoría
Correcta administración de usuarios	Exposición al mal uso de los bienes informáticos, lo cual puede ocasionar problemas a los servicios y operaciones de la organización.	ALTO	Política de seguridad de usuarios ha sido establecida para asegurar el correcto uso de los activos de información de la organización	1.- Solicitar y revisar la política de seguridad de usuarios de la organización. 2.- Si existiera determinar si es la versión más actualizada. 3.- Determinar quienes tiene acceso a la revisión de la política de seguridad de usuarios
	Asignación no documentada y descontrolada de los roles de los usuarios.	ALTO	Procedimientos para asegurar que un requerimiento de usuario es aprobado y documentado antes de asignarle los privilegios de accesos a los datos y sistemas.	1. Pregunte a la persona adecuada del proceso para Solicitar y revisar el acceso de usuario de la base de datos como del aplicativo. Asegúrese de que los controles internos existen para verificar que el acceso solicitado es apropiado y aprobado. 2. Asegúrese de que existe una lista de autorizaciones que define los aprobadores / propietarios de los recursos que debe aprobar el acceso solicitado antes de conceder el acceso. 3. Examinar y evaluar si la estructura organizacional es adecuada de acuerdo a los controles internos.

Objetivo de Control	Riesgo	Nivel de Riesgo	Actividad de Control	Procedimiento de Auditoría
Correcta administración de usuarios	Asignación no documentada y descontrolada de los roles de los usuarios.	ALTO	Procedimientos para asegurar que un requerimiento de usuario es aprobado y documentado antes de asignarle los privilegios de accesos a los datos y sistemas.	4. Revisar y evaluar los diferentes niveles de autorización para uno o más entornos de producción. Evaluar el alcance y la razonabilidad de estas autorizaciones, teniendo en cuenta la función del usuario y la posición en la organización. 5. Examinar y evaluar si el acceso del usuario con privilegios para la base de datos es controlado de acuerdo con los procedimientos. 6. Revisar y evaluar las autorizaciones seleccionadas de acuerdo con las regulaciones (por ejemplo, hacer identificaciones personales de los usuarios, tener identificado el acceso que se ha otorgado a través de un procedimiento formal y verificarlo tanto para la base de datos como para el aplicativo) 7. Solicitar y revisar la lista de usuarios de la tabla users tomar una muestra de cuentas creadas dentro del periodo de revisión. Revisar los accesos otorgados a estas cuentas que estén acorde al requerimiento aprobado formal. 8. Evaluar si existe y debe haber enlace entre los accesos otorgados a la base de datos, el sistema operativo establecido y el aplicativo. 9. Examinar y evaluar si la autorización a la base de datos ha sido definida a través del sistema operativo o el aplicativo

Objetivo de Control	Riesgo	Nivel Riesgo	Actividad de Control	Procedimiento de Auditoría
Correcta administración de los perfiles de usuario	Perfiles de usuarios no compatibles con el manual de funciones del personal	ALTO	Política y Procedimiento para la definición de perfiles	1.- Solicitar y revisar la política para la definición de los perfiles para el uso del aplicativo PC, como para la base de datos.
				2.- Solicitar y revisar el procedimiento usado por la organización para la documentación de los perfiles definidos para el uso de los diferentes usuarios del aplicativo, como los de la base de datos

Administración de Accesos de Usuarios & Datos

Objetivo de Control	Riesgo	Nivel de Riesgo	Actividad de Control	Procedimiento de Auditoría
Administración de Usuarios y datos	Existencias de falencias en la seguridad de los sistemas y bases de datos, sin las acciones correctivas correspondientes	ALTO	El administrador de seguridad supervisa y registra las actividades ejecutadas de seguridad	1.- Revisión de los registros de las actividades de seguridad ejecutadas por el administrador de seguridad.
	Desconocimiento de las gerencias de las falencias de seguridad que permitan el análisis respectivo para gestionar las acciones correctivas	ALTO	La violaciones de seguridad son identificadas y notificadas a la alta dirección e investigadas de manera oportuna por los procedimientos establecidos	1.- Revisión de la política y procedimiento existente para la revisión de seguridad de los sistemas. 2.- Revisión del procedimiento usado para realizar los reportes de incidentes de seguridad a la alta gerencia. 3.- Solicitar y revisar el procedimiento de asignación de responsabilidades para el manejo de incidentes. 4.- Revisión del los registros de incidentes de seguridad y las acciones correctivas implementadas.

Administración de contraseña

Objetivo de Control	Riesgo	Nivel de Riesgo	Actividad de Control	Procedimiento de Auditoría
Administración segura de Contraseñas	Acceso no autorizados a cuentas de usuarios por un usuario no propietario de la cuenta	ALTO	1.- Se establece un mínimo de claves en el histórico de claves, para no permitir la repetición de claves 2.- Existe el bloqueo de la cuenta cuando existen más de tres intentos de inicio de sesión y si las sesiones se cierran después de un tiempo de inactividad.	1. Entrevistar al administrador del sistema para determinar si hay productos de terceros o controles internos que se han desarrollado y que requiere seleccionar usuarios y contraseñas que no sean nulas, fáciles de adivinar, y contengan como mínimo dos caracteres alfabéticos y numéricos. 2. Asegúrese de que la configuración de la contraseña cumple con la directiva de contraseñas de la organización y las mejores prácticas. 3. Solicitar y revisar la documentación de las políticas de creación de claves. 4. Realizar la revisión de la configuración de la administración de claves. 5. Revisión de la documentación de entrenamiento al personal sobre el uso de contraseñas

Aplicaciones visuales – Integraciones

Objetivo de Control	Riesgo	Nivel de Riesgo	Actividad de Control	Procedimiento de Auditoría
Administración de Conexiones del aplicativo SVM PC y dispositivo móvil	Los información de los pacientes no puedan ser cargados en la base de datos del SVM desde el MIS y viceversa	ALTO	Procedimiento para la verificación de las conexiones de la base de datos del SVM al MIS (AS/400)	1.- Solicitar y revisar el procedimiento utilizado para la evaluación de las conexiones. 2.- Solicitar y revisar el registro de las revisiones de las conexiones. 3.- Solicitar y revisar el registro de los incidentes de fallos de conexión, con la respectiva acción correctiva. 4.- Determinas si las acciones correctivas dieron una solución estable a los fallos de conexión
	La información de los pacientes no pueda ser cargada en las dispositivos móviles	ALTO	Procedimiento de verificación de las conexiones de los dispositivos móviles con el PC	
		ALTO	Procedimiento alterno para el pase de información del PC al Móvil	1.- Solicitar y revisar el procedimiento establecido como contingente en el caso de que no esté disponible por robo o daño el dispositivo móvil. 2.- Solicitar y revisar el registro de incidente por daño o robo de dispositivos móviles. 3.-Solicitar y revisar si existen un plan de contingencia en caso de caída de la base de datos
	Robo o daño del dispositivo móvil	ALTO		

EJECUCIÓN DE LA AUDITORIA

Administración de Usuario y Perfiles

Actividad de Control	Procedimiento de Auditoría	Resultado de la revisión	Evidencia
Política de seguridad de usuarios ha sido establecida para asegurar el correcto uso de los activos de información de la organización	1.- Solicitar y revisar la política de seguridad de usuarios de la organización. 2.- Si existiera determinar si es la versión más actualizada. 3.- Determinar quienes tiene acceso a la revisión de la política de seguridad de usuarios	Se ha evidenciado que actualmente existen políticas de seguridad de la organización que se encuentra compartida en un directorio público, pero no se encontró un registro de revisión de la política.	Política Segdeusu
Procedimientos para asegurar que un requerimiento de usuario es aprobado y documentado antes de asignarle los privilegios de accesos a los datos y sistemas.	1. Pregunte a la persona adecuada del proceso para Solicitar y revisar el acceso de usuario de la base de datos como del aplicativo. Asegúrese de que los controles internos existen para verificar que el acceso solicitado es apropiado y aprobado. 2. Asegúrese de que existe una lista de autorizaciones que define los aprobadores / propietarios de los recursos que debe aprobar el acceso solicitado antes de conceder el acceso. 3. Examinar y evaluar si la estructura organizacional es adecuada de acuerdo a los controles internos. 4. Revisar y evaluar los diferentes niveles de autorización para uno o más entornos de producción. Evaluar el alcance y la razonabilidad de estas autorizaciones, teniendo en cuenta la función del usuario y la posición en la organización.	Se ha evidenciado que actualmente existen procedimientos para el acceso de usuario a las aplicaciones. Pero también se evidencio que no existe procedimiento para la creación de usuarios a las base de datos.	Procedimiento accesos

Administración de Usuario y Perfiles

Actividad de Control	Procedimiento de Auditoría	Resultado de la revisión	Evidencia
Procedimientos para asegurar que un requerimiento de Usuario es aprobado y documentado antes de asignarle los privilegios de accesos a los datos y sistemas.	5. Examinar y evaluar si el acceso del usuario con privilegios para la base de datos es controlado de acuerdo con los procedimientos. 6. Revisar y evaluar las autorizaciones seleccionadas de acuerdo con las regulaciones (por ejemplo, hacer identificaciones personales de los usuarios, tener identificado el acceso que se ha otorgado a través de un procedimiento formal y verificarlo tanto para la base de datos como para el aplicativo) 7. Solicitar y revisar la lista de usuarios de la tabla users tomar una muestra de cuentas creadas dentro del periodo de revisión. Revisar los accesos otorgados a estas cuentas que estén acorde al requerimiento aprobado formal. 8. Evaluar si existe y debe haber enlace entre los accesos otorgados a la base de datos, el sistema operativo establecido y el aplicativo. 9. Examinar y evaluar si la autorización a la base de datos ha sido definida a través del sistema operativo o el aplicativo	Se ha evidenciado que actualmente existen procedimientos para el acceso de usuario a las aplicaciones. Pero también se evidencio que no existe procedimiento para la creación de usuarios a las base de datos.	Procedimiento accesos

Administración de Usuario y Perfiles

Actividad de Control	Procedimiento de Auditoría	Resultado de la revisión	Evidencia
Política y Procedimiento para la definición de perfiles	1.- Solicitar y revisar el procedimiento para la definición de los perfiles para el uso del aplicativo PC, como para la base de datos. 2.- Solicitar y revisar el procedimiento usado por la organización para la documentación de los perfiles definidos para el uso de los diferentes usuarios del aplicativo, como los de la base de datos	Se evidencio que existe una política de los perfiles del aplicativo, pero no existe una política de perfiles o roles de base de datos.	Política Segdeusu

Administración de Accesos de Usuarios & Datos

Actividad de Control	Procedimiento de Auditoría	Resultado de la revisión	Evidencia
El administrador de seguridad supervisa y registra las actividades ejecutadas de seguridad.	1.- Revisión de los registros de las actividades de seguridad ejecutadas por el administrador de seguridad.	No se tuvo acceso a las políticas	No existen evidencias
Las violaciones de seguridad son identificadas y notificadas a la alta dirección e investigadas de manera oportuna por los procedimientos establecidos.	1.- Revisión de la política y procedimiento existente para la revisión de seguridad de los sistemas. 2.- Revisión del procedimiento usado para realizar los reportes de incidentes de seguridad a la alta gerencia. 3.- Solicitar y revisar el procedimiento de asignación de responsabilidades para el manejo de incidentes. 4.- Revisión del los registros de incidentes de seguridad y las acciones correctivas implementadas.		

Administración de Contraseñas

Actividad de Control	Procedimiento de Auditoría	Resultado de la revisión	Evidencia
1.- Se establece un mínimo de claves en el histórico de claves, para no permitir la repetición de claves 2.- Existe el bloqueo de la cuenta cuando existen más de tres intentos de loggeo y si las sesiones se cierran después de un tiempo de inactividad.	1. Entrevistar al administrador del sistema para determinar si hay productos de terceros o controles internos que se han desarrollado y que requiere seleccionar usuarios y contraseñas que no sean nulas, fáciles de adivinar, y contengan como mínimo dos caracteres alfabéticos y numéricos. 2. Asegúrese de que la configuración de la contraseña cumple con la directiva de contraseñas de la organización y las mejores prácticas. 3. Solicitar y revisar la documentación de las políticas de creación de claves. 4. Realizar la revisión de la configuración de la administración de claves. 5. Revisión de la documentación de entrenamiento al personal sobre el uso de contraseñas	Se evidencio que existe un procedimiento de contraseñas de aplicaciones, sin embargo no existe un procedimiento para las contraseñas de base de datos. Las sesiones no se cierran después de un tiempo de inactividad.	Procedimiento accesos

Aplicaciones visuales – Integraciones

Actividad de Control	Procedimiento de Auditoría	Resultado de la revisión	Evidencia
Procedimiento para la verificación de las conexiones de la base de datos del SVM al MIS (AS/400) Procedimiento de verificación de las conexiones de los dispositivos móviles con el PC	1.- Solicitar y revisar el procedimiento utilizado para la evaluación de las conexiones. 2.- Solicitar y revisar el registro de las revisiones de las conexiones. 3.- Solicitar y revisar el registro de los incidentes de fallos de conexión, con la respectiva acción correctiva. 4.- Determinas si las acciones correctivas dieron una solución estable a los fallos de conexión	1.- Comunicaciones Eventualmente existen fallas en las comunicaciones, causando problemas en la ejecución de los servicios de transferencia de datos desde la aplicación SVM – MIS 2.- Sincronización En ocasiones no se puede cargar la información a los dispositivos móviles, porque no fue colocado correctamente el dispositivo móvil en la base de sincronización del escritorio. 3.- Depuración Lentitud en el dispositivo móvil.	Log de Pedidos
Procedimiento alterno para el pase de información del PC al Móvil	1.- Solicitar y revisar el procedimiento establecido como contingente en el caso de que no esté disponible por robo o daño el dispositivo móvil. 2.- Solicitar y revisar el registro de incidente por daño o robo de dispositivos móviles. 3.-Solicitar y revisar si existen un plan de contingencia en caso de caída de la base de datos.	4.- Servidor de Contingencia No existe un Servidor de Contingencia para el Sistema de Visitas Médicas.	

Hallazgos y Recomendaciones

Administración de Usuarios y Perfiles

Hallazgos.-

Se ha evidenciado que actualmente existen políticas de seguridad de la organización, pero no se encontró un registro de revisión de la política, se recomienda la revisión periódica de las políticas para asegurar que se mantenga actualizada acorde al desarrollo tecnológico de la organización y su respectivo registro de revisión que evidencie dicho proceso.

Actualmente no existe un procedimiento para la creación de usuarios de base de datos.

Riesgos.-

1. Exposición al mal uso de los bienes informáticos, lo cual puede ocasionar problemas a los servicios y operaciones de la organización.
2. Asignación no documentada y descontrolada de los roles de los usuarios.
3. Perfiles de usuarios no compatibles con el manual de funciones del personal

Recomendación.-

Se recomienda estandarizar el proceso para la creación de usuarios a lo largo de todos los aplicativos y bases de datos; recomendable a través de las aplicaciones que se utilizan. Así como también la creación de un procedimiento formal de creación de usuarios para el sistema aplicativo, en el que conste la aprobación por parte del dueño de los datos para la asignación de permisos de acceso de información.

Es importante manejar roles en la aplicación, porque de esta manera minimizamos los riesgos de los accesos no autorizados.

Administración de Accesos de Usuarios & Datos

Hallazgos.-

El departamento de sistemas no ha implementado un procedimiento para el ingreso de problemas de seguridad, incidentes de seguridad y monitoreo de los mismos. Por lo que no se cuenta con información que permita emitir estadísticas de los problemas recurrentes que se les presentan a los usuarios. Esta situación impide determinar adecuadamente eventos de riesgos repetitivos o recurrentes, que afecten la calidad del servicio ofrecido al cliente interno, pudiendo ocasionar interrupciones en la ejecución de las operaciones diarias del negocio.

Riesgos.-

1. Existencias de falencias en la seguridad de los sistemas y bases de datos, sin las acciones correctivas correspondientes
2. Desconocimiento de las gerencias de las falencias de seguridad que permitan el análisis respectivo para gestionar las acciones correctivas

Recomendación.-

La Gerencia General deberá instruir al Jefe de Seguridad que establezca procedimientos que permitan determinar los problemas recurrentes, con la finalidad de llevar a cabo soluciones óptimas ante los diferentes eventos y así mejorar el nivel de servicio del departamento de tecnología.

Administración de contraseña

Hallazgos.-

Las sesiones no se cierran después de un tiempo de inactividad y no existe un procedimiento de contraseña de base de datos.

Riesgos.-

1. Acceso no autorizado a cuentas de usuarios por un usuario no propietario de la cuenta.

Recomendación.-

La Gerencia General deberá analizar la posibilidad de contratar personal calificado que realice las funciones de Oficial o Administrador de Seguridad de Información, quien deberá ser el responsable de proveer seguridad física y lógica adecuada para los programas y sistemas, datos y equipos, con base en los lineamientos establecidos por la política de seguridad de la información de la entidad. Es importante mencionar que para asegurar la independencia y evitar conflicto de intereses, el oficial o administrador de seguridad de información no debe de pertenecer al área de sistemas, ni a áreas operativas de la entidad.

Aplicaciones visuales – Integraciones

Hallazgos.-

Eventualmente existen fallas en las comunicaciones, causando problemas en la ejecución de los servicios de transferencia de datos desde la aplicación SVM – MIS y en ocasiones no se puede cargar la información a los dispositivos móviles, porque no fue colocado correctamente el dispositivo móvil en la base de sincronización del escritorio.

Existe lentitud en los dispositivos móviles. No existe servidor de contingencia para SVM.

Riesgos.-

1. Los información de los pacientes no puedan ser cargados en la base de datos del SVM desde el MIS y viceversa
2. La información de los pacientes no pueda ser cargada en las dispositivos móviles
3. Robo o daño del dispositivo móvil

Recomendación.-

La Gerencia General, deberá instruir al Jefe de Sistemas y Jefe de Gestión Hospitalaria para que revise los acuerdos de niveles de servicio y realizar un procedimiento para el uso del dispositivo móvil.

Realizar una depuración de la base de datos del dispositivo móvil periódicamente (cada 30 días) con la finalidad del que Sistema sea rápido y no cause retraso en el pase de vista del médico a los pacientes.

Establecer y formalizar los procedimientos contingentes en el caso que se materialicen los riesgos analizados.

Lo importante es que se atienda de manera oportuna la solicitud de medicinas, para que sea llevada a las Salas de Hospitalización para su uso.

INFORME DE AUDITORIA

De acuerdo con lo acordado con Usted, hemos realizado una Auditoría Informática a los controles de las Tecnologías de la Información utilizados en el aplicativo Sistemas de Visitas Medicas y la base de datos que soporta el dicho aplicativo, vigentes a Noviembre del 2011; con el propósito de evaluar si dichos controles garantizan de manera razonable la integridad, confidencialidad y disponibilidad de la información de la Organización.

Nuestro trabajo se realizó en base al marco referencial COBIT 4.1, que se refiere a los controles para la información y la tecnología relacionada, como también se utilizó como guía las GTAG. Estas normas requieren entre otras cosas, el diseño y desarrollo de pruebas de auditoría apropiadas, para cumplir con el objetivo de la misma; incluyendo la obtención de evidencia suficiente y competente, para sustentar nuestros hallazgos.

Alcance

El alcance de nuestra revisión, consistió en:

a) Levantamiento de información sobre la estructura de las Tecnologías de la Información que soporta el aplicativo Sistema de Visitas Médicas.

b) Evaluar políticas y procedimientos vigentes de administración de usuarios del Sistema de Visitas Médicas

c) Evaluar políticas y procedimientos de seguridad de la información.

d) Ejecutar la evaluación de Riesgos sobre Sistema de Visitas Médicas

e) Evaluar los procesos de desarrollo, pruebas, cambios e implementación de aplicativos.

f) Evaluar el plan de contingencia por fallos de la disponibilidad de la Base de Datos del SVM.

g) Revisar que los Usuarios del Sistemas de Visitas Medicas y de Base de Datos de ex trabajadores, estén desactivados

Conclusión

De acuerdo a los resultados de la evaluación realizada hemos determinado una opinión favorable, debido a que no tuvimos indicios de irregularidades que fueran explotadas en los objetivos de control evaluados, no obstante existen aspectos que deben ser considerados como mejoras del control interno, los mismos de no ser tomados en cuenta, podrían ser explotados y representar para la institución perjuicio a nivel económico, de imagen y reputación.