PLAN DE CONTINGENCIAS

1. ESTABLECER EL CONTEXTO.

La primera etapa dentro de la implementación de la administración de riesgos la constituye el establecimiento del contexto de la organización o área que se encuentra en estudio. Esto provee un conocimiento del escenario en el cual se desarrollará el contexto general de la administración de riesgos. Cabe aclarar que el estudio establecido en el presente documento se desarrolla según lo establecido en la norma AS/NZ 4360:1999, “Estándar australiano. Administración de riesgos”, y según los lineamientos planteados en la norma ISO 17799 “Tecnología de la información- Técnicas de seguridad- Código de prácticas para el manejo de la seguridad de la información”. También se utiliza la NTC 5254 Y NTC 27000:2005

1.2 Contexto estratégico

El contexto estratégico identifica tanto las debilidades como las oportunidades, fortalezas y amenazas de la organización; se toma la organización en todos los contextos que la afectan como el financiero, social, legal, entre otros.

Contexto financiero:

- ✓ Recursos de la Nación en especial los correspondientes al 2% del presupuesto asignado a la C.G.R.
- ✓ Aportes efectuados por los funcionarios de la C.G.R.
- ✓ Rendimientos operacionales y financieros.
- ✓ Por los auxilios y donaciones que reciba. Multas que imponga la C.G.R.
- ✓ Por los bienes que como persona jurídica haya adquirido o adquiera.
- ✓ Por el rubro correspondiente a cesantías tanto parciales como definitivas de los empleados.
- ✓ Recursos recibidos por servicios prestados por la Unidad Especial de Estudios Especializados de Control Fiscal – CECOF.
- ✓ Venta de papel rezago, remate de bienes, venta de pliegos, fotocopia y demás actividades administrativas que recibe de la Contraloría.

Contexto Social: El área de sistemas ofrece soporte de Software a las diferentes áreas del Fondo de Bienestar Social de la CGR, a saber: Centro médico, colegio, dirección administrativa y financiera y dirección de desarrollo y bienestar social.

Contexto operativo: Soporte de hardware y software a todos los funcionarios del Fondo de Bienestar Social de la CGR. Administración de aplicativos instalados en el NOC de la sede Administrativa y apoyo en los procesos del Centro médico y Colegio de la CGR

Contexto legal: El área de sistemas del Fondo de Bienestar Social de la CGR pertenece a un establecimiento público adscrito a la CGR. Cabe destacar que el Fondo de Bienestar Social de la CGR fue creado mediante la ley 106 de 1993.

Interesados internos y externos

- Interesados internos: Empleados de la CGR y FBS
  Dirección administrativa y financiera
  Dirección de Desarrollo y Bienestar
  Gerencia FBSCGR
  Auditoría.

- Interesado externos: Familias de los empleados.
  Funcionarios CGR-FBS
  Proveedores de hardware y de software.
  Departamento de Planeación Nacional.
  Ministerio de Hacienda
  MINTIC
  COINFO
  SIIF
  CHIIP
  LITIGOB
  SECOP

Percepciones de los interesados.

- Empleados: El área de sistemas debe velar por la disponibilidad de los sistemas de información existentes.
- Dirección administrativa y financiera: El área de sistemas debe velar por la disponibilidad de los sistemas de información existentes.
- Gerencia: El área de sistemas debe velar por la disponibilidad de los sistemas de información existentes con el fin de adelantar de manera exitosa el proceso de comunicación de la información generada por la entidad. Mantener operativo el hardware del FONDO DE BIENESTAR SOCIAL DE LA CGR.
- Auditoría: El área de sistemas del Fondo de Bienestar debe mantener la correcta operación del hardware y el software existente en las instalaciones del FONDO DE BIENESTAR SOCIAL DE LA CGR, incluyendo sus redes.

Políticas de comunicación con los interesados.

- Comunicación escrita a través de memorandos internos
- Comunicaciones a través de medios electrónicos “sistema de gestión documental, correo institucional”
- Certificaciones para recibos de satisfacción.
- Respuestas a quejas y reclamos.
- Informes de resultados.
- Informes de Gestión.

1.3 Contexto organizacional

Se entiende por contexto organizacional todo aquello que involucra a la organización, como sus objetivos, metas, y estrategias que piensa o está generando para lograrlo. A continuación se describe el contexto organizacional del área de sistemas del Fondo de Bienestar Social de la Contraloría General de la República en cuanto a actividad, meta y objetivo según manual de procedimientos entregado por la entidad.

Proyecto o actividad: Mantenimiento de primer nivel de la disponibilidad de los diferentes sistemas tanto a nivel hardware como software que pertenecen a las diferentes sedes del FONDO DE BIENESTAR SOCIAL DE LA CGR.

Meta: Asegurar la disponibilidad, integridad y confidencialidad de la información que procese, administre y sea entregada por los diferentes sistemas de información del FONDO DE BIENESTAR SOCIAL DE LA CGR en su sede Administrativa y el apoyo en el desarrollo de actividades en las sedes del Centro médico y del Colegio de la CGR.

Objetivo: Desarrollar políticas, planes, programas y proyectos relacionados con los sistemas de información que se deben utilizar al interior del Fondo, asesorar a las áreas en el manejo de los registros de la información, establecer procedimientos que permitan estandarizar los procesos y adoptar medidas de seguridad en todas las aplicaciones que se Implanten para permitir a los usuarios la integridad y funcionalidad de la información y asesorar a la Gerencia en la modernización, actualización y adquisición en nueva tecnología.

1.4 Contexto de la administración de riesgos

En este punto se busca contextualizar el escenario de la administración de riesgos; se identifican los procesos, productos o servicios que serán sometidos al proceso de administración de riesgos, y las áreas con las que se encuentran relacionados.

Después de revisado el manual de procesos y procedimientos del área de sistemas del Fondo de Bienestar social se concluye que esta área solamente maneja dos procedimientos: Administración y mantenimiento de las redes y equipos de cómputo de la sede Administrativa, brindando apoyo a las sedes del Centro médico y Colegio de la CGR, así mismo, se encuentra que está relacionado con el trámite de sistematización de la información y los procedimientos de la entidad como apoyo en la infraestructura requerida.

El segundo procedimiento es el soporte de primer nivel en software, en el cual se desarrollan actividades de soporte a los usuarios finales de la entidad.

1.5 Activos del área de sistemas.

A continuación se describen los activos con los que cuenta el área de sistemas del FONDO DE BIENESTAR SOCIAL DE LA CGR actualmente; en los siguientes cuadros se describen tanto los activos de hardware como los de software de las tres sedes.

Cuadro 1. Activos del área de sistemas sede Administrativa

ACTIVOS DEL AREA DE SISTEMAS	
No.	DESCRIPCIÓN
70	Equipos de cómputo de escritorio
2	Equipos de cómputo portátiles
3	Servidores con su correspondiente sistema operativo
3	Switchs de comunicaciones marca Tricom
3	Impresora de trabajo pesado
8	Impresoras monopuesto Hewllet Packard de varias referencias
1	Cableado estructurado de la red certificado bajo categoría 6A
1	Multifuncional Konika Minolta
	Herramientas de mantenimiento de hardware
	Herramientas de mantenimiento de software libres.

Cuadro 2 Activos sistemas sede Administrativa Medico

ACTIVOS DEL AREA DE SISTEMAS	
No.	DESCRIPCIÓN
17	Equipos de cómputo de escritorio
1	Servidores con su correspondiente sistema operativo
2	Switchs de comunicaciones
3	Impresoras monopuesto Hewllet Packard de varias referencias
1	Cableado estructurado de la red certificado bajo categoría 5e.
1	Ups de 20 KVA

Cuadro 3. Activos de sistemas sede Colegio de la CGR

ACTIVOS DEL AREA DE SISTEMAS	
No.	DESCRIPCIÓN
37	Equipos de cómputo de escritorio
1	Equipos de cómputo portátiles
1	Servidores con su correspondiente sistema operativo

1	Switchs de comunicaciones
2	Impresoras de trabajo pesado
1	Impresoras monopuesto Hewllet Packard de varias referencias
1	Ups de 20 KVA powertron
1	Fotocopiadora konika minolta
1	Escáner
	Herramientas de mantenimiento de hardware

El software con que cuenta el FONDO DE BIENESTAR SOCIAL DE LA CGR cumple con todos los requisitos de funcionalidad y legalidad establecidos por FEDESOFT, DIAN, agenda de conectividad, COINFO y el ente cabeza del sector (Contraloría General de la República); por tanto el FONDO DE BIENESTAR SOCIAL DE LA CGR cuenta con el software necesario para la realización de los procesos.

2. IDENTIFICAR RIESGOS

La identificación de riesgos consiste en detectar todos aquellos riesgos de la organización, independientemente de si se encuentran bajo control o no; es importante intentar que todos los riesgos sean identificados en esta parte del diagnóstico, ya que aquellos que no sean nombrados acá, quedarán excluidos del análisis posterior. A continuación, se muestran los riesgos identificados en el área de sistemas tanto en lo tecnológico, como en lo legal, político, de eventos naturales o actividades individuales.

FONDO DE BIENESTAR SOCIAL
CONTRALORÍA GENERAL DE LA REPÚBLICA
NIT. 800.252.683-3

		Determinación de Controles existentes		Matriz de análisis de Riesgos			
	RIESGOS	**¿EXISTE ALGUN CONTROL?**	**¿ES LO MÁS APROPIADO?**	**PROBABILIDAD**	**IMPACTO**	**NIVEL DE RIESGO**	TRATAMIENTO SUGERIDO
A	Incumplimiento de los acuerdos establecidos en los pliegos de contratación por parte de los proveedores y contratistas.	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.
B	Demoras en la gestión por parte de la	NO	No, este punto demuestra falta de relevancia para la	5	5	25	Aplicabilidad del manual de contratación de la

	administración en los trámites requeridos por el área de sistemas.		administración de los trámites por parte de la administración				entidad, Se realiza la mitigación del riesgo.
C	Disminución de la asignación de porcentaje del presupuesto asignado por parte de la Contraloría General de la República.	SI	Es el único control implementarle.	5	7	35	Redistribución de los recursos asignados a los proyectos de inversión y registro de nuevos proyectos ante el DNP, Se realiza la mitigación del riesgo a través del manejo de proyectos de inversión.
D	Aumento de la cartera morosa.	SI	Se hace seguimiento en el área de cartera con el fin de realizar su recuperación y disminuir este índice.	5	5	25	Ejecución de las cláusulas a los morosos con el fin de recuperar esta cartera. Se realiza la mitigación del riesgo, esta actividad

							corresponde al área financiera y al grupo de cartera de la entidad.
E	Disminución de los aportes entregados por los funcionarios.	SI	No, porque no se puede aplicar un control sobre el manejo de los aportes que cada funcionario quiera entregar.	3	5	15	Redistribución de fondos de funcionamiento. Se realiza la mitigación del riesgo.
F	Robo de información por parte de los funcionarios.	SI	Se encuentra bloqueado la copia de cd y dvs, 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	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

			momento que los funcionarios se llevan los datos para continuar con su trabajo fuera de las instalaciones de la entidad.				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.
G	Traslado de archivos en medios extraíbles	NO		10	7	70	Instalación de software de monitoreo de los equipos y bloqueo de accesos a USB, Se realiza la mitigación del riesgo.

H	Substracción de equipos.	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.
I	Terremotos	NO		3	10	30	Se transfiere el riesgo. Mediante las pólizas de seguros.

J	Tormentas eléctricas.	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.
K	Incendios.	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 administrativa y financiera.
L	Cambios a la normatividad en los procesos de contratación.	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.

M	Caída de los servidores	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 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	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 de apoyo tanto para los sistemas Windows, Linux, bases de datos y demás sistemas implementados en los servidores.

N	Ataques de virus, troyanos, gusanos y spyware.	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.
O	Mal diseño de la red de datos.	SI	No, porque se está utilizando software que no es el más funcional.	3	3	9	Revisión del plano lógico de la red de datos y diseñar los correctivos para solventar la falla en la transmisión de datos. Se realiza la

							mitigación del riesgo.
P	Desbalanceo de las cargas de la red eléctrica.	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 desbalanceo 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 desbalanceo y corregirlo mediante el balanceo de cargas sobre el tablero eléctrico. Se realiza la mitigación del riesgo.

Q	Desactualización de manuales y planes de contingencia	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.

R	Sabotaje a la red.	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 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.
S	Descontento de los funcionarios	NO		5	5	25	Realizar reuniones de concertación e identificar las causas y posibles fuentes de desconcierto 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.
T	Penetración indebida	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 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.
U	Cambio de las actividades establecidas en el manual de procesos.	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 actividades o procesos nuevos. Se realiza la mitigación del riesgo.
V	Pérdida de la información almacenada tanto en medio físico como en medio magnético y óptico.	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.
W	Falta de compromiso de los funcionarios responsables de las áreas en las cuales se utilizan los sistemas de información de la entidad	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.
X	Comunicaciones informales sobre el manejo y acceso a la información sin la debida documentación requerida ni el registro pertinente	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.

Y	Manejo indebido de los backup generados	NO		10	10	100	Se generara un documento para el manejo de los backup´s de igual manera se realizara las pruebas de eficiencia y se verificará la salvaguarda de dichas copias de respaldo, se mitiga el riesgo.
Z	Ingreso por parte de los funcionarios a páginas web no autorizas	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	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

			relevante para el desarrollo de las actividades al interior de la entidad.				entidad, se mitiga ese riesgo.
AA	Ejecución de software portable en la red de la entidad	SI	Existen restricciones desde las gpo implementadas en la red y en el sistema antivirus de la entidad. Más sin embargo hace falta definir la acción pertinente al momento de presentarse reiteración en la ejecución de aplicativos portables.	5	5	25	Se bloquea el acceso y ejecución de medios portables. Se mitiga este riesgo.

AB	Préstamo indebido de contraseñas token´s	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 CERTICAMARA S.A. 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.
AC	Debilidad en las contraseñas del aplicativo ALFANET	NO		10	3	30	Se solicitara al administrador del aplicativo el refuerzo de la seguridad de

							contraseñas, se mitiga este riesgo.
AD	El sistema ALFANET no se está utilizando por parte de los funcionarios de la entidad	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.
AE	La clasificación por organigrama dentro del aplicativo ALFANET no ha sido alimenta de forma adecuada	NO		10	3	30	Se solicita al administrador del aplicativo ALFANET el registro correcto de las dependencias y los niveles de accesos

							requeridos, se mitiga este riesgo.
AF	implementado la política de cero papel	NO		10	7	70	Se solicita al líder de implementación de GEL, los avances correspondientes, se mitiga este riesgo.
AG	Retraso de los procesos de contratación del área de sistemas	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.

AH	No obtener la revisión ni aprobación de los procedimientos externos para las solicitudes Departamento Nacional de planeación	NO		10	7	70	Generar los documentos en las fechas estipuladas y entregar al área de planeación para que adelante los trámites pertinentes. Este riesgo se Mitiga.
AI	Falta de avance en la implementación en la estrategia de Gobierno en Línea	NO		10	10	100	Solicitar a los Lideres de GEL y las profesionales de cada grupo el avance de las actividades estipuladas, Este riesgo se Mitiga.
AJ	Falta de personal de apoyo, No hay suficiente personal en el área de sistemas, esto implica una exceso en carga laboral de	NO		10	10	100	Solicitar un mayor número de personal para el área de sistemas, Este riesgo se Mitiga.

	la persona del área,						
AK	Manejo de información decentralizada	NO		10	10	100	Verificar la aplicabilidad de la norma de usabiulidad e igualdad tecnologica contemplada en GEL
AL	Aplicativo del Centro médico, sin una persona a cargo que tenga los conocimientos tanto de sistemas d einformación como manejo de aplicativos de salud y atención a pacientes	NO		10	10	100	Es necesario aplicar la normatividad vigente en cuento a la implementación de GEL en la entidad

AM	No existe una diferenciación en cuanto administración manejos, operatividad y funcionalidad de los aplciativos	NO		10	10	100	Es necesario establecer el nivel de jerarquias y responsabilidades en los aplicativos, se recomienda el cumplimiento de la NTC/ISO 27000 y sus subseries
AN	Centralización sobre el área de sistemas de los procedimeitnos, refernetes en los aplicativos de la entidad	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 manera es un alto riesgo

							mantener en una sola persona todo el control de los aplicativos

3. JERARQUIA DE APLICATIVOS

3.1 SEDE CENTRO MÉDICO:

El centro Médico cuenta con el aplicativo de gestión Médica parametrizado por la firma XIMIL TECHNOLOGIES. Este aplicativo cuenta con una base de datos desarrollado en sqlexpress. El mantenimiento de este aplicativo se ha realizado a través de contratos con la empresa XIMIL TECHNOLOGIES y la supervisión se canaliza a través de la dirección de desarrollo y bienestar, este aplicativo se encuentra fuera del NOC de la sede centro por este motivo su administración se realiza en el Centro Médico en cabeza de la Responsable de esta sede.

Se cuenta con 17 equipos Pc´s de escritorio los cuales se han instalado en atención al usuario, consultorios y laboratorios, conforme a los requerimientos del Responsable de esta sede. De estos 17 equipos todos fueron adquiridos hace un año con su software de ofimática licenciado, el antivirus es el MCAFEE END POINT licenciado para 250 nodos

3.2 SEDE COLEGIO DE LA CGR:

El Colegio de la CGR cuenta con un servidor, en este servidor se instaló el aplicativo SIIGO, en sus versiones académico y cartera, este aplicativo es propiedad del ingeniero Rodrigo Chávez, quien lo comercializa a través de la firma C3SISTEMAS. Se cuenta con el licenciamiento de utilización más no de modificación, por este motivo se han realizado contratos de mantenimiento con la firma C3 SISTEMAS para realizar los ajustes pertinentes. En la versión instalada en el Colegio de la CGR, se digita las notas por parte de los docentes para asegurar la veracidad de los datos ingresados al sistema, se cuenta con un esquema de seguridad usuario contraseña, la coordinadora académica administra el módulo académico de SIIGO, mientras que la parte de cartera es administrada por la secretaría General del Colegio. El sistema cuenta con una base de datos desarrollada en Access. El sistema operativo de este servidor es Windows server 2008 R2 de 64 Bits, con el antivirus, en este equipo se encuentra el dominio COLCGR. Este aplicativo se encuentra fuera del NOC de la sede centro por este motivo su administración se realiza en el Colegio

de la CGR y es responsabilidad de la Responsable de esta sede, quien canaliza los requerimientos de los usuarios finales y se encarga de los trámites para su mantenimiento. El aplicativo SIIGO no tiene conexiones salientes en la versión que se encuentra instalada, el acceso y registro de información se realiza en la sede del Colegio de la CGR.

Se cuenta con 37 equipos nuevos todos ellos licenciados con win seven de 32 Bits, antivirus mcafee 8.8 y office 2010, adquiridos mediante contrato 017 de 2010, a través del proyecto de modernización de la entidad.

SEDE ADMINISTRATIVA:

La sede administrativa cuenta con 3 servidores todos ellos con un sistema operativo windows server 2008 R2 Y SERVER 2012 R2 en los cuales se tiene los siguientes aplicativos:

Servidor Athenea; Servidor del ANTIVIRUS, Cuenta con una base de datos MYSQL.

Servidor Dedalo; Servidor de segundo Backup, servidor de impresoras y consola de actualizaciones del sistema operativo. Este servidor se encarga de administrar las impresoras y las actualizaciones de los sistemas operativos Windows de la sede centro.

Servidor POSEIDON; Servidor del Dominio, este servidor se encarga de la administración de los usuarios y permisos de acceso a los recursos de la sede centro.

Servidor EREBO; Servidor de backup del Dominio, este servidor se encarga de a replicación del servidor de dominio y maneja el DHCP y la primera copia de los backups

DATACENTER EXTERNO

Servidor Morpheo: Servidor de Tao “sistema financiero”, se cuenta con el licenciamiento de utilización del aplicativo TAO sistemas de información LTDA, ese aplicativo corre con una base de datos desarrollada en ORACLE 10G licenciado por procesador. Con el proceso de

virtualización se han separado en cuatro, dos servidores de aplicaciones con balanceador por aplicación, un servidor de base de datos y un servidor proxy.

Servidor Hermes: Servidor de ALFANET “sistema de gestión documental” desarrollado por ARCHIVAR LTDA. Aplicación licenciada para 150 usuarios desarrollada en .net framework, cuenta con una base de datos sqlexpress, esta aplicación es administrada por gestión documental quien posee cuentas administradoras para la creación, modificación de usuarios, esta aplicación es tipo web la cual puede ser visualizada a través de la dirección IP en la sede del centro médico y Colegio de la CGR por los usuarios que se encuentren registrados en el aplicativo

Servidor HADES; servidor de nómina se ha instalado el sistema SIGEP, el cual tiene una base de datos Oracle 11G a 64 Bits y el sistema operativo de este servidor es Windows server 2008 R2 64 Bits.

Servidor gestión médica, sistema Ubuntu 16, software instalado gestión médica.

El software instalado en las diferentes sedes del Fondo de Bienestar Social de la CGR instalado por la oficina de sistemas se encuentra licenciado, las aplicaciones que se encuentran sin licenciar son desinstaladas para no incurrir en violación de derechos de autor.

En cada sede se ha montado un sistema de Dominio por lo tanto se debe priorizar la atención de incidencias por sede.

4. REQUERIMIENTOS DE RECUPERACIÓN

SEDE ADMINISTRATIVA;

Software	Recurrencia de fallos	impacto	Contingencia	Estrategia de mitigación - recuperación	Tiempo empleado de recuperación	Acciones de mejora

Sistema Financiero (Crédito y cartera)	20 % Menos de 2 al año	Alto	Reinstalación según manual	Utilización de virtualización	1 Día	Cambio a versiones WEB del aplicativo Adquisición de un nuevo servidor de respaldo para implementar sistema de alta disponibilidad
	10 % Menos de un fallo	Alto	Importación de máquina virtual, esta máquina se genera una vez al mes	Plataforma de virtualización	4 Horas	Implementación de la redundancia del sistema virtual
Sistema Talento Humano SIGEP	20 % Menos de 1 al año	Alto	Reinstalación según manual	Realización de copias- Virtualización	1 Día	Adquisición de un nuevo servidor de respaldo para implementar sistema de alta disponibilidad
	10 % Menos de un fallo	Alto	Importación de máquina virtual, esta máquina se genera una vez al mes	Plataforma de virtualización	4 Horas	Implementación de la redundancia del sistema virtual
Sistema ALFANET	20 % Menos de 2 al año	Alto	Reinstalación según manual	Realización de copias- Virtualización	1 Día	Realización de virtualización
	10 % Menos de un fallo	Alto	Importación de máquina virtual, esta máquina se genera una vez al mes	Plataforma de virtualización	4 Horas	Implementación de la redundancia del sistema virtual
Portal Institucional	10 % Menos de 1 al año	Alto	Tercerizado, Acuerdos de Nivel de servicio 99,6% de disponibilidad	Realización de BAckups - Virtualización	4 Horas	

	10 % Menos de un fallo	Alto	Importación de máquina virtual, esta máquina se genera una vez al mes	Plataforma de virtualización	1 Horas	Puesta en servicio del sitio alterno conforme a los parámetros contratados por la empresa MICROSITIOS
Sistema de Dominio	10 % Menos de 1 al año	Alto	Realización de backups – utilización de segundo servidor de respaldo	Aumento en la frecuencia de los backup´s e implementación del esquema de virtualización	2 Horas	Redistribución de roles en dos equipos e importación del export de la máquina
Sistema Antivirus	10 % Menos de 1 al año	Moderado	Reinstalación según manual	Realización de copias-Virtualización	1Hora	Instalación de la réplica automática y el balanceo de aplicaciones

SEDE CENTRO MÉDICO;

Software	Recurrencia de fallos	impacto	Contingencia	Estrategia de mitigación	Tiempo empleado de recuperación	Acciones de mejora
Sistema Gestión Médica	20 % Menos de 2 al año	Alto	Reinstalación según manual	Import de la máquina con el apoyo del contratista y su sito alterno de servicios	2 Horas	Ajuste de la transferencia de los backups diarios
Sistema dominio	20 % Menos de 2 al año	Alto	Reinstalacion según manual	Realización de copias-	1 Día	Adquisición de un segundo

				Virtualización		servidor de respaldo
Sistema antivirus	10 % Menos de 1 al año	Moderado	Reinstalacion según manual	Realización de copias-Virtualización	1 Hora	Ajuste de la replicación

SEDE COLEGIO CGR;

Software	Recurrencia de fallos	impacto	Contingencia	Estrategia de mitigación	Tiempo empleado de recuperación	Acciones de mejora
Sistema de Gestión Académica	10 % Menos de 1 al año	Alto	Reinstalacion según manual	Utilización de virtualización	1 Día	Se contempla el outsorcing del aplicativo o su tercerización
Sistema de Dominio	10 % Menos de 1 al año	Alto	Reinstalacion según manual	Realización de copias-Virtualización	1 Día	Adquisición de un segundo servidor de respaldo
Sistema Antivirus	10 % Menos de 1 al año	Moderado	Reinstalacion según manual	Realización de copias-Virtualización	1 Día	Realización de virtualización

5. EJECUCION

SEDE ADMINISTRATIVA;

Software	Programación de pruebas	Medios de prueba	Recursos a utilizar	Responsable
Sistema Financiero TAO.	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Área de sistemas
Sistema Talento Humano SIGEP	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Área de sistemas
Sistema ALFANET	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Área de sistemas
Portal Institucional	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Área de sistemas
Sistema de Dominio	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Área de sistemas
Sistema Antivirus	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Área de sistemas

SEDE CENTRO MÉDICO;

Software	Programación de pruebas	Medios de prueba	Recursos a utilizar	Responsable
Sistema Gestión Médica	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Responsable del Colegio - contratista XIMIL TECHNOLOGIES
Sistema dominio	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Responsable del Centro médico - Apoyo Área de sistemas
Sistema antivirus	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Responsable del Centro médico - Apoyo Área de sistemas

SEDE COLEGIO CGR;

Software	Programación de pruebas	Medios de prueba	Recursos a utilizar	Responsable
Sistema de Gestión Académica	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Responsable del Colegio - Contratista C3 sistemas
Sistema de Dominio	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Responsable del Colegio - Apoyo Área de sistemas
Sistema Antivirus	Dos al año	Virtualización en equipos de prueba	Manuales de instalación – equipo servidor de virtualización	Responsable del Colegio - Apoyo Área de sistemas

Los manuales de instalación han sido verificados e cuanto a su operación, es necesario actualizar las contingencias para la virtualización con herramientas GNU con las cuales se puede implementar procedimientos contingencias temporales.

6. DOCUMENTOS DE REFERENCIA MEDIOS DIGITALES;

Manuales de instalación de aplicativos, se mantienen en las carpetas digitales.

ALEX WILLIAM JOJOA FERNANDEZ
PROFESIONAL ESPEIALIZADO G14
ÁREA DE SISTEMAS
FONDO DE BIENESTAR SOCIAL DE LA CGR