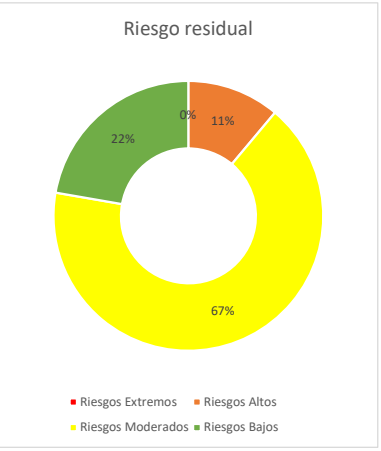
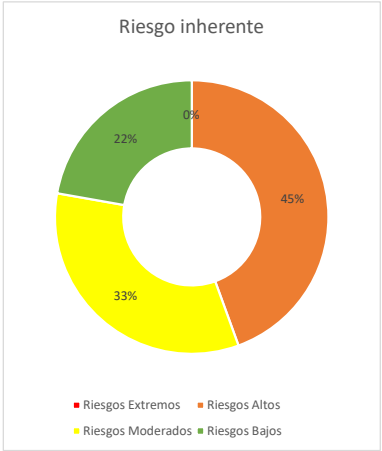


IDENTIFICACIÓN DEL ACTIVO					IDENTIFICACIÓN DEL RIESGO			VALORACIÓN DEL RIESGO			TRATAMIENTO DEL RIESGO		DISMINUCIÓN DE PROBABILIDAD E IMPACTO			
Proceso	Activo	Clasificación		Criticidad	Nro.	Riesgo	Clasificación	Probabilidad	Impacto	Riesgo Inherente	Opción de Manejo	Actividad de Control	Probabilidad	Impacto		Riesgo Residual
		Ley 1712 de 2014	Ley 1581 de 2012	Nivel de Criticidad												
SISTEMAS DE INFORMACIÓN Y GESTIÓN DOCUMENTAL	Hardware	Información Pública	Datos sensibles	Alta	1	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica	Tecnológicos	Probable	Moderado	ALTA	REDUCIR	* Renovación anual del sistema Firewall (Fortigate). * Renovación anual de la licencia de antivirus. * Renovación tecnológica. Cambio de los equipos de cómputo cuyo sistema operativo se encuentra obsoleto. * Renovación tecnológica. Renovación de la plataforma de servidores institucionales que se encuentran obsoletos. * Evaluar nuevas herramientas para el control de ataques informáticos. * Registro de actividades. Realización de contratos de soporte con Acuerdos de Niveles de Servicios (ANS) establecidos con los proveedores del Sistema de Información	Posible	Insignificante	PosibleInsignificante	BAJA
	Software	Información Clasificada	Datos sensibles	Media	2	Robo, alteración y/o pérdida de Información de la Entidad por robo informático	Seguridad digital	Rara vez	Mayor	ALTA	REDUCIR	* Renovación anual del sistema Firewall (Fortigate). * Renovación anual de la licencia de antivirus. * Renovación tecnológica. Cambio de los equipos de cómputo cuyo sistema operativo se encuentra obsoleto. * Renovación tecnológica. Renovación de la plataforma de servidores institucionales que se encuentran obsoletos. * Campañas de sensibilización en cuanto a seguridad informática. * Evaluar nuevas herramientas para el control de ataques informáticos. * Registro de actividades. Realización de contratos de soporte con Acuerdos de Niveles de Servicios (ANS) establecidos con los proveedores del Sistema de Información	Rara vez	Moderado	Rara vezModerado	MODERADA
	Software	Información Clasificada	Datos sensibles	Media	3	Acceder a la información de manera fraudulenta	Seguridad digital	Rara vez	Moderado	MODERADA	REDUCIR	* Segregación de funciones y controles de acceso * Política y procedimiento de copias de respaldo de la información	Rara vez	Moderado	Rara vezModerado	MODERADA
	Software	Información Clasificada	Datos sensibles	Media	4	Ingresos no autorizados físicos/Digitales	Seguridad digital	Rara vez	Insignificante	BAJA	EVITAR	* Segregación de funciones y controles de acceso * Política y procedimiento de copias de respaldo de la información	Rara vez	Moderado	Rara vezModerado	MODERADA
	Software	Información Reservada	Datos sensibles	Media	5	Falta de presupuesto para la renovación de la infraestructura tecnológica, lo que genera contar con infraestructura obsoleta e incompatibilidad con nuevas tecnologías.	Seguridad digital	Posible	Menor	MODERADA	REDUCIR	* Toma de conciencia, educación y formación en la seguridad de la información. * Plan de Sensibilización	Rara vez	Moderado	Rara vezModerado	MODERADA
	Software	Información Clasificada	Datos sensibles	Media	6	Cifrado no autorizado de la información por malware o acción mal intencionada	Seguridad digital	Probable	Moderado	ALTA	EVITAR	* Política y procedimiento de protección frente a software malicioso * Plan de capacitación y formación de empleados	Rara vez	Moderado	Rara vezModerado	MODERADA
	Software	Información Clasificada	Datos sensibles	Media	7	Ataque dirigido con el intención de interrumpir los servicios que se ejecutan en un servidor Ingeniería Social	Seguridad digital	Rara vez	Menor	BAJA	EVITAR	* Política y procedimiento de protección frente a software malicioso * Plan de capacitación y formación de empleados	Rara vez	Moderado	Rara vezModerado	MODERADA

	Intangibles	Información Reservada	Datos sensibles	Media	8	Entrega indebida de la información Daño en componentes tecnológicos Pérdida de Integridad de la información digital almacenada, procesada y manejada en los sistemas de información utilizados en el proceso.	De imagen	Posible	Menor	MODERADA	REDUCIR	* Gestionar conocimiento al personal nuevo que requiera creación de usuarios en las herramientas tecnológicas para garantizar una adecuada gestión y control de acceso. * Brindar capacitación en el alcance de la herramienta tecnológica a la cual tendrá acceso, denotando los controles de seguridad de la información que brinda la herramienta.	Rara vez	Menor	Rara vezMenor	BAJA
	Gestión del Conocimiento	Información Pública	Datos sensibles	Media	9	Pérdida de conocimiento institucional por la alta rotación de personal y no contar con mecanismos para capturar y materializar el conocimiento tácito. Pérdida de Integridad de la información digital almacenada, procesada y manejada en los sistemas de información utilizados en el proceso.	De imagen	Posible	Moderado	ALTA	EVITAR	El jefe inmediato, cada vez que se presenta el retiro de un funcionario de la entidad y con el fin recopilar el conocimiento, verifica y aprueba la información registrada en el informe. En caso de no entregar la información requerida, no se procederá a realizar la liquidación correspondiente. Como evidencia queda el informe firmado por el jefe inmediato.	Probable	Moderado	ProbableMod erado	ALTA

Riesgo inherente	
Riesgos Extremos	0
Riesgos Altos	0
Riesgos Moderados	0
Riesgos Bajos	0
TOTAL	0

Riesgo residual		
Riesgos Extremos		0
Riesgos Altos		0
Riesgos Moderados		0
Riesgos Bajos		0
TOTAL		0

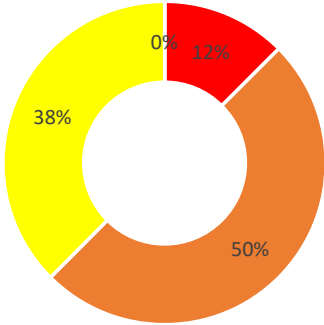


IDENTIFICACION DEL ACTIVOS		IDENTIFICACIÓN DEL RIESGO		VALORACIÓN DEL RIESGO			TRATAMIENTO DEL RIESGO		DISMINUCIÓN DE PROBABILIDAD E IMPACTO		
Proceso	Nro.	Riesgo	Clasificación	Probabilidad	Impacto	Riesgo Inherente	Opción de Manejo	Actividad de Control	Probabilidad	Impacto	Riesgo Residual
PROCESOS MISIONALES	1	Posibilidad de realizar cobros no autorizados a los usuarios para facilitar el acceso o prestación de un	De corrupción	Improbable	Mayor	ALTA	EVITAR	Restricción de permisos por usuarios del aplicativo de HC electronica Auditoria de trámites realizados por los usuarios	Casi seguro	Menor	ALTA
TALENTO HUMANO	2	Posibilidad de alteración de los documentos de las hojas de vida para acceder a un cargo	De corrupción	Rara vez	Mayor	ALTA	REDUCIR	Organización y custodia de las hojas de vida en el archivo exclusivo de talento humano Verificación de antecedentes disciplinarios y penales Verificación de veracidad del documentos como estudios y experiencia laboral acreditada	Rara vez	Menor	BAJA
	3	Posibilidad de recibir o solicitar dádiva o beneficio por direccionamiento de vinculación en favor propio o de un tercero.	De corrupción	Improbable	Moderado	MODERADA	REDUCIR	Documentar proceso de vinculación frente a cada una de las etapas.	Rara vez	Insignificante	BAJA
SISTEMAS DE INFORMACIÓN Y GESTIÓN DOCUMENTAL	4	Posibilidad de recibir o solicitar cualquier dádiva para la adquisición de bienes y servicios del proceso de tecnologías con el fin de beneficiarse a nombre propio o de terceros	De corrupción	Improbable	Moderado	MODERADA	REDUCIR	Evaluación de proveedores Aplicación de requisitos para seleccionar proveedores Solicitud de cotizaciones para selección de proveedor Seguimiento al proceso de contratación	Posible	Insignificante	BAJA

IDENTIFICACION DEL ACTIVOS		IDENTIFICACIÓN DEL RIESGO		VALORACIÓN DEL RIESGO			TRATAMIENTO DEL RIESGO		DISMINUCIÓN DE PROBABILIDAD E IMPACTO		
Proceso	Nro.	Riesgo	Clasificación	Probabilidad	Impacto	Riesgo Inherente	Opción de Manejo	Actividad de Control	Probabilidad	Impacto	Riesgo Residual
FINANCIERA	5	Posibilidad de modificación y/o alteración de la información financiera	De corrupción	Rara vez	Moderado	MODERADA	EVITAR	Modificaciones sujetas a aprobación de gerencia y revisoría fiscal	Rara vez	Moderado	MODERADA
	6	Posibilidad de robo de efectivo o cibernéticos	De corrupción	Posible	Moderado	ALTA	EVITAR	Control de recaudo de cajas mediante generación de informe y auditorías de tesorería	Rara vez	Moderado	MODERADA
	7	Posibilidad de no facturación de servicio o no cobro de copagos	De corrupción	Posible	Mayor	EXTREMA	EVITAR	Auditorías de proceso de facturación	Rara vez	Mayor	ALTA
RECURSOS FISICOS Y BIOMEDICOS	8	Posibilidad de favorecer la adquisición de proveedores específicos	De corrupción	Rara vez	Mayor	ALTA	EVITAR	Evaluación de proveedores Aplicación de requisitos para seleccionar proveedores Solicitud de cotizaciones para selección de proveedor a través de la plataforma OKA SYSTEM Seguimiento a las personas encargadas de la adquisición de	Rara vez	Mayor	ALTA
				Riesgo inherente				Riesgo residual			
				Riesgos Extremos		1		Riesgos Extremos		0	
				Riesgos Altos		4		Riesgos Altos		3	
				Riesgos Moderados		3		Riesgos Moderados		2	
				Riesgos Bajos		0		Riesgos Bajos		3	
				TOTAL		8		TOTAL		8	

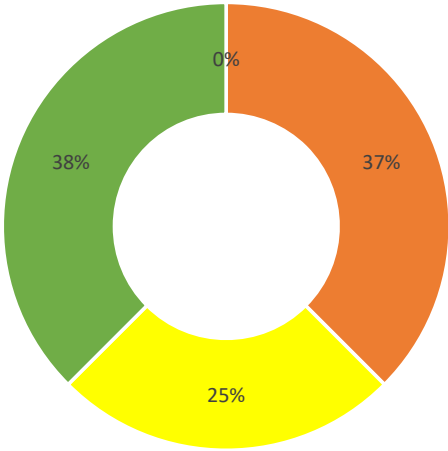
IDENTIFICACION DEL ACTIVOS		IDENTIFICACIÓN DEL RIESGO		VALORACIÓN DEL RIESGO			TRATAMIENTO DEL RIESGO		DISMINUCIÓN DE PROBABILIDAD E IMPACTO		
Proceso	Nro.	Riesgo	Clasificación	Probabilidad	Impacto	Riesgo Inherente	Opción de Manejo	Actividad de Control	Probabilidad	Impacto	Riesgo Residual

Riesgo inherente



- Riesgos Extremos
- Riesgos Altos
- Riesgos Moderados
- Riesgos Bajos

Riesgo residual



- Riesgos Extremos
- Riesgos Altos
- Riesgos Moderados
- Riesgos Bajos