

		DETERMINACIÓN DE CONTROLES EXISTENTES							MATRIZ DE ANALISIS DE RIESGOS				ANALISIS DE MITIGACIÓN EJECUCIÓN DEL CONTROL (RESIDUAL) ANÁLISIS A 30/7/2021				PLANTEAMIENTO DE AJUSTE
ITEM	RIESGOS	TIPO	PILAR AFECTADO NORMA 27000	¿EXISTE ALGUN CONTROL?	¿ES LO MÁS APROPIADO?	PROBABILIDAD	IMPACTO	NIVEL RESGO	DE	TRATAMIENTO SUGERIDO	FECHA DE INICIO	FECHA DE FIN	RESPONSABLE DE LA EJECUCIÓN	PROBABILIDAD	IMPACTO	NIVEL DE RESGO	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	5	5	25	25	Ejecución de los Acuerdos de Nivel de Servicio o los acuerdos contemplados en la ley 805 referente a contratación estatal. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Supervisor de contrato				
2	Quemas en la gestión por parte de la administración en los sistemas requeridos por el área de sistemas.	humano - administrativo	Integridad - Seguridad	-	SI	5	5	25	25	Se ajusta el manual y se ha dado ordenada a los procesos. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Dirección Administrativa				
3	Disminución de los recursos asignados al área de sistemas	humano - administrativo	Integridad - Seguridad	-	SI	5	7	35	35	Redistribución de los recursos asignados al FRS	1.02/2021	30/12/2021	Dirección Administrativa				
4	Disminución de los agentes entregados por los funcionarios.	humano - administrativo	Integridad - Seguridad	-	SI	3	5	15	15	Redistribución de los recursos asignados al FRS	1.02/2021	30/12/2021	Dirección Administrativa				
5	Robo de información por parte de los funcionarios.	humano - seguridad	Integridad - Seguridad	-	SI	5	7	35	35	Restricción de los medios de almacenamiento mediante chequeos periódicos. Revisión de la información subarrendada 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 penetración de políticas de manejo de la información generada, entregada y manipulada en la entidad.	1.02/2021	30/12/2021	Profesional área de sistemas				
6	Traslado de archivos en medios extraíbles	humano - seguridad	Integridad - Seguridad	-	SI	3	3	9	9	Resolución de software de monitoreo de los equipos y bloqueo de accesos a USB. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Profesional área de sistemas				
7	Substracción de equipos.	seguridad	Integridad - Seguridad	-	SI	3	2	6	6	Revisión del sistema de cámaras de seguridad y registro de acceso con el fin de determinar la ruta por la cual los equipos fueron extraídos 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.	1.02/2021	30/12/2021	Supervisor del contrato				
8	Terremotos	Naturaliza	Integridad - Seguridad	-	NO	3	10	30	30	Se transfiere el riesgo. Mediante las pólizas de seguros.	1.02/2021	30/12/2021	Dirección Administrativa				
9	Tormentas eléctricas.	Naturaliza	Disponibilidad	-	NO	5	5	25	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.	1.02/2021	30/12/2021	Dirección Administrativa - Recursos Físicos				
10	Incendios.	Naturaliza agentes humano agentes externo	Disponibilidad	-	NO	5	10	50	50	Se realiza 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.	1.02/2021	30/12/2021	Dirección Administrativa - Recursos Físicos				
11	Cambios a la normalidad en los procesos de contratación.	Normativo	Integridad - Seguridad	-	SI	3	3	9	9	Mediante la actualización de los requerimientos presentados en la normalidad vigente se adaptan documento y procedimientos del área.	1.02/2021	30/12/2021	Profesional área de sistemas				
12	Caída de los servidores	Software administrativo	Integridad - Seguridad	-	SI	5	10	50	50	Realizar la correspondiente revisión de la normalidad modificada con el fin de verificar el impacto sobre los procesos existentes y si resultan ser afectados aplicar procedimientos excepcionales. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Profesional área de sistemas				
13	Ataques de virus, troyanos, gusanos y spyware.	Seguridad	Integridad - Seguridad	-	SI	2	3	6	6	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.	1.02/2021	30/12/2021	Profesional área de sistemas - Empresa soporte				
14	Mal diseño de la red de datos.	Infraestructura	Disponibilidad	-	SI	3	3	9	9	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 la contención hasta lograr eliminarla de los equipos. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Empresa de soporte				
15	Desbalanceo de las cargas de la red eléctrica.	Infraestructura	Disponibilidad	-	SI	5	5	25	25	Revisión del plano lógico de la red de datos y diseñar los correctivos para solucionar la falla en la transmisión de datos. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Dirección Administrativa - Recursos Físicos				
16	Desactualización de manuales y planes de contingencia	Administrativo integridad	Integridad - Seguridad	-	SI	5	5	25	25	Identificar la fuente del desbalanceo de cargas y redistribuirlos a fin de evitar caídas en el sistema. De presentarse caídas iniciar la secuencia de respaldo para identificar la fuente del desbalanceo y corregirlo mediante el balanceo de cargas sobre el cableado eléctrico. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Dirección Administrativa - Recursos Físicos				
17	Sabotaje a la red.	Seguridad	Integridad - Seguridad	-	SI	5	5	25	25	Revisión de los procesos o identificación de los fallos de los manuales y los planes de contingencia de cada proceso con el fin de asegurar la continuidad del servicio, de no existir el manual ni el plan de contingencia este debe ser desarrollado. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Profesional área de sistemas				
18	Descontento de los funcionarios	Humano	Integridad - Seguridad	-	NO	5	5	25	25	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 avances del sabotaje con base en estos avances determinar la acción a tomar. Si es a nivel físico realizar la investigación para identificar a la persona responsable de la acción y tomar 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.	1.02/2021	30/12/2021	Profesional área de sistemas				
19	Penetración indebida	Seguridad	Integridad - Seguridad	-	SI	5	5	25	25	Realizar reuniones de concertación e identificar las causas y posibles fuentes de descontento 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.	1.02/2021	30/12/2021	Alta Gerencia				
20	Cambio de las actividades establecidas en el manual de procesos.	Administrativo	Disponibilidad	-	NO	3	3	9	9	Identificar el punto de acceso y determinar el grado de complejidad 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.	1.02/2021	30/12/2021	Profesional área de sistemas - alta gerencia				
21	Pérdida de la información almacenada tanto en medio físico como en medio magnético y digital.	Seguridad integridad	Seguridad	-	SI	10	7	70	70	Se debe realizar el ajuste de las normas de seguridad a las nuevas actividades, de ser necesario se deben ajustar los niveles de seguridad a actividades o procesos nuevos. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Dirección administrativa y financiera				
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 - Seguridad	-	NO	5	10	50	50	Identificar la causa y de ser posible la restauración de la información de las copias de seguridad. Se realiza la mitigación del riesgo.	1.02/2021	30/12/2021	Profesional área de sistemas				
23	Comunicaciones informales sobre el manejo y acceso a la información sin la debida documentación regada en el registro pertinente	Procedimientos	Integridad - Seguridad	-	SI	5	7	35	35	Se debe adoptar reuniones de concertación sobre la importancia del manejo adecuado de la información e identificar las posibles fallas en los procesos y determinar la responsabilidad de los funcionarios en el proceso, se mitiga el riesgo.	1.02/2021	30/12/2021	Dirección administrativa y financiera - Talento Humano				
24	Manejo indebido de los backup generados	Procedimientos disponibilidad	Seguridad	-	SI	5	7	35	35	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 correo electrónico, se mitiga este riesgo.	1.02/2021	30/12/2021	Alta Gerencia				
25	Ingreso por parte de los funcionarios a páginas web no autorizadas	Seguridad	Integridad - Disponibilidad	-	SI	5	3	15	15	Se genera un documento para el manejo de los backup's de nivel preventivo se validan los niveles de eficiencia y se verificará la salvaguarda de dichas copias de respaldo, se mitiga el riesgo.	1.02/2021	30/12/2021	Dirección administrativa y financiera				
26	Ejecución de software portable en la red de la entidad	Seguridad	Disponibilidad - Seguridad	-	SI	5	5	25	25	Se aplican bloqueos a través del sistema firewall y sistema antivirus, de permitirse el acceso indebido se procederá con el informe de esta situación a la dirección administrativa y financiera de la entidad, se mitiga este riesgo.	1.02/2021	30/12/2021	Profesional especializado área de sistemas				
27	Préstamo indebido de contraseñas token's	Humano	Integridad - Seguridad	-	SI	10	7	70	70	Se bloquea el acceso y ejecución de medios portables. Se mitiga este riesgo.	1.02/2021	30/12/2021	Profesional especializado área de sistemas				
28	Debilidad en las contraseñas del aplicativo ALFANET	Seguridad	Integridad	-	SI	5	3	15	15	El control del uso de este elemento debe ir 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 igualmente en el funcionario que tiene asignado el token o certificado de firma digital.	1.02/2021	30/12/2021	Funcionarios				
29	Debilidad en las contraseñas del aplicativo ALFANET	Seguridad	Integridad	-	SI	5	3	15	15	Como responsabilidad de los usuarios finales de los token's, en cualquier caso de usuarios se realizará un comunicado para dar a conocer los riesgos del préstamo y las implicaciones que conlleva esta actividad, se mitiga el riesgo.	1.02/2021	30/12/2021	Funcionarios - proveedor autorizado				

FONDO DE BIENESTAR SOCIAL CONTROLORA GENERAL DE LA REPUBLICA NIT. 900.252.683-3			DETERMINACIÓN DE CONTROLES EXISTENTES		MATRIZ DE ANALISIS DE RIESGOS					ANALISIS DE MITIGACIÓN EJECUCIÓN DEL CONTROL (RESIDUAL) ANÁLISIS A 18/10/2021				PLANTEAMIENTO DE AJUSTE		
ITEM	RIESGOS	TIPO	PLAR AFECTADO NORMA 27000	¿EXISTE ALGUN CONTROL?	¿ES LO MAS APROPIADO?	PROBABILIDAD	IMPACTO	NIVEL RIESGO	DE TRATAMIENTO SUGERIDO	FECHA DE INICIO	FECHA DE FIN	RESPONSABLE DE LA EJECUCIÓN	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	MITIGACIÓN PUNTUAL
29	El sistema ALFANET no se está utilizando por parte de los funcionarios de la entidad	Gestión	Integridad - Disponibilidad	SI	Con la entrada en producción de plantillas de respuestas y el uso de la aplicación de manera formal el sistema se encuentra en uso.	5	5	25	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.	1/02/2021	30/12/2021	Dirección administrativa y financiera				
30	La clasificación por organigrama dentro del aplicativo ALFANET no ha sido adecuada de forma adecuada	Administrativo	Disponibilidad	NO		10	3	30	Se solicita al administrador del aplicativo ALFANET el realice el correcto de las dependencias y los niveles de acceso de usuarios en el sistema.	1/02/2021	30/12/2021	Dirección administrativa y financiera				
31	Implementado la política de cero papel	Administrativo	Integridad - Disponibilidad - Seguridad	SI	SI, el software ALFANET se utiliza como medio de transmisión de documentos de trabajo en la entidad	5	7	35	Se solicita al administrador del aplicativo ALFANET el realice el correcto de las dependencias y los niveles de acceso de usuarios en el sistema.	1/02/2021	30/12/2021	Dirección administrativa y financiera				
32	Retraso de los procesos de contratación del área de sistemas	Administrativo	Disponibilidad	SI	SI, la revisión del PAA asegura la ejecución de los procesos	5	7	35	Este riesgo a pesar de ser identificado y de cumplir con los límites al interior de la entidad solo se puede mitigar con el apoyo de la dirección administrativa y financiera y el apoyo del personal de contratación.	1/02/2021	30/12/2021	Dirección administrativa y financiera				
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 los profesionales de cada grupo el avance de las actividades estipuladas. Este riesgo se Mitiga.	1/02/2021	30/12/2021	Alta Gerencia				
34	Falta de personal de apoyo. No hay suficiente personal en el área de sistemas, esto implica un exceso en carga laboral de los equipos de área.	Administrativo	Disponibilidad	NO		10	10	100	Solicitar un mayor número de personal para el área de sistemas. Este riesgo se Mitiga.	1/02/2021	30/12/2021	Dirección administrativa y financiera				
35	Manejo de información descentralizada	Administrativo	Integridad - Seguridad	NO		10	10	100	Verificar la aplicabilidad de la norma de usabilidad e igualdad tecnológica contemplada en la política.	1/02/2021	30/12/2021	Direcciones - alta gerencia				
36	Aplicativo del Centro médico, sin una persona a cargo que tenga los conocimientos tanto de sistemas d información como manejo de aplicativos de salud y atención a pacientes	Administrativo	Integridad - Disponibilidad - Seguridad	NO		10	10	100	Es necesario aplicar la normatividad vigente en cuanto a la implementación de la política.	1/02/2021	30/12/2021	Dirección de desarrollo y bienestar				
37	No existe una diferenciación en cuanto administración, manejo, operatividad y funcionalidad de los aplicativos	Administrativo	Integridad - Seguridad	SI	Según la resolución 413 de 2019 se desagregaron la funciones en los usuarios operativos y de seguridad	5	7	35	Es necesario establecer el nivel de jerarquías y responsabilidades en los aplicativos, se recomienda el cumplimiento de la NTC 8559:2020 y sus subsistemas.	1/02/2021	30/12/2021	Direcciones - alta gerencia				
38	Centralización sobre el área de sistemas de los procedimientos, referidos en los aplicativos de la entidad	Administrativo	Integridad - Disponibilidad - Seguridad	SI	Según la resolución 413 de 2019 se desagregaron la funciones en los usuarios operativos y de seguridad	5	7	35	No existe un documento que defina los roles administrativos, operativos, funcionales, auditoría 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.	1/02/2021	30/12/2021	Alta Gerencia				