Unidad Nacional de Protección
Área: Tecnología
Proceso: Gestión Tecnológica

Fecha de Reporte: 13/01/2017
Fecha de Seguimiento: 17/01/2017

Mapa de Riesgos de Corrupción			Acciones		
Causa	**Riesgo**	**Control**	**Efectividad de los controles**	**Acciones adelantadas**	**Observaciones de la Oficina de Control Interno**
1. Usuarios sin cultura de seguridad informática 2. Acciones indebidas en el uso de la información y los recursos informáticos de la Entidad 3. Falta de control de uso y acceso a la información de la Entidad. 4. Vandalismo informático que beneficia los intereses particulares de terceros 5. Presión, amenazas por parte de particulares a un funcionario o contratista para manipular o adulterar información en beneficio de terceros interesados.'	Omisión de acciones para el cuidado de los activos de información y acción de adulteración, daño, acceso o entrega no autorizada de información en beneficio de un privado perjudicando a la entidad o sus procesos.	Definir la Política General de la Seguridad de la Información. Levantar y mantener actualizado el inventario de activos de información con su calificación de criticidad y confidencialidad. Implementar controles tecnológicos o manuales para restringir y otorgar acceso a los activos de información de la Entidad.	SI	1. La "Política general de Seguridad de la Información" y la "Política de tratamiento de Datos Personales" se mantienen vigentes y a disposición de los usuarios y la ciudadanía en general en la Página Web de la Entidad. 2. De igual forma en la Página Web de la Entidad es posible acceder al Inventario de Activos de Información, el cual se encuentra en permanente actualización con los reportes de los procesos y se proyecta consolidar los datos con los entregables del Proyecto de Gestión Documental, los cuales son entregados al concluir la vigencia 2016. 3. Como parte de la implementación de la conectividad de Red de Datos unificada, se configuró para las sedes a nivel nacional canales dedicados tipo MPLS con encapsulamiento de datos para aumentar los niveles de seguridad y confidencialidad de la información que transmite por este medio. La infraestructura tecnológica cuenta con una configuración de acceso lógico a la red, Sistemas operativos, Bases de Datos, archivos compartidos, con controles basados en usuario, perfiles y contraseña, así como la incorporación de barreras físicas que permiten restringir el ingreso a las instalaciones. Así mismo, se cuenta con formatos que permiten llevar un registro controlado de las solicitudes de creación de usuario y acceso a los recursos tecnológicos. 4. Como mecanismo de control y gestión de la Plataforma Tecnológica se implementó la Solución del System Center, el cual permite monitorear el funcionamiento de los equipos de red, periféricos, dispositivos de red, bases de datos y servicios tecnológicos soportados con la plataforma tecnológica de la Entidad. NOTA: los servicios del SYSTEM CENTER fueron suspendidos a finales del mes de diciembre/ 2016, puesto que no se priorizó como servicio crítico en el Datacenter de contingencia durante el traslado de sede. Se priorizó como servicio crítico los servicios de la operación general de la Entidad (Entre ellos: SER, SIGOB, TNS). De igual forma, se cubrió la contingencia de almacenamiento y acceso a la información de los servidores, con la solución en la nube AZURE durante el traslado del Datacenter. 5. Para la campaña de seguridad se crearon unas piezas gráficas para promover las buenas prácticas sobre el uso de los recursos informáticos y los dispositivos tecnológicos, información que fue remitida mediante correo masivo a todos los usuarios. De igual forma se ejecutaron jornadas de socialización a los grupos de trabajo y los Procesos con el propósito de promover el uso de los recursos tecnológicos para fomentar la racionalización del uso del papel, así como presentar las herramientas que provee el uso del Windows 10 y el Office 365 en cuanto a almacenamiento, movilidad y seguridad de la información. Por otra parte, Se implementó en la Intranet el Portal "Clic", espacio virtual en el cual se busca promover una plataforma de formación virtual sobre las buenas prácticas en el manejo de la seguridad de la información, el uso de los sistemas de información y los contenidos institucionales.	La Oficina de Control Interno observa que de acuerdo a la información aportada por el proceso no se ha materializado el riesgo y que las acciones desarrolladas están dirigidas a la protección, control y trazabilidad de a información de la entidad siendo efectivas para controlar el riesgo identificado.
1. Estudios previos o de factibilidad manipulados para beneficiar a un tercero en particular o privado. 2. Términos de referencia condicionados para favorecer la elección de un tercero en particular 3. Falta en la ejecución de supervisión y seguimiento al proveedor y el producto o servicio contratado. 4. Deficiencias en el manejo de la documentación y el archivo. . 5. Ofrecimiento de Beneficios económicos para la elección de Proveedores de servicios de TI 6. Presión, amenazas por parte de particulares a un funcionario o contratista para manipular o adulterar un proceso de selección de proveedores	Uso del poder para beneficio privado de un tercero en los procesos de selección de proveedores y contratación de servicios de tecnología	Revisión dual en la definición y revisión de anexos técnicos que son usados en los procesos de selección y calificación de Proveedores. Realizar la supervisión de los contratos que son entregados en responsabilidad de tecnología, cumpliendo las políticas internas definidas para tal fin. Evaluar el cumplimiento y la ejecución de los contratos prestados por los proveedores de TI de conformidad a los términos requeridos por la Entidad.	SI	1. Durante el tercer cuatrimestre se ejecutaron a conformidad los contratos de Tecnología: 505-2016, 506-2016, 513-2016, 520-2016, 524-2016, 561-2016, 572-2016, 574-2016, 608-2016, 609-2016, 644-2016, 652-2016, 669-2016. La ejecución de los contratos se documentó mediante los reportes realizados en los informes de supervisión de acuerdo a las actividades realizadas por los proveedores y de acuerdo a los términos contractuales suscritos. 2. Los documentos técnicos de los procesos de adquisición que se originan del área de Tecnología son revisados por los ingenieros de infraestructura, la coordinación de TI y el líder de contratos de TI a fin de determinar el alcance de los requisitos de manera integral. Como resultado de esta revisión se conservan los soportes en las carpetas de cada proceso de adquisición del producto o servicio. 3. La definición y supervisión de los contratos de TI se ejecutaron de acuerdo al Manual de Contratación. Adicionalmente se documentaron las actividades y el seguimiento en los formatos establecidos en el SGI. 4. En consideración a la terminación de la vigencia 2016 y que se han ejecutado la mayoría de los contratos de TI se gestionó la calificación de los proveedores de acuerdo al análisis del cumplimiento del objeto de cada contrato y la valoración de los criterios de satisfacción y calidad establecidos en el Manual de Contratación. Es de aclarar que, debido a las condiciones de continuidad de la operación de la entidad, se hicieron prórroga a los contratos de CLARO y Premier de Microsoft.	La Oficina de Control Interno observa que de acuerdo a la información aportada por el proceso no se ha materializado el riesgo y que las acciones desarrolladas están dirigidas a la protección, control y trazabilidad de los recursos adquiridos por la entidad siendo efectivos para controlar el riesgo identificado.

Jefe Oficina Control Interno
Unidad Nacional de Protección