Ficha Registro de Riesgos

Riesgo	Posibilidad de pérdida reputacional por quejas de grupos de valor y/o sanciones de entes de control debido a pérdida de Integridad (modificación no autorizada) de la información o configuración de los servicios gestionados por la OTIC causados por posible ataque informático, falla eléctrica, errores de configuración, error humano en la aplicación de procedimientos, falla tecnológica, vulnerabilidades conocidos o desconocidos en el software y hardware	**Código No.**	053
Tipo	Seguridad Digital	**Proceso**	Tecnologías de la Información

Zona Inherente		Controles	Responsable	Zona Residual
Riesgo Alto	**4**	El jefe de la Oficina de TIC convoca el comité de crisis, cuando se presente un incidente o evento potencial de seguridad de la información para gestionar de manera efectiva y oportuna los incidentes de seguridad # El profesional encargado del manejo de los certificados digitales asociados a los sistemas de información y portales, verifica oportunamente la vigencia e implementación de los mismos, con el fin de mantener la autenticidad, integridad y garantizar la confidencialidad de la información de las plataformas tecnológicas en las que están instalados los sistemas. # El coordinador del grupo de servicios de TI en conjunto con los líderes técnicos de los sistemas o servicios de información evalúan y ajustan las solicitudes de cambio para garantizar que estos cuando se implementen no afecten la integridad y disponibilidad de la información. # El profesional asignado valida y aplica parches y acciones de	hsanchez # evargas # hsanchez # evargas	**Riesgo Moderado**
		Periodicidad reporte:		**TRIMESTRAL**

	Actividades de Control	Responsable
1	El jefe de la OTIC se encarga de gestionar la adquisición de servicios de soporte sobre las plataformas de los sistemas de información.	hsanchez