

HOJA DE RUTA			
Empresa:	HOSPITAL GENERAL DE MEDELLÍN		
Tipo de Relación:	Auditoría de Sistemas de Información		
Etapas de la prestación del servicio:	Ejecución		
Informe de:	Auditoría de los procesos de TI basados en ISO 27001 y Estado actual en relación con MIPG.		
Fecha de Corte:	Noviembre de 2018		
Estado del informe:	Socializado	Borrador	Definitivo

INFORMACIÓN GENERAL DEL CLIENTE			
NATURALEZA JURÍDICA:	Entidad del Estado	NORMAS APLICADAS A LA AUDITORÍA REALIZADA	
		<ul style="list-style-type: none">• ISO 27001• MIPG	
DIRECCIÓN SEDE:	Carrera 48 No.32 - 102		
DEPARTAMENTO:	Antioquia	MUNICIPIO	Medellín
CONMUTADOR:	3847300	FAX:	232 0227

Medellín, 26 de Noviembre de 2018

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

Asunto: Informe de la auditoría a los procesos de TI basados en la Norma Internacional ISO 27001 y estado actual del área de Sistemas en relación con el Modelo Integrado de Planeación y Gestión (MIPG).

Respetado Doctor Bustamante,

En cumplimiento del escrito contractual suscrito entre las partes, ponemos a su consideración el resultado obtenido de la segunda fase de la **AUDITORIA DE SISTEMAS** realizada al área de Sistemas del Hospital General de Medellín (en adelante HGM), la cual se programó para ejecutar a partir del 7 de noviembre de 2018.

Nuestra revisión contempló los siguientes aspectos:

1. Evaluación de los procesos del área de Sistemas tomando como referencia la Norma ISO 27001, y que cubrió los siguientes dominios de control:
 - ✓ Política de seguridad de la información
 - ✓ Organización de la seguridad de la información
 - ✓ Gestión de activos
 - ✓ Seguridad de los recursos humanos
 - ✓ Seguridad física y del entorno
 - ✓ Gestión de comunicaciones y operaciones
 - ✓ Control de acceso
 - ✓ Adquisición, desarrollo y mantenimiento de sistemas de información
 - ✓ Gestión de los incidentes de la seguridad de la información
 - ✓ Gestión de la continuidad del negocio
 - ✓ Cumplimiento y normatividad
2. Seguimiento al estado de implementación de MIPG, para los siguientes componentes:
 - ✓ Estrategia de TI
 - ✓ Gobierno de TI
 - ✓ Información
 - ✓ Sistemas de información
 - ✓ Servicios tecnológicos
 - ✓ Uso y apropiación
 - ✓ Capacidades Institucionales

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 que 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 con el consolidado de todas las observaciones identificadas a lo largo de nuestro proceso de auditoría. 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.

Informe General: Se desarrolla de forma específica los resultados obtenidos en la evaluación de los objetivos de control a nivel de la norma ISO27001, el cual se observa en el Capítulo II.

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 emitir 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,

A handwritten signature in black ink, appearing to read "Edwin Arango Montes".

EDWIN ARANGO MONTES
GERENTE SOLUCIONES TI

En Representación de **NEWSOL CONSULTING S.A.S.**

<p style="text-align: center;">CAPÍTULO I INFORME EJECUTIVO MATRIZ DE RESULTADOS AUDITORÍA DE LOS PROCESOS DE TI CON BASE EN LA NORMA ISO27001 – ESTADO ACTUAL EN RELACIÓN CON MIPG CON CORTE A NOVIEMBRE DE 2018</p>

A continuación, enmarcamos las definiciones de conceptos que se aplican dentro del área de sistemas y tecnología del Hospital General de Medellín, esto con el fin de tener claridad de la terminología utilizada durante el desarrollo 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.
- **LOG:** registros y/o reportes de las transacciones y movimientos realizados en un aplicativo por usuarios determinados
- **Sistema de Información:** conjunto de datos que ayudan administrar, recolectar, procesar, almacenar y entregar información de manera automatizada y ordenada.
- **Segregación de funciones:** método utilizado para separar las responsabilidades de las diversas actividades que intervienen en la elaboración de los estados financieros, incluyendo la autorización y registro de transacciones, así como mantener la custodia de activos y sus sistemas de información.
- **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.
- **MIPG:** Modelo Integrado de Planeación y Gestión es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas con el fin de generar resultados que atiendan a los planes de desarrollo y que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en los servicios.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Disponibilidad:** propiedad de la información de ser accesible y utilizable por solicitud de una entidad autorizada.
- **Seguridad Informática:** hace referencia a la protección de la integridad y privacidad de la información almacenada en un sistema informático.
- **ISO27001:** Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.
- **Incidentes:** cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio.
- **Problemas:** causa desconocida de uno o más incidentes, o sea, un incidente que no tiene su causa raíz identificada acaba transformándose un problema.

Seguidamente se presenta la matriz que contiene las oportunidades de mejora que resultan de la auditoría efectuada a los procesos del área de sistemas del Hospital General de Medellín en lo que

respecta a la Norma ISO 27001 y el estado de avance en la implementación de los requerimientos de TI exigidos por MIPG:

I. AUDITORÍA DE LOS PROCESOS DE TI BAJO LA NORMA ISO 27001

ASPECTO EVALUADO	OBSERVACIÓN
Organización de la seguridad de la información	<p>Observación No.01: Revisión sobre el modelo de Seguridad de la Información</p> <p>Si bien el HGM, cuenta con un modelo de seguridad de la información conformado por políticas, instructivos, procedimientos, manuales, entre otros y desde su implementación ha generado un esfuerzo en su implementación y mejoramiento, se observaron las siguientes situaciones susceptibles de mejora:</p> <p>a. No se observó un plan de revisión a este modelo que le permita al HGM contar con la documentación actualizada y formalizada de acuerdo con los cambios y la realidad del mismo. Como resultado de lo anterior, se observa que existen documentos que no han sido revisados desde el momento de su elaboración, como, por ejemplo:</p> <ul style="list-style-type: none"> • La política de seguridad de la información versión 00, liberada en el 2014. • El manual de seguridad de la Información, versión 02 y su última revisión fue realizada en el año 2016. • Instructivo de Acceso a la red, Instructivo de Acceso VPN, Instructivo de proveedores, entre otros se encuentran en la versión 00. <p>b. En el Manual de Seguridad de la Información, se observa la definición de los siguientes roles como parte del Gobierno de Seguridad de la Información que a la fecha no han sido implementados por el HGM y que están siendo asumidos por el Líder de Sistemas, generando una inadecuada segregación de funciones:</p> <ul style="list-style-type: none"> • Comité de gobierno en Línea • Oficial de la Seguridad de la Información (CISO) • Administrador de la seguridad de la información (ISM)
	<p>Recomendación:</p> <p>Teniendo en cuenta la información evidenciada y los esfuerzos del área de sistemas por mejorar y alinear su modelo de seguridad de la información a la Norma ISO 27001, es necesario realizar lo siguiente:</p> <ul style="list-style-type: none"> • Establecer revisiones periódicas al modelo de seguridad de la información al menos dos veces al año, con el fin de identificar posibles cambios ya sea a nivel de la entidad o por temas regulatorios que deban ser incluidos en este modelo. Dichas revisiones, deberán quedar documentadas como control de cambios en los documentos relacionados. • Evaluar la posibilidad de implementar los roles definidos en el Manual de Seguridad de la información de forma tal que se cuente con un adecuado Gobierno de

	<p>seguridad de la información que esté alineado a las buenas prácticas sugeridas por la Norma ISO 27001 manteniendo así la segregación de funciones relacionadas con la gestión de la seguridad de la información.</p> <p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
<p>Gestión de activos de la información</p>	<p>Observación No.02: Actualización de inventario de activos de la información</p> <p>Si bien el HGM cuenta con un inventario de los activos de la información que incluye infraestructura e información tanto física como digital y el cual está bajo la responsabilidad del área de Gestión Documental, éste no se encuentra actualizado. Se conoció que se está iniciando un proceso de actualización de este inventario y se espera finalizar en el 2019.</p> <p>El no contar con un inventario de activos actualizado, posibilita la existencia de activos de la información que no se hayan identificado, clasificado, valorado y por tanto no estén siendo utilizados de forma segura y de acuerdo con el procedimiento de Clasificación de la información establecido por el HGM.</p>
	<p>Recomendación:</p> <p>Establecer un cronograma de revisión del inventario de activos de la información que pueda cumplirse en el menor tiempo posible por parte del área de Gestión Documental y de los dueños de las áreas de negocio.</p> <p>Así mismo, se deberán establecer revisiones periódicas a estos activos de información de forma tal que se minimice el riesgo de uso no autorizado de los mismos por parte del personal interno y/o externo del HGM.</p>
	<p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
<p>Seguridad física y del Entorno</p>	<p>Observación No.03: Controles de acceso y ambientales en los centros de cómputo</p> <p>El HGM tiene definidos controles para la seguridad de acceso a los centros de cómputo ubicados dentro del hospital como planilla de acceso para personal externo, uso de tarjeta de proximidad y llaves de las puertas de acceso y controles ambientales como extintores, sistemas de humedad y temperatura, entre otros.</p> <p>Sin embargo, durante la visita a los centros de cómputo, se observaron las siguientes situaciones que presentan oportunidad de mejora:</p> <ul style="list-style-type: none"> • EL extintor SOLKAFLAM ubicado en el centro de cómputo del piso 3 no ha sido recargado en la fecha estipulada (Abril de 2018), lo cual posibilita que en caso de un incendio se pueda evitar la propagación del mismo y por tanto la

	<p>pérdida o daño de los activos de información ubicados al interior de los centros de cómputo.</p> <ul style="list-style-type: none"> • Si bien el acceso a los centros de cómputo se realiza con llaves y tarjeta de proximidad, el sistema de acceso a través de tarjeta de proximidad no funciona para el centro de cómputo del piso 3, quedando expuesto a posibles accesos no autorizados al mismo. <p>A nivel de los controles de acceso en el datacenter de TIGO UNE, durante la visita efectuada se observaron las siguientes situaciones:</p> <ul style="list-style-type: none"> • 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, aún 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. <p>Recomendaciones:</p> <p><u>Centros de cómputo del HGM:</u></p> <ul style="list-style-type: none"> • Realizar la recarga del extintor SOLKAFLAM del centro de cómputo del piso 3 y asegurarse de establecer la recarga anual de los extintores de los centros de cómputo como parte del mantenimiento preventivo realizado por el HGM a los dispositivos de control ambiental. • Revisar el sistema de acceso que controla las tarjetas de proximidad del centro de cómputo ubicado en el piso 3. <p><u>Datacenter TIGO UNE:</u></p> <ul style="list-style-type: none"> • Establecer mecanismos adicionales de acceso a las puertas de acceso al datacenter que son comunes a las áreas del edificio (p.e. sistemas biométricos). • Retirar del centro de cómputo el material inflamable identificado o elementos que no requieran estar ubicados en esta locación. <p><i>Disposición, Julián Gómez – Líder de Sistemas del HGM:</i></p> <p>De acuerdo con la recomendación</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Control de acceso	<p>Observación No.04: Validación periódica de cuentas de usuario</p> <p>Si bien el acceso a los sistemas de información del HGM (SAP, CARESTREAM, WINLAB, entre otros) se realiza a través del uso de cuentas de usuario y contraseña y que las actividades que se ejecutan en los mismos se realizan a través de la asignación de permisos. Se conoció que no se realizan validaciones periódicas de los permisos de los usuarios en los sistemas de información.</p> <p>Lo anterior, posibilita el acceso no autorizado de los usuarios a opciones de los sistemas de información para las cuales no requieran de dicho acceso para el ejercicio de sus funciones y por tanto resulte en la pérdida de la integridad y/o confidencialidad de la información.</p>
	<p>Recomendación:</p> <p>Establecer por parte del área de Sistemas en conjunto con las áreas usuarias del HGM revisiones periódicas sobre los usuarios y sus permisos en los sistemas de información con el fin de identificar posibles permisos que no sean requeridos para el cargo o funciones que realicen los usuarios en los sistemas de información.</p>
	<p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
	<p>Observación No.05: Notificación de retiro de personal externo en los sistemas de información</p> <p>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 en la Mesa de Ayuda para que se proceda con el bloqueo de las cuentas de usuario por parte del responsable de administrar los usuarios en los sistemas de información, conocimos que esta actividad no se realiza en todos los casos y por tanto, las cuentas de estos usuarios no se bloquean de forma oportuna.</p> <p>Esta situación posibilita el acceso no autorizado a los sistemas de información a través del uso de cuentas de usuario de personal retirado.</p>
	<p>Recomendaciones:</p> <ul style="list-style-type: none"> Definir a nivel del HGM un área o persona encargada de la gestión de personal externo y concientizarla de la importancia de notificar de forma oportuna el retiro de estos funcionarios para que se proceda con el bloqueo de sus cuentas de usuario y la eliminación de sus permisos en los sistemas de información por parte de la responsable del área de Sistemas. Adicionalmente, una vez se haya definido esta área/persona se le deberá hacer responsable por el cumplimiento de las políticas y procedimientos definidos para la administración de las cuentas de usuario en los diferentes sistemas de información.

	<p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
Control de acceso	<p>Observación No.06: Seguridad de contraseñas</p> <p>Se conoció que el HGM se encuentra en la revisión de las políticas de seguridad de contraseñas de acceso a los servidores y sistemas de información y por tanto a la fecha de la auditoría (4 de octubre de 2018) los parámetros de configuración de contraseñas no están implementados.</p> <p>Lo anterior, podría exponer la seguridad de los recursos tecnológicos a través del uso de contraseñas de acceso que no mantienen una robustez adecuada y que son susceptibles de ser vulneradas.</p>
	<p>Recomendación:</p> <p>Debido a que las contraseñas son el primer paso para la autenticación de los usuarios en los diferentes sistemas de información e Infraestructura, sugerimos que basados en las buenas prácticas de seguridad de contraseñas, el HGM deberá definir e implementar en el menor tiempo posible, los parámetros de seguridad de contraseñas tanto en los servidores como en los sistemas de información.</p> <p>Así mismo, se deberá actualizar el Manual de Seguridad de la Información con la nueva definición de la política de contraseñas.</p>
	<p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
	<p>Observación No.07: Política de escritorio y pantalla despejada</p> <p>Si bien el HGM en relación con las prácticas de escritorio y pantalla despejados, tiene estipulado:</p> <ul style="list-style-type: none"> • Toda la información que resulte de las actividades/funciones de los empleados deberá ser almacenada en carpetas de red a las cuales solo acceden los funcionarios que sean autorizados y que aquella que no esté almacenada en dichas carpetas no hará parte del proceso de respaldo. • Bloqueo de pantalla del escritorio del computador se activa cada 5 minutos, bloqueando la sesión de usuario. <p>Se observa y se conoce que los funcionarios almacenan información personal en sus computadores, y en general se observa que los documentos son almacenados en el escritorio de su computador para un fácil acceso.</p> <p>De otra parte, se evidencian documentos en físico en los puestos de trabajo que podrían ser confidenciales y/o reservados y por tanto están expuestos a</p>

	<p>daños/pérdidas de la información contenida en éstos. Esto sumado a que el acceso a las áreas del HGM no están restringidas y se puede transitar de forma libre por las mismas.</p> <p>La ausencia de políticas y procedimientos sobre buenas prácticas sobre escritorio y pantalla despejada, podría dar lugar a la pérdida/daño de la integridad, confidencialidad y disponibilidad de la información.</p> <p>Recomendación:</p> <p>Definir e implementar una política de escritorio y pantalla despejada la cual defina las medidas preventivas con respecto a los escritorios y computadores de los funcionarios tanto internos como externos del HGM, con el fin de proteger la información de la entidad. Esta política no sólo abarca al HGM sino también hace responsables a los funcionarios del mismo los cuales deberán ser concientizados sobre la importancia de la misma y la preservación de la confidencialidad, integridad y disponibilidad de la información.</p> <p>Una vez definida la política, se deberá integrar al Modelo de Seguridad de la Información definido. Así mismo, se deberán hacer campañas de parte del HGM en las cuales se realice el monitoreo al cumplimiento de la política y aplicar medidas para aquellos que la incumplan.</p> <p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p>
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Gestión de Comunicaciones y Operaciones</p>	<p>Observación No. 08: Uso de medios Removibles</p> <p>En el Manual de Seguridad de la Información, numeral 9.8.9, se establece que el uso de medios removibles está restringido sólo a personal autorizado. Sin embargo, a la fecha esta política no se cumple dado que en el HGM todos los funcionarios pueden utilizar USBs, Discos externos, celulares, entre otros.</p> <p>Si bien una vez se conectan estos medios removibles a los equipos del HGM y éstos se escanean para identificar código malicioso, no existen controles sobre el uso de dichos medios y la información que se copia o extrae hacia/desde los mismos.</p> <p>La ausencia de controles sobre el uso de medios removibles, posibilita que se genere fuga de información del HGM que pudiera ser de carácter confidencial o reservada.</p> <p>Recomendación:</p> <p>Aplicar de forma consistente el Manual de Seguridad de la Información en relación con el uso de medios removibles, definiendo y estableciendo controles para dicho fin (p.e. bloqueo de puertos de almacenamiento externo, implementación herramientas de inscripción de la información, entre otros) que permitan restringir el uso no autorizado de la información y la exposición de la confidencialidad o reserva de esta por parte del personal tanto interno como externo del HGM.</p>

	<div data-bbox="407 273 1445 405"></div> <div data-bbox="407 405 1445 531"> <p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p> </div> <div data-bbox="407 531 1445 867"> <p>Observación No. 09: Restauración de copias de respaldo</p> <p>En el Manual de Seguridad de la Información se establece en el numeral 9.8.8., que el HGM deberá contar con un plan de restauración el cual deberá probarse regularmente. Sin embargo, el HGM no tiene definido un plan de restauración como práctica regular, sino que se hacen restauraciones a demanda.</p> <p>La ausencia de un procedimiento formal de restauración de copias de respaldo, posibilita que al momento de requerir una información contenida en las copias de respaldo o ante la presencia de un evento que requiera la restauración de la misma, ésta no esté disponible o se haya perdido su integridad.</p> </div> <div data-bbox="407 867 1445 1371"> <p>Recomendación:</p> <p>Definir e implementar un procedimiento de restauración de copias de respaldo que le permita al HGM confirmar la integridad y disponibilidad de la información ante un evento que lo requiera. Este procedimiento deberá estar alineado a las políticas y manuales de seguridad de la información del HGM, incluyendo entre otros los siguientes aspectos:</p> <ul style="list-style-type: none"> • Periodicidad de la restauración de las copias de respaldo. • Responsables ejecutar la restauración. • Fecha/hora de la ejecución. • Pruebas para verificar la integridad de la información restaurada. • Definición de las ventanas de tiempo para la ejecución del proceso. • Acciones en caso de fallas durante la restauración. • Documentación soporte del proceso. </div> <div data-bbox="407 1371 1445 1497"> <p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p> </div> <div data-bbox="407 1497 1445 1686"> <p>Observación No.10: Activación y monitoreo de logs de auditoría</p> <p>El HGM tiene configurados logs de auditoría en los servidores y sistemas de información. Sin embargo, no cuenta con un procedimiento formal de revisión de dichos logs que le permita identificar de forma oportuna situaciones inusuales o intentos de acceso no autorizados por parte de los usuarios en los sistemas de información.</p> </div> <div data-bbox="407 1686 1445 1803"> <p>Recomendaciones:</p> <p>Validar en conjunto con las áreas de negocio los logs que actualmente se encuentran activados tanto a nivel de servidores como de los sistemas de información, y definir las</p> </div>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>actividades que por la operación del HGM son críticas o relevantes. Una vez se definan estas actividades, se deberá:</p> <ul style="list-style-type: none"> • Activar los logs de auditoría y definir un procedimiento formal de revisión de los mismos, que incluya entre otros: <ul style="list-style-type: none"> - Definición de las actividades/eventos objeto de la revisión. - Fecha de la revisión. - Personal responsable. - Situaciones identificadas. - Planes de acción en caso de identificar actividades inusuales. - Documentación soporte de la revisión. • Almacenar los logs de auditoría mínimo por un año, con el fin de contar con esta información para dar respuesta a requerimientos regulatorios, de auditoría, o cuando sean requeridos por la entidad. <p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
<p>Adquisición, Desarrollo y Mantenimiento de los sistemas de información</p>	<p>Observación No. 11: Optimización del proceso de gestión de cambios en los sistemas del HGM</p> <p>Si bien el HGM tiene definido un procedimiento para la gestión de cambios en los sistemas de información e infraestructura, se identificó que este procedimiento presenta las siguientes situaciones susceptibles de mejora:</p> <ul style="list-style-type: none"> • No todas las solicitudes de cambios ingresan por la 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 las 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 las 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). <p>La no aplicación constante y consistente del procedimiento de cambios podría conllevar a que se soliciten, autoricen, prueben y se ejecuten cambios en el ambiente productivo sin la debida autorización de las áreas de negocio y/o que no cumplan con las necesidades requeridas.</p>

	<p>Recomendaciones:</p> <ul style="list-style-type: none"> • Aplicar de forma consistente el procedimiento de gestión de cambios que permita catalogar las diferentes solicitudes de cambio de acuerdo con la criticidad de las mismas 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, tanto para cambios relacionados con infraestructura y los sistemas de información, 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. <p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
<p>Gestión de incidentes de seguridad</p>	<p>Observación No. 12: Alineación del proceso de gestión de incidentes de seguridad con el Manual de Seguridad de la Información</p> <p>En el Manual de Seguridad de la Información no se observa la inclusión de políticas y procedimientos relacionados con la gestión de incidentes de seguridad de la información, pese a que el HGM tiene definido el “Manual Operativo de los sistemas de información” que describe las actividades relacionadas con la gestión de incidentes de seguridad de la información. Esta situación puede conllevar a que se omitan controles importantes de la gestión de incidentes de seguridad de la información al no estar contenidos en el Manual de Seguridad de la Información, el cual es el documento guía para el Modelo de seguridad del HGM.</p> <p>Recomendación:</p> <p>Revisar el Manual de Seguridad de la Información e incluir y relacionar las actividades y procedimientos de la gestión de incidentes de seguridad, nombrando el Manual de Operaciones de los Sistemas de Información, lo cual le permitirá al HGM contar con lineamientos claros y aprobados para gestionar y responder a todos los incidentes que puedan presentarse en el HGM.</p> <p>Como parte de las revisiones que se definan sobre el Modelo de Seguridad de la Información, se deberán considerar cada uno de los procedimientos, instructivos, entre otros con los que cuenta el HGM y los cuales deberán estar contenidos en el Manual de Seguridad de la Información y a su vez en la Política de Información.</p>

	<p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
<p>Gestión de la Continuidad del negocio</p>	<p>Observación No. 13: Plan de continuidad del negocio (BCP):</p> <p>El HGM cuenta con planes de contingencia para los sistemas de información e infraestructura que soporta la operación de este.</p> <p>Sin embargo, no existe la definición de un Plan de Continuidad de negocio que le permita al HGM continuar sus operaciones hasta que se restablezca la plataforma tecnológica, donde se pueda ver:</p> <ul style="list-style-type: none"> • Objetivos y Alcance del Plan de Continuidad • Roles, mecanismos y responsabilidades • Generalidades del Plan de Continuidad • Análisis del entorno institucional • Riesgos asociados a la continuidad del negocio
	<p>Recomendación:</p> <p>Definir e implementar un plan de continuidad del negocio, que le permita al HGM reaccionar de forma oportuna frente a un evento que pudiera impactar la operación y funcionamiento del HGM. Este plan de continuidad deberá incluir entre otros, los siguientes aspectos:</p> <ul style="list-style-type: none"> • Identificación de las amenazas a las que está expuesto el HGM. • Definir un Análisis de Impacto al negocio (BIA), en el cual se determinen los procesos, áreas de negocio, sistemas de información, entre otros que son críticos para el funcionamiento del HGM. • Integrar los planes de recuperación ante desastres (Planes de Contingencia) definidos actualmente para la plataforma tecnológica del HGM. • Definir planes de prueba del plan de continuidad del negocio de forma periódica, que le permita al HGM conocer y medir los tiempos de respuesta frente al mismo y tomar acciones para optimizarlos. Adicionalmente, es importante que cada vez que se presenten cambios en la operación del HGM éstos sean considerados en el Plan de Continuidad de Negocio definido.
	<p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>

II. ESTADO DE AVANCE EN LA IMPLEMENTACIÓN DE LOS REQUERIMIENTOS DE TI EXIGIDOS POR MIPG:

ASPECTO EVALUADO	OBSERVACIÓN
Avances MIPG	Observación No.01: Uso y Apropiación Encontramos que actualmente se han planteado iniciativas de TI para mejorar el gobierno de TI y entregar un adecuado servicio a sus clientes internos, sin embargo, falta generar la estrategia y medición de dichas iniciativas, gestión de cambios y proyectos que generen innovación tecnológica para el servicio del HGM.
	Recomendación: Es importante que el área de TI defina un procedimiento para el uso y apropiación tecnológica donde se tengan en cuenta: <ul style="list-style-type: none"> • Estrategia para el uso y apropiación de TI • Gestión de cambios, que apalanque los proyectos e iniciativas que se generen desde TI. • Puntos de control e indicadores que ayuden a medir la evaluación del impacto de la estrategia de uso y apropiación de los proyectos de TI.
	Disposición, Julián Gómez – Líder de Sistemas del HGM: De acuerdo con la recomendación
Avances MIPG	Observación No.02: Información Durante nuestra revisión de los componentes Información y Gobierno de TI, observamos que se tiene una concentración de funciones sobre el líder de sistemas a nivel de la gestión de la Seguridad de la Información, ya que debe cumplir tres roles: <ul style="list-style-type: none"> • Líder de sistemas • Oficial de seguridad • Administrador de Seguridad de la información Por lo anterior, se denota una inadecuada segregación funcional que podría impactar los procedimientos y actividades a nivel de seguridad y administración de la información.
	Recomendación: Tomando como punto de partida la segregación funcional dentro del área de TI, recomendamos que la entidad evalúe la posibilidad de incorporar un colaborador que ejecute el rol de Oficial de Seguridad de la Información, el cual deberá ser

ASPECTO EVALUADO	OBSERVACIÓN
	<p>independiente del área de TI, con el fin de no afectar su independencia desde el punto de vista de cumplimiento y asegurabilidad de los controles gestionados y evaluados.</p> <p>Es importante que desde el área de Control Interno se tenga en cuenta esta recomendación como apoyo fundamental de la seguridad de la información en todo el HGM.</p> <p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>
Avances MPG	<p>Observación No.03: Gobierno de TI</p> <p>Al verificar el componente de gobierno de TI, observamos que, si bien se tiene definido el esquema y procedimientos para la gestión de infraestructura de TI, hace falta diseñar y construir el esquema de gobierno de TI que contemple las políticas, procesos, recursos, gestión del talento humano y proveedores, compras, calidad, instancias de decisión, estructura organizacional e indicadores de la operación de TI (<i>tomado de la guía de diagnóstico de MIPG</i>).</p>
	<p>Recomendación:</p> <p>Realizar la documentación necesaria y requerida por MIPG en cuanto a Gobierno de TI, con el fin de optimizar y mejorar las políticas y procedimientos actuales que corresponden al gobierno y administración de TI.</p> <p>No solo es su diseño y construcción, sino también su publicación, oficialización y divulgación en la entidad con el fin de que sea conocida y aplicada por todos los funcionarios tanto internos como externos del HGM.</p>
	<p>Disposición, Julián Gómez – Líder de Sistemas del HGM:</p> <p>De acuerdo con la recomendación</p>

**CAPÍTULO II
INFORME GENERAL
AUDITORÍA DE LOS PROCESOS DE TI CON BASE EN LA NORMA ISO27001 – ESTADO ACTUAL
EN RELACIÓN CON MIPG
CON CORTE A NOVIEMBRE DE 2018**

A continuación, detallamos cada uno de los aspectos correspondientes a buenas prácticas de la seguridad de la información:

- Evaluación de seguridad de la información a partir de la Norma ISO27001.
- Conclusiones del trabajo realizado.

Evaluación de la seguridad de la información a partir de la Norma ISO27001

Para esta evaluación aplicamos una herramienta que contiene los objetivos de control y sus puntos de calificación según lo detallado en la norma ISO27001. Dicha evaluación, presenta un esquema general del estado actual del área de sistemas con respecto a la seguridad de la información.

La norma ISO 27001 se compone de 11 dominios y cada uno de ellos contiene objetivos de control, los cuales, describen las pautas a seguir para mejorar y adecuar el ambiente de control de TI alineándolo con los objetivos del negocio.

A continuación, presentamos un fragmento de la herramienta utilizada sobre los objetivos de control pertenecientes al dominio “Política de seguridad corporativa de la información”, compuesto por 6 objetivos de control; se anexa el detalle de los resultados obtenidos por medio de dicha herramienta, por cada uno de los dominios, evaluados:

			DIAGNÓSTICO EN ISO - 27001 SEGURIDAD DE LA INFORMACIÓN										SUFICIENCIA DE LOS CONTROLES										RESPONSA- BLES	ESTADO	PLAN DE ACCIÓN																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						
													2 CUMPLE																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
RAZON SOCIAL DE LA EMPE			HOSPITAL GENERAL DE MEDELLIN										1 CUMPLE PARCIAL																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
FECHA DE EJECUCION			2 NOVIEMBRE DE 2018										0 NO CUMPLE																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
NOMBRE DEL ASESOR:			Luz Angela Gordillo										ÁREAS																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
CONTACTO:			3155453529										MAIL: angela.gordillo@newsol.com																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
FICHA TECNICA DE LEVANTAMIENTO DE INFORMACION DE LOS CONTROLES EXISTENTES PARA LA SEGURIDAD DE LA INFORMACIÓN																							Sistemas e Informatica	Control Interno	Proveedores																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						

Imagen No. 01 – Tomada de la matriz de la norma ISO27001 evaluada para el Hospital General de Medellín

A continuación, presentamos la herramienta utilizada para realizar la evaluación y diagnóstico de MIPG:

	B	C	D	E	F	G	H
	LOGROS DEL COMPONENTE	CRITERIOS	SUB-CRITERIOS	Responsable (s)	% cumplimiento	% avance	
1							
2		C3.3.1. Planeación y Gobierno de Componentes de Información. Busca incorporar un esquema de gestión de los componentes de información en las entidades.	a) La entidad cuenta con un catálogo de componentes de información (datos, información, servicios y flujos de información).	Líder de Sistemas		0,5%	0,5%
15		C3.3.2. Diseño de los Componentes de Información. Busca estructurar y caracterizar los componentes de información.	a) La entidad dispone de medios electrónicos que permiten gestionar certificaciones y constancias garantizando la seguridad y privacidad de la información.	Líder de Sistemas		0,5%	0,4%
16			b) La entidad provee y/o consume componentes de información a través de la Plataforma de Interoperabilidad.	Líder de Sistemas		0,5%	0,5%
17	C3.3. INFORMACIÓN. Busca aportar valor estratégico a la toma de decisiones a partir de la gestión de la información como un producto y servicio de calidad.	C3.3.3. Análisis y Aprovechamiento de Componentes de Información. Busca el uso eficiente de los componentes de información para la toma de decisiones.	a) La entidad cuenta con procesos y herramientas que facilitan el consumo, análisis, uso y aprovechamiento de los componentes de información.	Líder de Sistemas	3,0%	0,5%	0,5%
18		C3.3.4. Gestión de la Calidad y de Seguridad de los Componentes de Información. Busca definir y gestionar controles y mecanismos que contribuyan a alcanzar los niveles requeridos de calidad, seguridad, privacidad y trazabilidad de los componentes de información.	a) La entidad aplica los mecanismos adecuados de aseguramiento, control, inspección y mejoramiento de la calidad de los componentes de información.	Líder de Sistemas		0,5%	0,5%
19			b) La entidad define y gestiona los controles y mecanismos para alcanzar los niveles requeridos de seguridad, privacidad y trazabilidad de los componentes de información.	Líder de Sistemas		0,5%	0,5%
20		C3.4.1. Planeación y gestión de los Sistemas de Información. (Busca planear y gestionar los sistemas de información (misional, de apoyo, portales digitales y de direccionamiento estratégico).	a) La entidad cuenta con una arquitectura de sistemas de información.	Líder de Sistemas		0,5%	0,2%
21							

Imagen No. 02 – Tomada de la matriz de Diagnostico de MIPG evaluada para el Hospital General de Medellín

LOGROS DEL COMPONENTE	CRITERIOS	SUB-CRITERIOS	Responsable (s)	% cumplimiento	% avance
C3.6. USOS Y APROPIACIÓN. Busca realizar actividades orientadas al desarrollo de competencias TI y vincular los diversos grupos de interés en las iniciativas TI	C3.6.1. Estrategia para el uso y apropiación de TI. Busca definir e implementar la estrategia de uso y apropiación de TI.	a) La entidad establece e implementa la estrategia de uso y apropiación de TI, de acuerdo con la caracterización de sus usuarios, ciudadanos y grupos de interés.	Líder de Sistemas	1,0%	0,35%
	C3.6.2. Gestión del cambio de TI. Busca adaptarse al cambio generado por la implementación de los proyectos o iniciativas de TI.	a) La entidad desarrolla acciones de sensibilización y socialización de los proyectos o iniciativas de TI, a partir de la estrategia de uso y apropiación de TI.	Líder de Sistemas	3,0%	1,0%
	C3.6.3. Medición de resultados de uso y apropiación. Busca establecer e implementar el monitoreo y evaluación del impacto de la estrategia de uso y apropiación de los proyectos de TI.	a) La entidad realiza el monitoreo, evaluación y mejora continua de la Estrategia de uso y apropiación de los proyectos de TI.	Líder de Sistemas	1,0%	0,25%
C3.7. CAPACIDADES INSTITUCIONALES. Busca desarrollar capacidades institucionales para la prestación de servicios a través de la automatización de procesos y procedimientos y la aplicación de buenas prácticas de TI.	C3.7.1. Uso eficiente del papel. Busca el uso eficiente de papel a través de la definición y adopción de buenas prácticas mediatas por TI.	a) La entidad define e implementa buenas prácticas para el uso eficiente del papel, mediatas por TI.	Líder de Sistemas	1,0%	1,0%
	C3.7.2. Gestión de documentos electrónicos. Busca incorporar el uso de documentos electrónicos con base en el análisis de los procesos de la entidad.	a) La entidad cuenta con esquemas y herramientas de gestión de documentos electrónicos, con base en el análisis de los procesos de la entidad.	Líder de Sistemas	3,0%	1,0%
	C3.7.3. Automatización de procesos y procedimientos. Busca automatizar los procesos y procedimientos estratégicos en la institución.	a) La entidad identifica y prioriza las acciones o proyectos a implementar para la automatización de procesos y procedimientos.	Líder de Sistemas	1,0%	0,9%
C3.8. CAPACIDADES INSTITUCIONALES. Busca desarrollar capacidades institucionales para la prestación de servicios a través de la automatización de procesos y procedimientos y la aplicación de buenas prácticas de TI.	C3.8.1. Automatización de procesos y procedimientos. Busca automatizar los procesos y procedimientos estratégicos en la institución.	a) La entidad automatiza procesos y procedimientos internos.	Líder de Sistemas	1,0%	1,0%
TOTAL CUMPLIMIENTO COMPONENTE 3: TIC PARA LA GESTIÓN.				25,0%	19%

Imagen No. 03 – Tomada de la matriz de Diagnóstico MIPG evaluada para el Hospital General de Medellín

Al realizar la evaluación de la Norma ISO 27001 obtuvimos los siguientes resultados por cada uno de los dominios:

TABLA DE PONDERACIÓN	DIAGNÓSTICO	SIN INVERSIÓN EN TECNOLOGÍA	CON INVERSIÓN EN TECNOLOGÍA
DOMINIOS APLICABLES			
1. POLÍTICA DE SEGURIDAD CORPORATIVA	83,33%	50,00%	0,00%
2. ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD INFORMÁTICA	87,50%	37,50%	0,00%
3. CLASIFICACIÓN Y CONTROL DE COMPONENTES CRÍTICOS	83,33%	0,00%	0,00%
4. SEGURIDAD DEL RECURSO HUMANO	88,89%	11,11%	0,00%
5. SEGURIDAD FÍSICA Y AMBIENTAL	81,82%	0,00%	0,00%
6. ADMINISTRACIÓN DE OPERACIONES Y COMUNICACIONES	26,09%	0,00%	4,35%
7. CONTROL DE ACCESO	44,44%	16,67%	5,56%
8. DESARROLLO, MANTENIMIENTO Y ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN	50,00%	25,00%	12,50%
9. ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA	100,00%	20,00%	0,00%
10. GESTIÓN DE CONTINUIDAD DEL NEGOCIO	0,00%	0,00%	0,00%
11. CUMPLIMIENTO Y NORMATIVIDAD LEGAL	100,00%	0,00%	0,00%
TOTAL EVALUACION Y VALORACION	67,76%	14,57%	2,04%

Tabla No. 01 – Tomada de la matriz de la Norma ISO27001 evaluada para Hospital General de Medellín

Dichos resultados se presentan gráficamente así:

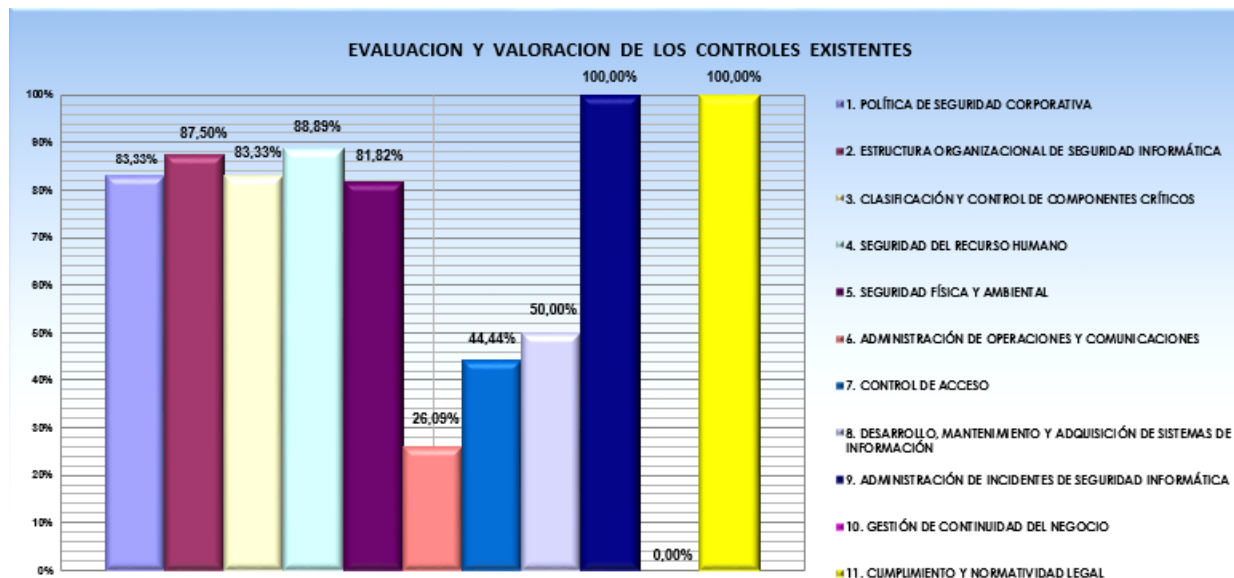


Imagen No. 04 – Tomada de la matriz de la Norma ISO27001 evaluada para Hospital General de Medellín

Conclusiones del trabajo realizado:

ISO 27001:

1. En la gráfica anterior se ilustra el porcentaje actual de implementación y madurez de la seguridad de la información el cual está en 67,72%, lo cual demuestra el compromiso del HGM en la adopción de buenas prácticas para la gestión de la seguridad de la información.
2. Las oportunidades de mejora expuestas en este informe implican por parte del HGM implementar planes de acción a corto/mediano plazo que le ayudarán en el logro de un ambiente de control eficiente y eficaz sobre la seguridad de la información y a reducir los riesgos de la pérdida/daño de la integridad, confidencialidad y disponibilidad a los que podría estar expuesta la información.
3. Es importante resaltar que el HGM no sólo debe completar la definición de políticas, procedimientos, manuales e instructivos de la Seguridad de la Información actual, sino que deberá poner en marcha la operación del Gobierno de Seguridad de la Información definido y propender por la adopción del modelo de mejoramiento continuo (P – Planear, H – Hacer, V – Verificar, A – Actuar) sobre el Modelo de Gestión de la Seguridad de la Información definido.

MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG

1. En cuanto al componente de estrategia de TI en MIPG, se está elaborado el catálogo de servicios de acuerdo con los proyectos y necesidades de la entidad.
2. Adicionalmente se cuenta con el Plan Estratégico de TI construido y aprobado. Así mismo, se busca alinear el modelo PMP de gestión de proyectos en las actividades que contiene el PETI y de esta manera poder realizar una adecuada gestión de éstos.
3. Es importante que se desarrollen indicadores y/o puntos de control sobre la gestión de la seguridad. Esta actividad debe estar en cabeza de un Oficial de seguridad de la Información, quien se encargue de administrar no solo los indicadores sino sus causas, riesgos y controles que ayuden a mitigar y minimizar el riesgo en la entidad.
4. En cuanto al manejo de los desechos tecnológicos, es importante que se destine un espacio físico para almacenar los residuos tecnológicos, donde se pueda ver una clasificación y orden adecuado para su reciclaje.
5. Finalmente, se denota un gran compromiso y avance de implementación y madurez del área de TI en la implementación de MIPG, lo cual genera valor y confiabilidad de esta área hacia los demás procesos de la entidad. Si bien existen aspectos por mejorar, debemos resaltar los avances obtenidos a la fecha y el estado actual de la información allí contenida.