PROCESO:	Administración de sistemas de información	TIPO DE PROCESO:		MACROPROC	
OBJETIVO:					N.A.

IDENTIFICACIÓN							RIESGO INHERENTE					CRITERIOS ERICA (Evitar, Reducir, Compartir, Asumir)	CONTROLES	TIPO DE CONTROL	EVALUACIÓN DEL RIESGO RESIDUAL										RIESGO RESIDUAL					ACCIONES ASOCIADAS AL REGISTRO			MONITOREO Y REVISIÓN			
FACTORES EXTERNOS	FACTORES INTERNOS	CAUSAS	RIESGOS	Clasificación del riesgo	DESCRIPCIÓN	CONSECUENCIAS	Probabilidad	Descriptor	Impacto	Descriptor	Nivel riesgo				Riesgos inherentes relacionados a procedimientos, responsables del control (15 puntos)	Riesgos definidos y responsables de la ejecución del control y del seguimiento (5 puntos)	¿El control es AUTOMÁTICO? (30 puntos)	¿El control es MANUAL? (30 puntos)	¿La frecuencia del control y seguimiento es adecuada? (10 puntos)	¿Se cuenta con evidencia de la ejecución y seguimiento del control? (10 puntos)	¿Es el tiempo que toma... hace mitiga los atributos del riesgo? (30 puntos)	Si no,	CONTROLES CUMPLE?	Probabilidad	Descriptor	Impacto	Descriptor	Nivel riesgo	PERIODO DE EJECUCIÓN	ACCIONES	REGISTROS	RESPONSABLES	Fecha	acciones	Responsables	Indicador (Riesgos de Corrupción
No identificados	- Sistemas de información - Usuarios	- Pérdida deliberada del servicios - Vulnerabilidad en los sistemas informáticos - Equipos tecnológicamente no adecuado - Falta de conocimiento o específico sobre las caracteristicas técnicas y	R1	Pérdida de información	Riesgo operativo	Pérdida de Información guardada en los sistemas de información y servicios tecnológicos. Información almacenada en los equipos locales y que no se encuentran en los sistemas archivos centralizad	- Datos erróneos Información Incompleta - Fuga de información Información desactualizada - Acceso no autorizado a la información	4		5			RIESGO DE CORRUPCIÓN	Control: Mantenimiento preventivos de la infraestructura Control: Control contratado a los sistemas de información Control: Gestión de carpetas compartidas Periodicidad Control: Identificación y de	PREVENTIVO	SI	SI	SI	NO	SI	SI	SI									Anual	Actividades asociadas al mantenimiento de los equipos de	Contrato de mantenimiento, Informe de ejecución, Registros	Coordinado r Grupo GTIR		N.A.	N.A.	N.A.
														PREVENTIVO	NO	SI	SI	NO	SI	SI	SI									Segundo Semestre	Documentación de roles de cada usuario	Documento roles Administración de Sistemas de	Administrad or del Sistema de Información		Validar ejecución	Coordinado r Sistemas de Información y Redes	N.A.
														PREVENTIVO	NO	SI	SI	NO	SI	SI	SI									julio a diciembre de 2018	Circular de actualizado de las	Circular de actualizado de las	Grupo de sistemas de información		Circular de ejecución de las	Coordinado r Sistemas de Información y Redes	N.A.
														PREVENTIVO	SI	SI	SI	NO	NO	SI	SI									julio a diciembre de 2018	Incluir propietario de la	Matriz de gestión de activos de	Grupo de sistemas de información		Validar ejecución	Coordinado r Sistemas de Información y Redes	N.A.
Ciberataques	Caida servidores ue soportan la infraestructura	- Pérdida deliberada del servicio. - Vulnerabilidad en los sistemas informáticos	R2	Indisponibilidad del servicio de Hora Legal	Riesgo operativo	La infraestructura que soporta la Hora Legal, se ve afectada	Afectación comunidad académica que basa sus estudios a la Hora Legal Colombiana. En caso de	4	#¡REF!	4			RIESGO DE CORRUPCIÓN	Control: Contratar alta disponibilidad con a todos los servicios de TI que soportan la Hora Legal Periodicidad	PREVENTIVO	NO	SI	SI	NO	SI	NO	NO	#¡REF!	#¡REF!						julio a diciembre de 2018	Identificación de los activos de información asociados a todo el proceso de generación	Matriz de gestión de activos de información	Grupo de sistemas de información		Validar ejecución	Coordinado r Sistemas de Información y Redes	N.A.
Ciberataques	Falta de documentación y sensibilización de metodologías de ejecución	- Accesos no autorizados a funcionalidades desarrollos con estructuras vulnerables	R3	Alteración de información de aplicativos y desarrollos	Riesgo operativo	Afectación en la integridad y confidencialidad de la información	Pérdida de trazabilidad en la información	4		4			RIESGO DE CORRUPCIÓN	Control: Procedimiento de desarrollo seguro Periodicidad: Responsable:	PREVENTIVO	NO	SI	NO	SI	SI	NO	NO									julio a diciembre de 2018	Generación del procedimiento de desarrollo de software seguro	Procedimiento	Grupo de sistemas de información		Validar ejecución	Coordinado r Sistemas de Información y Redes	N.A.
No identificados	- Sistemas de información - Usuarios	- Comunicaciones electrónica s no codificadas - Descuido por parte del usuario	R4	Pérdida de la confidencialidad en la información y las comunicaciones	Riesgo tecnológico	electrónico s remitidos pueden ser abiertos por personal no autorizado Personal no	Vulnerabilidad de la información - Pérdida de la confidencialidad y	4		5			RIESGO DE CORRUPCIÓN	Control: Cambio mensual de las claves de acceso a sistemas electrónicos. Periodicidad : Mensual Responsable	PREVENTIVO	SI	SI	SI	NO	SI	SI	SI									Segundo Semestre	Ejecución automática en el sistema de información	políticas y procedimientos aprobados por CIGD	Profesional Universitari o responsabl e		políticas y procedimientos implementados	Coordinado r Sistemas de Información y Redes	N.A.
Ciberataques	Keyloggers, falta de cifrado de información Malware alojado en los equipos de usuario final	Sistemas de información intervenidos No hay segmentación de redes, ni servidores	R5	Pérdida de confidencialidad de los activos de información del grupo directivo o lo intervenido por personal externo	Riesgo operativo	Acceso indebido a la información almacenada en los equipos de los integrantes de la junta directiva Los invitados a cursos o terceros, que tienen acceso a las	Toma de decisiones estratégicas del ORM puede verse comprometida. Fuga de información confidencial Pérdida de privacidad	4		4			RIESGO DE CORRUPCIÓN	Autenticación de de 2 pasos Identificación de vulnerabilidades	PREVENTIVO	NO	SI	SI	NO	SI	SI	NO									julio a diciembre de 2018	Análisis de vulnerabilidades en cada PC	Listado de vulnerabilidades	Grupo de sistemas de información		Validar ejecución	Coordinado r Sistemas de Información y Redes	N.A.
														PREVENTIVO	SI	SI	NO	SI	SI	SI	SI									julio a diciembre de 2018	Segmentar las redes en #VLANS	Matriz de #VLANS Asignadas con su respectivo segmento de red	Grupo de sistemas de información		Validar ejecución	Secretaria General	N.A.
No identificados	- Sistemas de información	- Asaques cibernetico s - Acceso indebido de personal no	R6	pérdida de disponibilidad de los servicios informático s	Riesgo tecnológico	se presentaría cuando se pierda la comunicaci ón electrónica	- interrupción del servicio previsto - Afectación de las operaciones	2		5			RIESGO DE CORRUPCIÓN	Control: campañas de sensibilizaci ón Control: Informe anual de	PREVENTIVO	NO	SI	SI	NO	SI	SI	SI									Primer Semestre	Documentar y el manejo del control de acceso biométrico al Data	Documento de control de acceso aprobado por CIGD, Formato	Profesional Universitari o responsabl e		Validación de funcionamiento de controles de acceso	Coordinado r Sistemas de Información y Redes	N.A.