HOJA DE RUTA						
Empresa:	**HOSPITAL GENERAL DE MEDELLÍN**					
Tipo de Relación:	Auditoria de Sistemas de Información					
Etapa de la prestación del servicio:	**Ejecución**					
Informe de:	Auditoría de Sistemas Controles de los procesos de TI					
Fecha de Corte:	Octubre de 2018					
Estado del informe:	Socializado		Borrador	■	Definitivo	

Medellín, 26 de octubre 2018

Señores
Hospital General de Medellín S.A.
DR. Jesús Eugenio Bustamante Cano
Gerente General
Ciudad

Asunto: Auditoria de Sistemas – Evaluación de controles generales de SAP

Respetado Doctor Bustamante:

En cumplimiento del escrito contractual suscrito entre las partes, ponemos a su consideración el resultado obtenido de la primera fase de la **AUDITORIA DE SISTEMAS,** la cual, se programó para ejecutar a partir del 04 de octubre de 2018.

Nuestra revisión contempló los siguientes aspectos:

- *Entendimiento de los procesos de TI*
- *Revisión del proceso de control de accesos*
- *Revisión del proceso de gestión de cambios*
- *Validación de las operaciones de cómputo*
- *Revisión del data center*

Es importante indicar, que todos los aspectos mencionados en el alcance anterior fueron evaluados por parte de esta auditoría y aquellos que fueron susceptibles de mejora, se relacionan en la matriz presentada en el capítulo I.

Nuestra labor es ejecutada bajo la técnica de muestreo y áreas críticas, que por tal motivo, podría o no detectarse errores materiales o ausencia de controles dado que las revisiones no abordan la totalidad de las operaciones ejecutadas por la entidad evaluada. En consecuencia es la administración y los funcionarios en quien ella delegue, los responsables de velar porque las operaciones ejecutadas se efectúen con las técnicas de calidad profesionalmente admisibles, y que las actividades de control desarrolladas de manera rutinaria al interior de la entidad, sean efectivas, eficaces y concluyentes, de tal manera que se salvaguarden los intereses comunes y corporativos de la entidad, en procura de minimizar errores y de mitigar riesgos, de manera tal, que se proteja el patrimonio del ente económico.

El documento que presentamos se compone de los siguientes aspectos:

Informe Ejecutivo: Se ilustra una matriz de resultados. La misma puede ser utilizada como una "Herramienta" para la elaboración de "Planes de Mejoramiento". Ésta comprende:

- (1) Aspecto evaluado: Tema objeto de auditoría.
- (2) Observación: Hallazgo concreto.

- (3) Recomendación: Acción que se sugiere debería emprender la administración o el dueño del proceso de así considerarlo.
- (4) Disposición: Comentario de la entidad con respecto a la observación encontrada.

Conclusiones generales: Se desarrolla de forma específica al alcance que fue determinado para el trabajo de auditoría.

Para fines de comprensión todos nuestros informes obligatoriamente deben estar sometidos a la respectiva socialización y conocimiento previo por parte de los dueños y líderes de cada proceso, quienes en ejercicio de su derecho de controversia o contradicción, pueden establecer disposiciones sobre nuestras valoraciones u observaciones técnicas; de las cuales se deja evidencia en los informes emitidos. Lo antes expuesto, no significa, que aceptemos o estemos de acuerdo con las mismas, y mucho menos que la inclusión de éstas, en dichos documentos, se conviertan en una medida de retractación o de corrección por parte nuestra.

En cumplimiento de nuestra política institucional, ponemos en consideración de la Alta Administración, el documento aludido para que ésta a su vez lo analice y en caso de estimarlo prudente emita sus conceptos; aclarando que si en el término de tres (3) días hábiles, no hemos recibido respuesta alguna por parte de dicho órgano de Administración; de nuestra parte, entenderemos que las observaciones y demás manifestaciones de la auditoría, son plenamente aceptadas gerencialmente.

Agradecemos la colaboración prestada por los funcionarios de la entidad, por la disposición y colaboración que brindan para con este órgano de control.

Atentamente,

Edwin Arango Montes
Gerente Soluciones TI
NewSol In Consulting SAS

CAPITULO I
HOSPITAL GENERAL DE MEDELLÍN
MATRIZ DE RESULTADOS
DE LA ETAPA DE PRESTACIÓN DEL SERVICIO - EJECUCIÓN DE LA PLANEACIÓN
AUDITORÍA DE SISTEMAS

A continuación presentamos una serie de definiciones para tener en cuenta a lo largo del informe:

- Seguridad de la información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la **información** buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
- ERP: Planeación de los Recursos Empresariales. Esta práctica tiene que ver con el gerenciamiento de los distintos recursos, negocios, aspectos y cuestiones productivas y distributivas de bienes y servicios en una empresa.
- SAP*: Super usuario de SAP, que se utiliza durante la configuración inicial del ERP. Contiene todos los permisos del ERP
- SAP_ALL: perfil que otorga todos los permisos y autorizaciones del ERP SAP para un usuario.
- Objetos de Autorización: Permisos, actividades y restricciones que contienen los usuarios al ser asignados dentro de un rol.
- Tablespace: es una ubicación de almacenamiento donde pueden ser guardados los datos correspondientes a los objetos de una base de datos.
- JOBS: tareas programadas para ejecutar procesos de fondo en SAP
- Transacción: programa que me permite ejecutar una determinada actividad y/o movimiento en el ERP
- Objetos de autorización: conjunto de permisos y actividades que componen una transacción en SAP para realizar una determinada tarea
- Rol: es el medio por el cual se le permite al usuario que acceda a una transacción dentro de SAP con unos permisos determinados
- BASIS: Línea base de configuración de la plataforma y seguridad del ERP SAP
- ABAP: lenguaje de programación nativo de SAP
- Transportes: método usado en SAP para el paso de cambios en los programas en cada uno de los ambientes existentes, es decir, desarrollo, calidad y productivo.
- Mandantes: instancias creadas dentro de los diferentes ambientes de SAP para realizar actividades especificas

Seguidamente se presenta la matriz que contiene las oportunidades de mejora que surgen del grupo de auditores de NewSol en desarrollo de la auditoría:

<table>
<tr><th>ASPECTO EVALUADO</th><th>OBSERVACIÓN</th></tr>
<tr><td>Seguridad General de SAP</td><td>
Observación No.01: Seguridad de Contraseñas

Durante la revisión de la configuración de los parámetros de contraseñas en SAP se observaron los siguientes parámetros cuyos valores no están acordes con las buenas prácticas de seguridad de contraseñas:

<table>
<tr><th>Parámetro</th><th>Descripción</th><th>Valor recomendado</th><th>Valor configurado</th></tr>
<tr><td>login/min_password_lng</td><td>Longitud mínima de la contraseña. Valor adecuado</td><td>8 caracteres</td><td>6</td></tr>
<tr><td>login/min_password_digits</td><td>Número mínimo de caracteres numéricos que deben contener las contraseñas.</td><td>1</td><td>0</td></tr>
<tr><td>login/min_password_letters</td><td>Número mínimo de letras de deben contener las contraseñas</td><td>1</td><td>0</td></tr>
<tr><td>login/min_password_specials</td><td>Número de caracteres especiales que debe incluir una contraseña.</td><td>1</td><td>0</td></tr>
</table>

El no contar con parámetros de seguridad de contraseñas robustos podría exponer la seguridad de los recursos tecnológicos a través del uso de contraseñas de acceso que podrían ser vulneradas.

Recomendación:

Configurar los parámetros de seguridad de contraseñas en SAP de acuerdo con las buenas prácticas de seguridad y actualizar y socializar el documento que contiene la política de seguridad de contraseñas definida por el HGM.

Esto con el fin de mejorar la seguridad y protección de accesos en el ERP que cubre los procesos de negocio misionales y de apoyo en el HGM.
</td></tr>
</table>

<table>
<tr><th>ASPECTO EVALUADO</th><th>OBSERVACIÓN</th></tr>
<tr><td></td><td>
Disposición, Líder de TI:

De acuerdo con la recomendación
</td></tr>
<tr><td></td><td>
Observación No.02: Usuarios por defecto de SAP

Durante la revisión del reporte RSUSR003 se observaron los siguientes usuarios por defecto creados, cuyas contraseñas no han sido cambiadas desde su instalación:
<table>
<tr><th>Mandante</th><th>Usuario</th><th>Contraseña por defecto</th><th>Cuenta bloqueada?</th></tr>
<tr><td>001
066</td><td>SAPCPIC</td><td>Si</td><td>No</td></tr>
<tr><td rowspan="2">066</td><td>EARLYWATCH</td><td>Si</td><td>No</td></tr>
<tr><td>SAP*</td><td>Si</td><td>No</td></tr>
<tr><td rowspan="4">300</td><td>SAPCPIC</td><td>Si</td><td>No</td></tr>
<tr><td>TMSADM</td><td>Si</td><td>No</td></tr>
<tr><td>DDIC</td><td>Si</td><td>No</td></tr>
<tr><td>SAP*</td><td>Si</td><td>Si</td></tr>
</table>
El tener usuarios genéricos y con contraseñas por defecto en los mandantes de SAP, podría resultar en accesos no autorizados.
</td></tr>
<tr><td></td><td>
Recomendaciones:

Modificar las contraseñas por defecto de los usuarios en los mandantes 001, 066 y 300 y realizar su respectivo bloqueo, con el fin de evitar accesos no autorizados a través de estos usuarios que contienen permisos privilegiados.

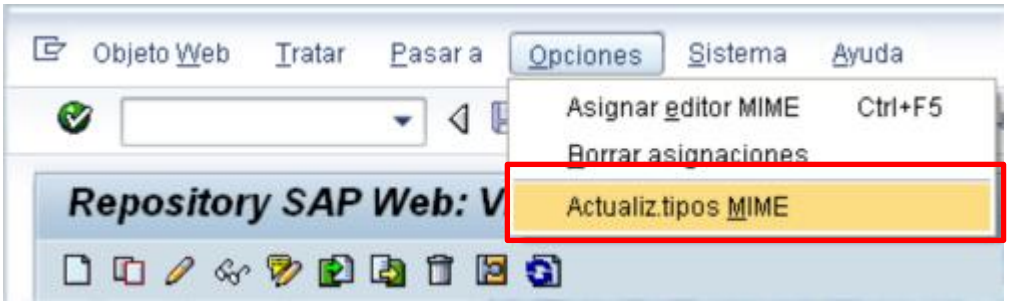
Adicionalmente, en el caso del usuario SAP*, este debe ser bloqueado en todos los mandantes, tanto calidad como productivo, debido a su criticidad y complejidad en el sistema.
</td></tr>
<tr><td></td><td>
Disposición, Líder de TI:

De acuerdo con la recomendación
</td></tr>
<tr><td></td><td>
Observación No.03: Seguridad del mandante de producción

Durante la revisión a la seguridad del mandante de producción se observaron las siguientes situaciones:

• A través de la transacción SCC4, observamos que el nivel de protección del mandante se encuentra configurado con valor 0, es decir que no tiene
</td></tr>
</table>

ASPECTO EVALUADO	OBSERVACIÓN
	limitaciones, lo cual posibilita que se puedan realizar cambios directamente en el ambiente productivo de forma no autorizada. • El área de Sistemas ha realizado 14 aperturas del mandante durante el 2018 relacionadas con la publicación de campañas de seguridad para los usuarios. • En el procedimiento de gestión de cuentas de usuario de SAP, se establece que para realizar la apertura del mandante se debe realizar la solicitud al analista encargado de administración de usuarios quien le asignará el rol respectivo para ejecutar esta actividad. Sin embargo, en este procedimiento no se incluye: o Descripción de las situaciones por las cuales se amerita la apertura del mandante o Personal autorizado para realizar la solicitud de apertura del mandante. o Personal autorizado para otorgar la apertura del mandante. o Ventanas de tiempo para la apertura del mandante. • No se evidencia un procedimiento para el monitoreo de las aperturas de mandante que permitan verificar que éstas se han realizado de forma autorizado y para los fines requeridos. El no contar con una seguridad adecuada del ambiente de producción, realizar aperturas constantes del mismo y no contar con un procedimiento formal para controlar la apertura del mismo, aumentan la posibilidad de que se omitan los controles establecidos lo que podría resultar en cambios no autorizados en el ambiente de producción que impacten el correcto funcionamiento del mismo y la integridad de la información.
	Recomendaciones: • Establecer el nivel de protección del mandante en valor 1 (No se puede sobrescribir) o nivel 2 (No se puede sobrescribir, sin disponibilidad externa). • Evaluar la posibilidad de no generar aperturas del mandante para la publicación de campañas de seguridad liberadas por el área de Sistemas y en su reemplazo validar otras alternativas que cumplan con el mismo propósito, por ejemplo utilizar la transacción SMW0 para publicar estas campañas sin necesidad de abrir el mandante como se ilustra a continuación: Se accede a la transacción SMW0 y se selecciona la opción para datos binarios:

ASPECTO EVALUADO	OBSERVACIÓN
	 Para verificar los tipos de imágenes soportados se accede al menú Opciones -> Actualizar tipos MIME:  Aquí se muestran las extensiones de ficheros permitidas. Si no existe la extensión deseada se puede añadir eligiendo “Asignar editor MIME” en el menú “Opciones” de la pantalla anterior:

ASPECTO EVALUADO	OBSERVACIÓN
	 • Documentar y formalizar un procedimiento para la apertura del mandante productivo, que incluya entre otros, los siguientes aspectos: o Definición de situaciones que ameritan la apertura del mandante. o Justificación de la apertura. o Responsables. o Autorización formal antes del evento de apertura. o Límites de tiempo en que debe permanecer el mandante abierto. o Actividades de monitoreo durante los eventos de apertura del mandante. o Definición de los soportes documentales del proceso. • Realizar revisiones periódicas a la configuración del mandante y a los logs de apertura que permitan identificar de forma oportuna posibles cambios en su configuración y/o modificaciones sobre el mandante que no hayan surtido el procedimiento establecido. Esta revisión deberá quedar documentada.
	Disposición, Líder de TI: De acuerdo con la recomendación
Acceso a transacciones críticas	**Observación No.04: Usuario ANALISTA** Durante la revisión de accesos, se observaron las siguientes situaciones relacionadas con el usuario ANALISTA para el cual según lo descrito en el instructivo AP-INF-TI003I04 – Instructivo de Gestión de usuarios, este usuario es de consulta y no debería tener permisos para crear, modificar y/o eliminar en el ambiente productivo: • Tiene asignado el perfil SAP_ALL, el cual le otorga altos privilegios en el sistema SAP.

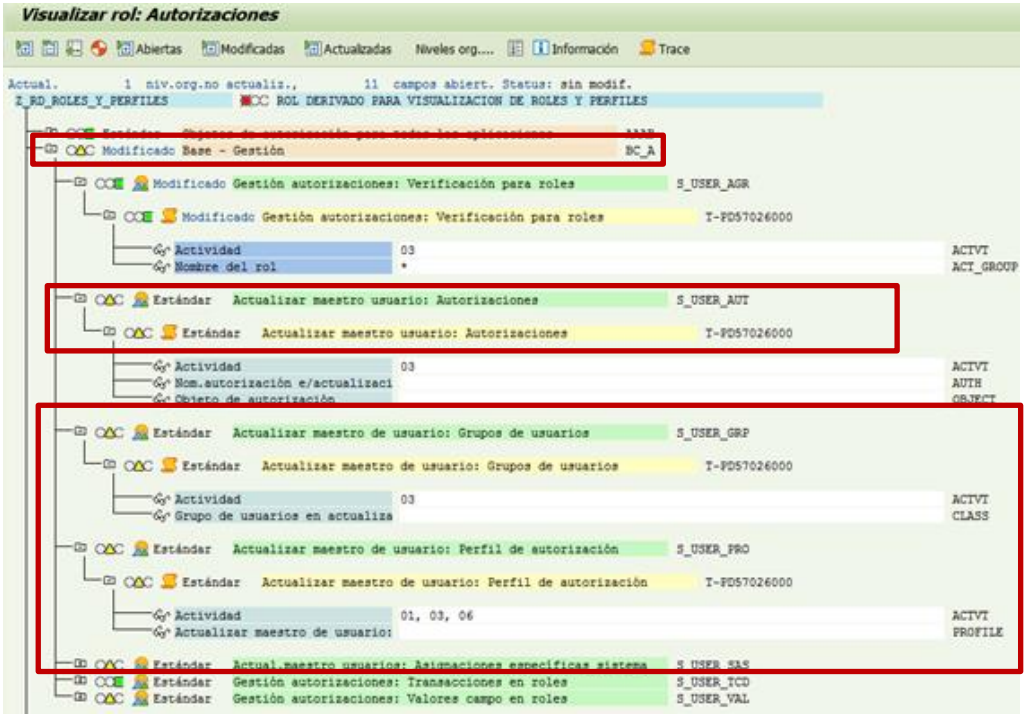
ASPECTO EVALUADO	OBSERVACIÓN
	• Acceso a la transacción STMS (utilizada para realizar transportes al ambiente de producción de SAP) y el objeto de autorización S_TRANSPRT con las actividades 01 - crear, 02 – Modificar, 06 – eliminar, 50 – Mover, 64 – generar y 43 – liberar. • Es de uso compartido de los líderes de los módulos para dar soporte a los usuarios finales de la aplicación y adicionalmente para administrar cuentas de usuario por parte de Maribel Cardona – Analista, como backup de la responsable de ejecutar esta actividad. El uso de un usuario genérico y compartido, y que adicionalmente tengan accesos privilegiados en la aplicación SAP, posibilita la ejecución de actividades que no corresponden con las funciones del personal que usa dicho usuario y la dificultad de identificar el responsable que ejecutó cierta actividad en el sistema SAP.
	Recomendaciones: • Restringir el perfil SAP_ALL eliminándolo del usuario ANALISTA y asignar una cuenta de usuario para cada uno de los líderes de los módulos (Analistas) que tenga únicamente acceso a aquellas transacciones para realizar soporte a usuarios finales. Si bien la asignación del perfil SAP_ALL estaba siendo monitoreada semanalmente por la responsable de la administración de usuarios, ésta no volvió a ejecutarse. Por lo cual se recomienda retomar esta actividad en aras de identificar posibles usuarios con este este perfil de forma no autorizada y ejecutar las respectivas acciones sobre los mismos. • Diseñar y desarrollar un rol que contenga las transacciones necesarias para consultar y visualizar informes, datos, reportes y otros relacionados con las funciones de cada uno de los analistas. • Asignar al usuario de Maribel Cardona adicional a los roles de soporte, los roles para la administración de usuarios, sólo por tiempos limitados en caso que la responsable de dicha actividad no pueda ejercer estas funciones y retirarlos una vez se haya cumplido la actividad. • Establecer un procedimiento para asignar usuarios temporales en el ambiente productivo para realizar actividades puntuales que requieran de la intervención de uno de los analistas. Esta asignación debe ser por tiempo limitado y bajo monitoreo Basis.

ASPECTO EVALUADO	OBSERVACIÓN
	Disposición, Líder de TI: De acuerdo con la recomendación
Gestión de cambios a programas	**Observación No. 05: Procedimiento para la gestión de cambios** Si bien el HGM tiene definido un procedimiento para la gestión de cambios en los sistemas de información incluyendo SAP, conocimos que este procedimiento presenta las siguientes situaciones susceptibles de mejora: • No todas las solicitudes ingresan por mesa de ayuda, es decir se hacen de forma verbal, directamente con el analista encargado. • No se aplica de manera consistente el procedimiento para catalogar y tipificar loas diferentes solicitudes de cambio que ingresan a la mesa de ayuda. • Aunque se cuenta con una herramienta para mesa de ayuda "ITOP", de licenciamiento libre, no se está utilizando adecuadamente para gestionar la etapas del proceso de gestión de cambios. • No se almacenan las evidencias que soportan la ejecución del procedimiento de cambios establecido (p.e. solicitud de cambio, confirmación de pruebas de usuario, aceptación y paso a producción, entre otros). La no aplicación constante del procedimiento de cambios en la aplicación SAP podría conllevar a que se soliciten, autoricen, prueben y se ejecuten cambios en el ambiente productivo sin la debida autorización de parte de las áreas usuarias.
	Recomendaciones: • Aplicar de forma consistente el procedimiento de gestión de cambios que permita catalogar las diferentes solicitudes de cambio y de esta forma proceder a su evolución de acuerdo con el procedimiento establecido. • Optimizar el uso de la herramienta de la mesa de ayuda para realizar todo lo referente a la gestión y administración de cambios, ya sea para aplicaciones SAP y no SAP, infraestructura, gestión de usuarios y roles, entre otros. • Almacenar la documentación soporte de cada una de las fases respectivas para cada tipo de cambio en la herramienta de Mesa de Ayuda. • Para el caso del ERP SAP, se recomienda configurar y parametrizar SOLDOC desde SOLMAN para la documentación de cada uno de los casos y soportes requeridos.

ASPECTO EVALUADO	OBSERVACIÓN
	Disposición, Líder de TI:
Gestión de cuentas de usuario	**Observación No. 06: Especificación de permisos para las cuentas de usuario en SAP** En el procedimiento ejecutado por el HGM para otorgar acceso a la aplicación SAP se presentan solicitudes de creación de cuentas de usuario sobre todo para el caso de los reemplazos, en los que se hace referencia a otros usuarios existentes, sin que se especifiquen los permisos particulares para las nuevas cuentas. Si bien la responsable de administrar los usuarios en SAP definió para algunos cargos los roles a asignar con base en los roles y cargos de otros usuarios, los cuales asigna al momento de la creación de nuevas cuentas de usuario, no existe una matriz de roles versus cargos formal que incluya las transacciones (roles y/o perfiles) que deben ser asignadas a un usuario según el cargo o función que desempeñe en el HGM. Dado que los permisos de un usuario pueden variar en el tiempo, el permitir que las solicitudes de acceso se creen con base en permisos de una cuenta existente, posibilita la asignación de accesos más allá de los requeridos según sus funciones, o la asignación de permisos que puedan generar conflictos en las funciones que realizarán los usuarios, habilitándolos para realizar actividades que podrían no estar autorizadas.
	Recomendaciones: • Definir y formalizar una matriz en conjunto con las áreas usuarias que consolide los roles clave de la aplicación SAP versus los diferentes cargos del HGM que pueda ser utilizada tanto en la solicitud de creación de cuentas de usuario por parte del personal que solicita y autoriza la creación como por el responsable de la administración de cuentas de usuario para asignar los roles apropiados para el cargo y/o funciones de los usuarios. • Documentar un procedimiento de revisión y actualización periódica de esta matriz, para verificar su validez en el tiempo frente a los cambios y realidad operativa del HGM.
	Disposición, Líder de TI: De acuerdo con la recomendación

ASPECTO EVALUADO	OBSERVACIÓN
	Observación No. 07: Notificación de Personal retirado externo Si bien el HGM tiene establecido en el Instructivo de Gestión de cuentas de usuario que los retiros de personal externo deben ser reportados por el Jefe de área a través de un ticket para que se proceda con el bloqueo de las cuentas de usuario por parte del responsable, conocimos que esta actividad no se realiza de forma y por tanto, las cuentas de estos usuarios no se bloquean de forma oportuna sino al momento en que la responsable de la administración de usuarios de SAP, realiza la validación de personal que no accede a SAP por más de 45 días. Esta situación posibilita el acceso no autorizado al sistema SAP a través del uso de cuentas de usuario de personal retirado.
	Recomendaciones: • Definir a nivel del HGM un área o persona encargada de la gestión de personal externo y concientizarla de la importancia de retirar los permisos de las cuentas de usuario del personal externo. • De otra parte, una vez se haya establecido esta área/persona se deberá alinear con el procedimiento actual para la administración de cuentas de usuario en los diferentes sistemas de la información.
	Disposición, Líder de TI: De acuerdo con la recomendación
	Observación No.08: Validación periódica de cuentas de usuario Se conoció que la responsable de la administración de usuarios en SAP realiza una verificación semanal a los usuarios que no han accedido al sistema SAP durante los últimos 45 días y envía el listado de los usuarios identificados al área de Gestión Humana vía correo electrónico quien los valida e indica si están en vacaciones, retirados, en licencia, o son “No vinculados” (no hacen parte de la nómina del HGM) para realizar el respectivo bloqueo de las cuentas de usuario. Sin embargo, de esta actividad no se almacena la documentación que resulta de la ejecución de la misma por parte de la responsable de administración de usuarios en SAP. El no contar con la documentación que soporta la ejecución de esta actividad de control debilita el ambiente de control establecido por el HGM, lo cual conlleva a la aplicación de controles sin documentación y a criterio de las personas que ejecutan estas actividades de control.

ASPECTO EVALUADO	OBSERVACIÓN
	Recomendación: Almacenar la documentación que soporte la verificación de los usuarios que no han accedido al sistema SAP por más de 45 días, los correos enviados y recibidos al área de Gestión Humana y documentar las acciones ejecutadas para cada uno de los usuarios identificados.
	Disposición, Líder de TI: De acuerdo con la recomendación
	Observación No.09: Matriz de Segregación de funciones Se conoció que el área de Sistemas ha venido adelantando en conjunto con las áreas usuarias la definición de matrices de segregación de funciones para cada uno de los módulos de SAP. Sin embargo, a la fecha solo se han entregado y formalizado las matrices de los módulos de MM, FI-AR, FI-TR, FI-CO y BI. Falta la definición, entrega y formalización de las matrices de segregación de funciones para los módulos de: • ISH-PA • ISH-PM • ISH-MED • MM • SD • FI-GL • FI-PSM • HCM La no definición y formalización con las áreas usuarias de matrices de segregación de funciones en un ambiente SAP posibilita la creación y asignación de roles que contengan transacciones que presenten conflicto y por tanto se otorguen accesos no autorizados al sistema SAP.
	Recomendación: Establecer una fecha final de entrega y finalización de la definición de las matrices de segregación de funciones para cada uno de los procesos de negocio del HGM, dado que esta actividad lleva más de un año en implementación, y por tanto afecta el Gobierno, Riesgo y Control en lo correspondiente a control de accesos y gestión de riesgos en el ERP.
	Disposición, Líder de TI: De acuerdo con la recomendación

ASPECTO EVALUADO	OBSERVACIÓN
Perfilamiento en SAP	**Observación No. 10: Perfiles e instancias descompensadas** Realizando nuestra validación de perfiles y objetos de autorización, hemos encontrado que existen casos en los cuales los objetos de autorización no están ajustados tal como se muestra a continuación:  El no ajustar y compensar roles, perfiles y objetos de autorización genera desorganización en el modelo actual de roles y perfiles, sumando objetos de autorización y valores que no se utilizarán, pero que el sistema valida al momento de ejecutar una transacción, generando demoras en la ejecución de programas y transacciones al tener que validar objetos que no son requeridos ni aplicados.
	Recomendación: Organizar y depurar todos los roles, perfiles y objetos de autorización que se encuentran vacíos, o con valores no permitidos, como asteriscos o “todas las actividades”. Dado que esta actividad requiere de conocimiento y tiempo, se sugiere evaluar la posibilidad de contar con una asesoría y acompañamiento durante dicha actividad.

ASPECTO EVALUADO	OBSERVACIÓN
Tareas Programadas en SAP	**Observación No. 11: Depuración de Jobs en SAP** Se observó que existen más de 1500 jobs programados en el sistema SAP los cuales no todos son de conocimiento del área de Sistemas y tampoco se cuenta con una documentación formal (ficha técnica) sobre su funcionamiento. El área de Sistemas tiene como proyecto iniciar la depuración de dichos Jobs en conjunto con el proveedor de Consultoría UTAVANZA. Esta situación posibilita la ejecución de Jobs innecesarios para el buen funcionamiento de los procesos de negocio del HGM que por el contrario podrían consumir recursos del sistema y/o deterioro del mismo.
	Recomendación: Realizar la depuración de los Jobs configurados en SAP y en conjunto con las áreas de negocio determinar cuáles son requeridos para el desarrollo eficiente de sus procesos, documentando una ficha técnica para cada Job, que contenga la descripción, tiempos de ejecución, dueños y/o responsables, tiempo de vigencia, entre otros.
	Disposición, Líder de TI: De acuerdo con la recomendación

ASPECTO EVALUADO	OBSERVACIÓN
Seguridad física y ambiental Datacenter	**Observación No. 12: Seguridad física y ambiental del datacenter de TIGO UNE** Si bien el dataceter de TIGO UNE en el cual se encuentran los servidores de aplicación y de base de datos de SAP está certificado en Nivel 4, durante la visita efectuada observamos las siguientes situaciones: • Algunas de las puertas dan a los corredores del edificio donde hay oficinas de EPM, a las cuales únicamente se accede con tarjeta de proximidad y no se cuenta con otro sistema de acceso complementario como sistemas biométricos, aun cuando al interior del datacenter existen algunas puertas que se acceden con tarjeta de acceso y sistema biométrico. • Material inflamable como espuma, tela, tubos, cajas, entre otros, que hacen parte de una remodelación que se viene adelantando y el cual no debería almacenarse al interior del datacenter. Estas situaciones posibilitan: • Posibles accesos no autorizados al datacenter por personal diferente al personal autorizado de TIGO UNE. • El almacenamiento de material inflamable en el datacenter podrían facilitar la expansión del fuego en el mismo, en el evento que se presente un incendio.
	Recomendación: Retirar del centro de cómputo el material inflamable identificado o elementos que no requieran estar ubicados en esta locación.
	Disposición, Líder de TI: De acuerdo con la recomendación

CAPITULO II
HOSPITAL GENERAL DE MEDELLÍN
CONCLUSIONES DEL TRABAJO REALIZADO
DE LA ETAPA DE PRESTACIÓN DEL SERVICIO - EJECUCIÓN DE LA PLANEACIÓN
AUDITORÍA DE SISTEMAS

Conclusiones:

Con base la evaluación de controles generales de TI efectuada para el sistema SAP, se observa que si bien existen oportunidades de mejora, los controles diseñados e implementados por el HGM están siendo aplicados en su mayoría de forma consistente.

Fortalezas:

El HGM cuenta con una estructura de gobierno de TI en relación a políticas, procedimientos, instructivos y manuales que le permiten establecer e implementar controles para mitigar los riesgos a los cuales están expuestos en relación con la gestión de usuarios en las sistemas de información, gestión de cambios a programas, gestión de operaciones de cómputo.

En relación con los procesos evaluados durante la auditoría resaltamos:

- Proceso de administración de usuarios:

  Toda creación y/o modificación de cuentas de usuario se encuentra autorizada y las cuentas de usuario evaluadas cuentan con los permisos requeridos para el ejercicio de sus funciones.

  Se observa que el HGM ha invertido tiempo y recursos en continuar con el fortalecimiento de la seguridad de SAP, definiendo e implementando matrices de segregación de funciones que le permiten a la responsable de la administración de usuarios, asignar de forma adecuada los permisos en el sistema.

- Proceso de Gestión de cambios:

  En general todos los cambios en funcionalidad y/o configuración en el sistema SAP son evaluados y aprobados por el Comité de cambios para su respectivo desarrollo/evolución y por tanto todo transporte resultado de dichos cambios efectuado en el ambiente de producción se encuentra autorizado por parte del personal encargado.

- Proceso de Operaciones de Cómputo:

  Existen procedimientos y planes para la ejecución de backups de la información clave en los sistemas de información y se cuenta con una planeación de la ejecución de los mismos.

Debilidades:

Se identifican como oportunidades de mejora las descritas en este informe. Toda vez que las recomendaciones dadas como resultado de esta evaluación general de controles de TI sobre SAP sean evaluadas e implementadas por el HGM, se optimizará el ambiente de control para SAP.