PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACIÓN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

Las entidades hoy en día reconocen el protagonismo de la información en sus procesos, por tanto, la importancia de tener su información adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La seguridad de la información en las entidades tiene como objetivo la protección de los activos de información, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

El Fondo de Bienestar Social de la CGR, decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por la Alta Dirección, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado.
- Integridad: Propiedad que la información se mantenga exacta y completa.
- Disponibilidad: Propiedad que la información sea accesible y utilizable en el momento que se requiera.

2. OBJETIVO

Brindar al Fondo de Bienestar Social de la CGR una herramienta con enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, a través de métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas, así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

2.1 Objetivos específicos: En beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en la FONDO DE BIENESTAR SOCIAL DE LA CGR, se declaran los siguientes objetivos específicos:

- Brindar lineamientos y principios que propendan por la unificación de criterios para la administración de los riesgos de seguridad de la información.
- Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas

- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información y su mitigación.

- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.

- Lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad e impacto residual de los riesgos a el nivel aceptable por parte de la Alta Dirección.

3. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la FONDO DE BIENESTAR SOCIAL DE LA CGR, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

4. TÉRMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro del Fondo de Bienestar Social de la CGR.

- Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

- Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

- Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

- Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- Consecuencia: Resultado de un evento que afecta los objetivos.

- Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

- Control: Medida que modifica el riesgo.

- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

- Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

- Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

- Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

- Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- Integridad: Propiedad de la información relativa a su exactitud y completitud.

- Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

- Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

- Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

- Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

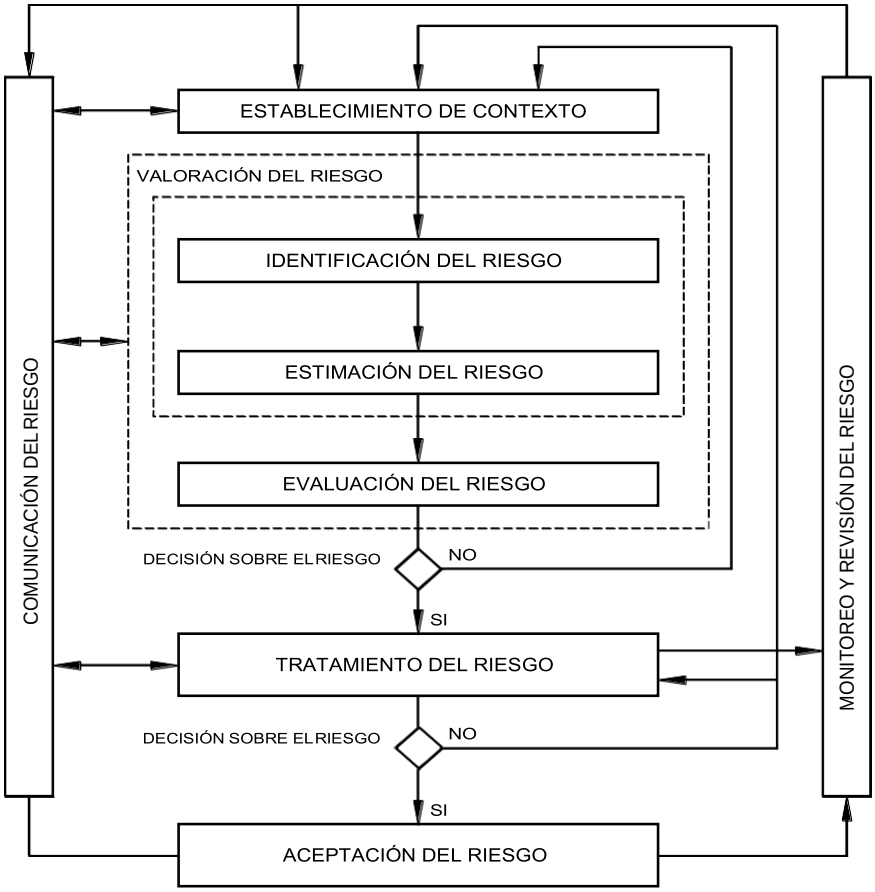
- Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

- Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

- Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- Riesgo: Efecto de la incertidumbre sobre los objetivos.
- Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular
- Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
- Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).
- Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información
- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- SGSI: Sistema de Gestión de Seguridad de la Información.

5. VISIÓN GENERAL DEL PROCESO DE GESTIÓN DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado basado tanto en la norma ISO/IEC 31000 como en la ISO 27005; los elementos que lo componen son:



Fuente ISO 27005

La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.

Establecimiento del contexto de riesgos de seguridad de la información.

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte del Fondo de Bienestar Social de la CGR y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos del Fondo de Bienestar Social de la CGR, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

Criterios de evaluación del riesgo de seguridad de la información: La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en el FONDO DE BIENESTAR SOCIAL DE LA CGR.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones del FONDO DE BIENESTAR SOCIAL DE LA CGR
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación del Fondo de Bienestar Social de la CGR.

Criterios de Impacto: Los criterios de impacto se especificarán en términos del grado, daño o de los costos para el Fondo de Bienestar Social de la CGR, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Criterios de Aceptación: Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos del Fondo de Bienestar Social de la CGR y de las partes interesadas.

Valoración de los riesgos de seguridad de la información. Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información. Se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para el Fondo de Bienestar Social de la CGR, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:
Análisis del riesgo

- Identificación de los riesgos
- Estimación del riesgo
- Evaluación del riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los activos de información se clasifican en dos tipos:

Primarios:

- Procesos o subprocesos y actividades del Negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

- Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

- Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

De soporte:

- Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

- Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

- Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

- Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

- Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

- Estructura organizativa: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los proesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los

activos de información de la FONDO DE BIENESTAR SOCIAL DE LA CGR. Existen distintos métodos para analizar amenazas, por ejemplo:

Entrevistas con líderes de procesos y usuarios

Inspección física

Uso de las herramientas para el escaneo automatizado

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

Estimación del riesgo: La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos.

El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- Probabilidad: La posibilidad de ocurrencia del riesxzgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.

- Impacto: Hace referencia a las consecuencias que puede ocasionar al Fondo de Bienestar Social de la CGR la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio

A continuación, se presenta la matriz de riesgos del Fondo de Bienestar Social de la CG

		DETERMINACIÓN DE CONTROLES EXISTENTES				MATRIZ DE ANALISIS DE RIESGOS							ANALISIS DE MITIGACIÓN EJECUCIIÓN DEL CONTROL (RESIDUAL)				PLANTEAMIENTO DE AJUSTE
ITEM	**RIESGOS**	**TIPO**	**PILAR AFECTADO NORMA 27000**	**¿EXISTE ALGUN CONTROL?**	**¿ES LO MÁS APROPIADO?**	**PROBABILIDAD**	**IMPACTO**	**NIVEL DE RIESGO**	**TRATAMIENTO SUGERIDO**	**FECHA DE INICIO**	**FECHA DE FIN**	**RESPONSABLE DE LA EJECUCIÓN**	**PROBABILIDAD**	**IMPACTO**	**NIVEL DE RIESGO**	**MITIGACIÓN PUNTUAL**	
1	Incumplimiento de los acuerdos establecidos en los pliegos de contratación por parte de los proveedores y contratistas.	Humano - Proceso	Integridad - Disponibilidad - Seguridad	SI	Si, ya que existe un supervisor experto en el área para revisar el cumplimiento de los acuerdos establecidos.	5	5	25	Ejecución de los Acuerdos de Nivel de Servicios o las sanciones contempladas en la ley 80 referente a contratación estatal, Se realiza la mitigación del riesgo.	17/01/2020	30/12/2020	Supervisor de contrato	2	5	10	15	
2	Demoras en la gestión por parte de la administración en los trámites requeridos por el área de sistemas.	humano - administrativo	Integridad - Disponibilidad - Seguridad	SI	Se ajustó el manual y se ha dado celeridad a los procesos	5	5	25	Aplicabilidad del manual de contratación de la entidad, Se realiza la mitigación del riesgo.	17/01/2020	30/12/2020	Dirección Administrativa	1	1	1	24	
3	Disminución de los recursos asignados al área de sistemas	humano - administrativo	Integridad - Disponibilidad - Seguridad	SI	Es el único control implementarle.	5	7	35	Redistribución de los recursos asignados al FBS	17/01/2020	30/12/2020	Dirección Administrativa	5	5	25	10	

5	Robo de información por parte de los funcionarios.	humano - seguridad	Integridad - Seguridad	SI	Se encuentra bloqueado la copia de CD y DVD, la información del sistema financiero se encuentra restringida a registro y acceso, más sin embargo el acceso por USB se encuentra habilitado, por lo tanto se vulnera la seguridad de la información al momento que los funcionarios se llevan los datos para continuar con su trabajo fuera de las instalaciones de la entidad.	10	7	70	Restricción de los medios de almacenamiento mediante bloqueos de periféricos. Revisión de la información substraída con el fin de determinar las implicaciones del robo. Se realiza la mitigación del riesgo con el ajuste de los sistemas de dominio y antivirus con el fin de implementar restricciones de dispositivos USB y la presentación de políticas de manejo de la información generada, entregada y manipulada en la entidad.	1/01/2019	30/12/2019	Profesional área de sistemas	5	5	25	45	

6	Traslado de archivos en medios extraíbles	humano - seguridad	Integridad - Disponibilidad - Seguridad	NO		10	7	70	Instalación de software de monitoreo de los equipos y bloqueo de accesos a USB, Se realiza la mitigación del riesgo.	1/01/2019	30/12/2019	Profesional área de sistemas	2	2	4	66	Restricción de accesos de memorias USB mediante software de gestión de seguridad
7	Substracción de equipos.	seguridad	Integridad - Disponibilidad - Seguridad	SI	Se realiza la revisión y solicitud de autorizaciones por parte de la empresa de vigilancia contratada por la entidad.	3	5	15	Revisión del sistema de cámaras de seguridad y registro de acceso con el fin de determinar la ruta por la cual los equipos fueron retirados de las instalaciones, con base en esta información identificar a los implicados con el fin de aplicar las correspondientes medidas. Se realiza la mitigación del riesgo.	1/01/2019	30/12/2019	Supervisor del contrato	1	2	2	13	
8	Terremotos	Naturaleza	Integridad - Disponibilidad - Seguridad	NO		3	10	30	Se transfiere el riesgo. Mediante las pólizas de seguros.	1/01/2019	30/12/2019	Dirección Administrativa	3	5	15	15	

9	Tormentas eléctricas.	Naturaleza	Disponibilidad	NO		5	5	25	De acuerdo con la intensidad empezar la secuencia de apagado de equipos con el fin de evitar daños en la infraestructura de comunicaciones como en los equipos del FONDO DE BIENESTAR SOCIAL DE LA CGR. Se realiza la mitigación del riesgo.	1/01/2019	30/12/2019	Dirección Administrativa - Recursos físicos	5	5	25	0	
10	Incendios.	Naturaleza agentes humano agentes externo	Disponibilidad	NO		5	10	50	Se realizó la solicitud a la administración para contratar la implementación de sistema de aviso y extinción de incendios. Se realiza la mitigación del riesgo con la solicitud que se dirigió a la gerencia de la entidad y la dirección administrati	1/01/2019	30/12/2019	Dirección Administrativa - Recursos físicos	2	5	10	40	Validar la operación de los sistemas de extinción

									va y financiera.								
11	Cambios a la normatividad en los procesos de contratación.	Normativo	Integridad - Disponibilidad - Seguridad	NO		3	3	9	Realizar la correspondiente revisión de la normatividad modificada con el fin de verificar el impacto sobre los procesos existentes y si resultan ser afectados aplicar correctivos necesarios. Se acepta el riesgo.	1/01/2019	30/12/2019	Profesional área de sistemas	2	2	4	5	
12	Caída de los servidores	Software administrativo	Integridad - Disponibilidad - Seguridad	SI	Se realiza el registro de los eventos en el formato de operación de los servidores y se hace la corrección del evento, si es de hardware se adelanta el trámite de solicitud de soporte	10	10	100	Utilizar el protocolo de mantenimiento referente al proceso de respaldo en cuanto a caída de servidores. Se realiza la mitigación del riesgo a través de la contratación de empresas	17/01/2020	30/12/2020	Profesional área de sistemas	2	10	20	80	Realizar la contratación de un tercero para aumentar el nivel de eficiencia del control

					al contratista de mantenimiento y si es de software se realiza la revisión y el debido a acompañamiento por parte del proveedor de las aplicaciones montadas en los servidores				de apoyo tanto para los sistemas Windows, Linux, bases de datos y demás sistemas implementados en los servidores.								
13	Ataques de virus, troyanos, gusanos y spyware.	Seguridad	Integridad - Disponibilidad - Seguridad	SI	Se actualiza el antivirus y se mantienen parchados los sistemas a través de las consolas	5	5	25	Dependiendo de la severidad del ataque y la vulnerabilidad de los sistemas ejecutar rutinas de contención y utilización de antivirus con el fin de eliminar la infección o realizar su contención hasta lograr eliminarla de los equipos. Se realiza la mitigación del riesgo.	17/01/2020	30/12/2020	Profesional área de sistemas - Empresa soporte	2	2	4	21	
14	Mal diseño de la red de datos.	Infraestructura	Disponibilidad	SI	No, porque se está utilizando software	3	3	9	Revisión del plano lógico de la red de datos y	17/01/2020	30/12/2020	Empresa de soporte	1	2	2	7	

					que no es el más funcional.				diseñar los correctivos para solventar la falla en la transmisión de datos. Se realiza la mitigación del riesgo.								
15	Desbalanceo de las cargas de la red eléctrica.	Infraestructura	Disponibilidad	SI	No, porque no hay un sistema de monitoreo en la red eléctrica y se realizan reasignación de personal y áreas sin contar con el estudio previo de distribución de cargas.	5	5	25	Identificar la fuente del desbalance o de cargas y redistribuirlas a fin de evitar caídas en el sistema. De presentarse caídas iniciar la secuencia de encendido para identificar la fuente del desbalance o y corregirlo mediante el balanceo de cargas sobre el tablero eléctrico. Se realiza la mitigación del riesgo.	17/01/2020	30/12/2020	Dirección Administrativa - Recursos físicos	1	5	5	20	

16	Desactualización de manuales y planes de contingencia	Administrativo integridad	Integridad - Seguridad	NO		10	5	50	Revisión de los procesos e identificación de las falencias de los manuales y los planes de contingencia de cada proceso con el fin de asegurar la continuidad del negocio, de no existir ni el manual ni el plan de contingencia este debe ser desarrollado. Se realiza la mitigación del riesgo.	17/01/2020	30/12/2020	Profesional área de sistemas	5	5	25	25	
17	Sabotaje a la red.	Seguridad	Integridad - Disponibilidad - Seguridad	NO		10	5	50	Identificar la procedencia del sabotaje, determinar si es a nivel lógico o físico, si es a nivel lógico realizar el seguimiento del tráfico a través del software de monitoreo e identificar los alcances	17/01/2020	30/12/2020	Profesional área de sistemas	2	5	10	40	Adquisición de equipos de seguridad y software especializado

									del sabotaje con base en estos alcances determinar la acción a tomar. Si es a nivel físico realizar la investigación debida para identificar a las personas implicadas y determinar la acción a ser tomada. En cualquier caso, se debe realizar un análisis para determinar las acciones correctivas para evitar futuros sabotajes. Se realiza la mitigación del riesgo.								
18	Descontento de los funcionarios	Humano	Integridad - Seguridad	NO		5	5	25	Realizar reuniones de concertación e identificar las causas y posibles fuentes de desconciert	17/01/2020	30/12/2020	Alta Gerencia	4	4	16	9	

									o para tomar medidas correctivas, que pueden ir desde la modificación de funciones hasta el nivel de investigación interna con sus debidas implicaciones. Se realiza la mitigación del riesgo.							
19	Penetración indebida	Seguridad	Integridad - Disponibilidad - Seguridad	SI	Se registra a través del acceso de firewall y con políticas de auditoria sobre los recursos compartidos del servidor.	5	5	25	Identificar el punto de acceso y determinar el grado de complicidad de los diversos funcionarios, con base en estos hechos realizar el proceso de investigación interna con las debidas implicaciones que esto conlleva, paralelamente se debe dar parte a las autoridades y entes de	17/01/2020	30/12/2020	Profesional área de sistemas - alta gerencia	2	2	4	21	

									control, para identificar a los participantes en la acción y realizar el debido proceso legal, de igual forma se debe identificar las intenciones de dicha acción. Se debe verificar si el acceso fue consecuencia de un punto de acceso desprotegido y corregir dicha situación. Se realiza la mitigación del riesgo.								
20	Cambio de las actividades establecidas en el manual de procesos.	Administrativo	Disponibilidad	NO		3	3	9	Se debe realizar el ajuste de las normas de seguridad a las nuevas actividades, de ser necesario se deben ajustar las normas de seguridad a	17/01/2020	30/12/2020	Dirección administrativa y financiera	2	2	4	5	

									actividades o procesos nuevos. Se realiza la mitigación del riesgo.							
21	Pérdida de la información almacenada tanto en medio físico como en medio magnético y óptico.	Seguridad integridad	Seguridad	SI	A través de la consola antivirus, generación de backups y atención de solicitudes de recuperación.	10	7	70	Identificar la causa y de ser posible la restauración de la información de las copias de seguridad. Se realiza la mitigación del riesgo.	17/01/2020	30/12/2020	Profesional área de sistemas	5	5	25	45	
22	Falta de compromiso de los funcionarios responsables de las áreas en las cuales se utilizan los sistemas de información de la entidad	Procedimientos	Integridad - Disponibilidad - Seguridad	NO		5	10	50	Se debe adelantar reuniones de concientización sobre la importancia del manejo adecuado de la información e identificar las posibles falencias en los procesos y determinar la responsabilidad de los funcionarios en el proceso, se mitiga este riesgo.	17/01/2020	30/12/2020	Dirección administrativa y financiera - Talento Humano	5	5	25	25	

23	Comunicaciones informales sobre el manejo y acceso a la información sin la debida documentación requerida ni el registro pertinente	Procedimientos	Integridad - Disponibilidad - Seguridad	NO		5	10	50	Se debe realizar el registro de toda información proveniente desde y hacia las áreas con el fin de poder medir la trazabilidad existente. Se debe realizar el registro en el sistema de gestión documental o a través de correos electrónicos, se mitiga este riesgo.	17/01/2020	30/12/2020	Alta Gerencia	5	5	25	25	
24	Manejo indebido de los backup generados	Procedimientos seguridad disponibilidad	Seguridad	NO		10	10	100	Se generara un documento para el manejo de los Backus de igual manera se realizará las pruebas de eficiencia y se verificará la salvaguarda de dichas copias de respaldo, se mitiga el riesgo.	17/01/2020	30/12/2020	Dirección administrativa y financiera	5	5	25	75	Contratar a un externo especializado en manejo de backup´s

25	Ingreso por parte de los funcionarios a páginas web no autorizas	Seguridad	Integridad - Disponibilidad	SI	Se realiza un seguimiento de las páginas no autorizadas, más sin embargo hace falta definir la acción pertinente al momento de presentarse reiteración en el acceso de páginas web o contenido no autorizado o con contenido no relevante para el desarrollo de las actividades al interior de la entidad.	5	5	25	Se aplican bloqueos a través del sistema firewall y sistema antivirus, de persistir el acceso indebido se procederá con el informe de esta situación a la dirección administrativa y financiera de la entidad, se mitiga ese riesgo.	17/01/2020	30/12/2020	Profesional especializado área de sistemas	2	2	4	21	
26	Ejecución de software portable en la red de la entidad	Seguridad	Disponibilidad - Seguridad	SI	Existen restricciones desde las gpo implementadas en la red y en el sistema antivirus de la entidad. Más sin embargo hace falta	5	5	25	Se bloquea el acceso y ejecución de medios portables. Se mitiga este riesgo.	17/01/2020	30/12/2020	Profesional especializado área de sistemas	1	2	2	23	

					definir la acción pertinente al momento de presentarse reiteración en la ejecución de aplicativos portables.											
27	Préstamo indebido de contraseñas token´s	Humano	Integridad - Disponibilidad - Seguridad	SI	El control del uso de este elemento toke´n o certificado de firma digital se encuentra asignado mediante acuerdo firmado por el funcionario ante la empresa certificadora. De existir algún fallo o vulnerabilidad en este uso la responsabilidad recae enteramente en el funcionario que tiene asignado el toke´n o certificado de firma digital.	10	7	70	Como responsabilidad de los usuarios finales de los toke´s, contraseñas cuentas de usuarios se realizara un comunicado para dar a conocer los riesgos del préstamo y las implicaciones que conlleva esta actividad, se mitiga el riesgo.	17/01/2020	30/12/2020	Funcionarios	5	5	25	45	

28	Debilidad en las contraseñas del aplicativo ALFANET	Seguridad	Integridad	NO		10	3	30	Se solicitara al administrador del aplicativo el refuerzo de la seguridad de contraseñas, se mitiga este riesgo.	17/01/2020	30/12/2020	Funcionarios - proveedor aplicación	2	3	6	24	
29	El sistema ALFANET no se está utilizando por parte de los funcionarios de la entidad	Gestión	Integridad - Disponibilidad	NO		10	5	50	Se solicita a los funcionarios que manejan el sistema ALFANET la realización de capacitaciones y talleres de utilización del aplicativo con el fin de implementar las políticas de cero papel al interior de la entidad y sus sedes externas.	17/01/2020	30/12/2020	Dirección administrativa y financiera	5	2	10	40	Mantener un ciclo de refuerzos en el uso de ALFANET
30	La clasificación por organigrama dentro del aplicativo ALFANET no ha sido alimenta	Administrativo	Disponibilidad	NO		10	3	30	Se solicita al administrador del aplicativo ALFANET el registro correcto de las dependencias y los	17/01/2020	30/12/2020	Dirección administrativa y financiera	2	2	4	26	Realizar el seguimiento de los ajustes

	de forma adecuada								niveles de accesos requeridos, se mitiga este riesgo.								
31	implementado la política de cero papel	Administrativo	Integridad - Disponibilidad - Seguridad	NO		10	7	70	Se solicita al líder de implementación de GEL, los avances correspondientes, se mitiga este riesgo.	17/01/2020	30/12/2020	Dirección administrativa y financiera	10	7	70	0	
32	Retraso de los procesos de contratación del área de sistemas	Administrativo	Disponibilidad	NO		10	7	70	Este riesgo a pesar de ser identificado y de cumplir con los trámites al interior de la entidad solo se puede mitigar con el apoyo de la dirección administrativa y financiera y el apoyo del comité de contratación.	17/01/2020	30/12/2020	Dirección administrativa y financiera	10	5	50	20	
33	Falta de avance en la implementación en la estrategia de Gobierno Digital	Administrativo	Integridad - Disponibilidad - Seguridad	NO		10	10	100	Solicitar a las direcciones y las profesionales de cada grupo el avance de las actividades estipuladas,	17/01/2020	30/12/2020	Alta Gerencia	5	5	25	75	Implementar el comité de PETI

									Este riesgo se Mitiga.							
34	Falta de personal de apoyo, No hay suficiente personal en el área de sistemas, esto implica una exceso en carga laboral de la persona del área,	Administrativo	Disponibilidad	NO		10	10	100	Solicitar un mayor número de personal para el área de sistemas, Este riesgo se Mitiga.	17/01/2020	30/12/2020	Dirección administrativa y financiera	10	10	100	0	
35	Manejo de información descentralizado	Administrativo	Integridad - Seguridad	NO		10	10	100	Verificar la aplicabilidad de la norma de usabilidad e igualdad tecnológica contemplada en la política	17/01/2020	30/12/2020	Direcciones - alta gerencia	2	2	4	96	Establecer los parámetros de Gobierno digital,
36	Aplicativo del Centro médico, sin una persona a cargo que tenga los conocimientos tanto de sistemas de información como manejo de aplicativos de salud y	Administrativo	Integridad - Disponibilidad - Seguridad	NO		10	10	100	Es necesario aplicar la normatividad vigente en cuento a la implementación de la política	17/01/2020	30/12/2020	Dirección de desarrollo y bienestar	5	10	50	50	Definir el rol Operativo y administrativo de la aplicación

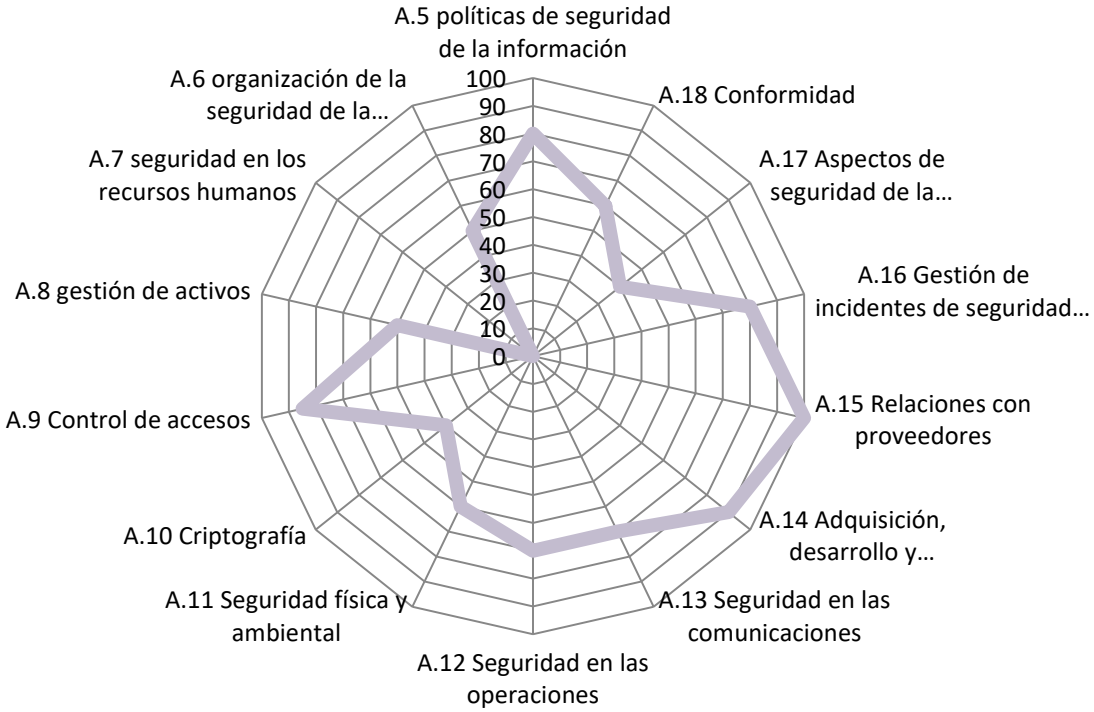
	atención a pacientes															
37	No existe una diferenciación en cuanto administración manejos, operatividad y funcionalidad de los aplicativos	Administrativo	Integridad - Seguridad	NO		10	10	100	Es necesario establecer el nivel de jerarquías y responsabilidades en los aplicativos, se recomienda el cumplimiento de la NTC/ISO 27000 y sus subseries	17/01/2020	30/12/2020	Direcciones - alta gerencia	5	5	25	75	Establecer los preceptos de la norma al interior de la entidad
38	Centralización sobre el área de sistemas de los procedimientos, referentes en los aplicativos de la entidad	Administrativo	Integridad - Disponibilidad - Seguridad	NO		10	10	100	No existe un documento que defina los roles administrativos, operativos, funcionales, auditoria ni manejo de la información, la centralización sobre una única persona va en contra de las normas vigentes en la actualidad, de igual	17/01/2020	30/12/2020	Alta Gerencia	5	5	25	75	Establecer los preceptos de la norma al interior de la entidad

									manera es un alto riesgo mantener en una sola persona todo el control de los aplicativos								

RESULTADO ANALISIS DE BRECHA

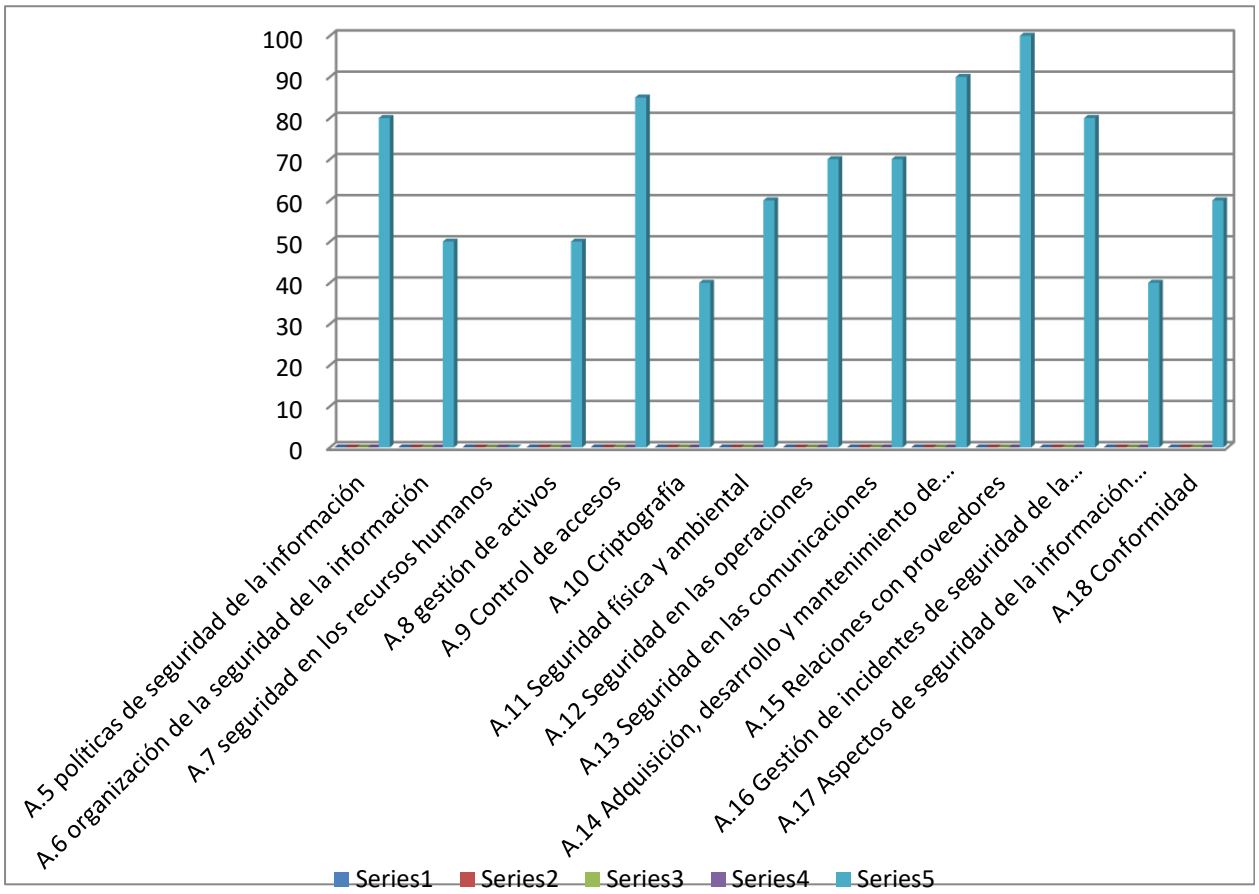
A continuación, se presenta el resultado del análisis GAP (Brecha)

GRÁFICA RADIAL CONTROLES ANEXO A 27002:2013



En el documento anexo se pueden verificar el análisis realizado.

GRÁFICO DE BARRAS PORCENTAJE CUMPLIMIENTO DOMINIOS



Se verifica que existen falencias en el cumplimiento de los dominios de:

1. Seguridad en los recursos humanos: Es necesario fomentar una cultura en el uso de TICS,
2. Seguridad física y ambiental: Es necesario adecuar y brindar de espacios seguros en cada sede al área de sistemas, en la actualidad la ubicación del puesto y del área no ofrece la seguridad requerida ya que expone el puesto a cualquier persona tanto interno como externo.

Es necesario adecuar en todas las sedes un lugar en el cual se pueda desarrollar las actividades del área con los estándares de seguridad requeridos por la norma vigente y la política de Gobierno Digital.