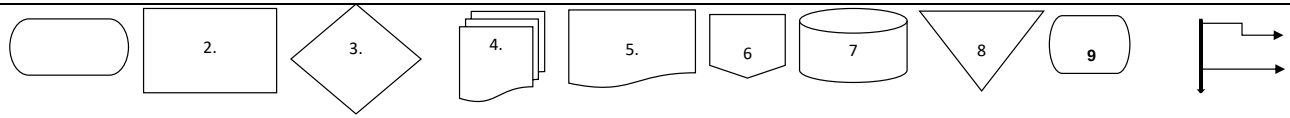
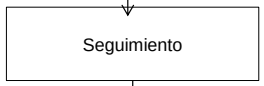
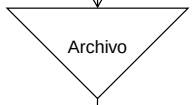
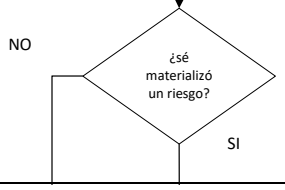
PROCEDIMIENTO
MONITOREO DE ACTIVOS Y SERVICIOS

PROCESO: Gestión de TIC	**LIDER:** Profesional Especializado TIC
OBJETIVO: Establecer las actividades y controles para realizar el monitoreo adecuado y permanente de la disponibilidad, capacidad y desempeño de los activos y servicios TIC.	

ENTRADAS	CONDICIONES GENERALES
Metodología y procedimiento para la gestión de incidentes de seguridad y ciberseguridad • Manual de politicas de SICS . Formato matriz de monitoreo activos y servicios • Inventario de activos de tecnología • Instructivos de herramientas de monitoreo • Herramientas software de monitoreo • Plan de Contingencia y Continuidad • Matriz de Riesgos	El monitoreo se realiza periódicamente el primer día hábil de cada periodo. El periodo puede ser diario, semanal, mensual o anual, de acuerdo con lo establecido en la Matriz de monitoreo de activos y servicios, o cuando se requiera. Durante el monitoreo de activos TIC se deben reportar las incidencias encontradas. Las incidencias de seguridad o ciberseguridad deben ser reportadas y de acuerdo al análisis preliminar ser clasificadas según las categorias de criticidad e impacto descritas en el documento "metodología y procedimiento para la gestión de incidentes de seguridad y ciberseguridad" Toda incidencia reportada debe registrar el detalle del técnico. Todas las acciones deben estar documentadas. Aplica a los servicios sujetos de monitoreo definidos en la Matriz de monitoreo de activos y servicios. Alcance en PCN: En situación de contingencia, se debe garantizar el monitoreo de servicios considerados contingentes en el Plan PCN, es decir, sistemas y componentes seleccionados como críticos en el análisis BIA, y que entran en funcionamiento en situación de contingencia. La actividad de monitoreo en situación de contingencia está sujeta a la disponibilidad del activo, así como la disponibilidad de la herramienta de monitoreo requerida.
SALIDAS	**DEFINICIONES**
• Matriz de Monitoreo de Activos y Servicios ejecutada. • Plan de Monitoreo • Registro en el aplicativo Mesa de ayuda de la actividad de monitoreo.	**Activo de información:** Componente del proceso de negocios. Los activos pueden incluir, gente, edificios, sistemas computacionales, redes, registros en papel, faxes, etc.Acuerdo de Niveles de Servicio (Service Level Agreement - SLA): Acuerdo escrito entre el proveedor de servicios y el cliente sobre los niveles de servicio acordados entre ambas partes. **Administración de Niveles de Servicio (Service Level Management - SLM)**: El proceso de definir, acordar, documentar y manejar los niveles de servicio del cliente de TI, que son requeridos y justificados en costo. **Monitoreo de TI:** Actividad de control y supervisión; que mide el movimiento de los activos digitales que conforma el ecosistema de TI de una organización. Su objetivo es comprender a fondo el comportamiento de la red de recursos tecnológicos que interactúan dentro de la empresa; para optimizar su desempeño y responder de forma rápida ante cualquier posible falla. **Monitorización e Escalado de Incidentes:** Monitorizar constantemente el estatus del procesamiento de Incidentes pendientes, para que inmediatamente se tomen medidas que contrarresten efectos adversos en caso de que peligren los niveles de servicio. **Notificación de Fallos al Servicio:** Es el informe de un fallo en el servicio al personal del Service Desk, que puede llegar por vía telefónica o por correo electrónico de parte de un usuario, o a través de alguna herramienta de monitorización de sistemas. **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo. Usualmente es expresado por una relación de disponibilidad, por ejemplo: La proporción de tiempo que el servicio está disponible para uso del servicio por el usuario, dentro del horario de servicio acordado. **Incidente:** Cualquier evento que no forma parte usual o normal de la operación diaria del proceso de negocio, que causa o puede causar una interrupción o reducción en la calidad del servicio. **Elementos de Configuración (Configuration Item - CI)**: Componente de la infraestructura o elemento, tal como el requerimiento de cambio asociado a la infraestructura que es o estará bajo control de la Administración de la Configuración. Un CI pueden variar mucho en complejidad, tamaño y tipo, desde un sistema completo incluyendo todo el hardware, software y documentación, hasta un solo módulo o un pequeño componente de hardware. **Métrica / Umbral** : Elemento medible de un proceso o una función. Nivel de Servicio: Expresión de un aspecto del servicio, en términos cuantificables y definitivos.

SIMBOLOGÍA	
SIGNIFICADO	1. Inico 2. Operación. 3 Decisión "SI o NO". 4. Multidocumento. 5. Documento. 6. Conector. 7. Sistema. 8. Archivo. 9. Fin. 10. Flechas

No.	FLUJOGRAMA	ACTIVIDAD	REGISTRO	RESPONSABLE	TIEMPO TOTAL HORAS
	INICIO	INICIO			
1	Actualizar matriz de monitoreo.	Revisar y actualizar una vez al año o cuando se requiera por cambios en la plataforma, el levantamiento del inventario de activos y servicios de TIC a monitorear, identificando las variables de medición, equipos y servicios, tipo de monitoreo requerido, periodicidad, asi como los activos y servicios sujetos de monitoreo en situación de contingencia.	Matriz de monitoreo de activos y servicios actualizada.	Profesional Especializado de TIC	16
2	Aprobación de la matriz de monitoreo	Presentar para revisión y aprobación	Matriz de monitoreo de activos y servicios. Acta de comíté	Comité de Riesgos	2
3	Programación y registro del plan de monitoreo	Elaborar el cronograma, definir responsable de la ejecución, revisar y programar el plan de monitoreo. (Registrar en el aplicativo mesa de ayuda)	matriz de monitoreo de activos y servicios. Plan de monitoreo	Profesional Especializado de TIC	4
4	Verificación vigencia de los instructivos	Chequear que los instructivos de operación que hacen referencia a las actividades consignadas en la matriz se encuentren actualizados. Si se identifica un instructivo desactualizado se procede a aperturar en el caso del aplicativo de mesa de ayuda.	matriz de monitoreo de activos y servicios, actualizada. Registro de incidente en aplicativo Mesa de ayuda	Profesional Especializado / Profesional universitario de TIC	4
5	Configuración herramientas de monitoreo.	Realizar la configuración de la herramienta de acuerdo a la matriz de monitoreo actualizada, registrando la evidencia de realizacion de la actividad de monitoreo en el aplicativo Mesa de Ayuda: Clasificarla en la categoria respectiva. Para aquellos casos cuya actualización requiere soporte externo se transfiere al proveedor el requerimiento de configuración respectiva.	Registro de la actividad y/o incidente en aplicativo Mesa de ayuda	Profesional Especializado / Profesional Universitario de TIC	16

No.	FLUJOGRAMA	ACTIVIDAD	REGISTRO	RESPONSABLE	TIEMPO TOTAL HORAS
6		Ingresar a cada una de las herramientas de monitoreo identificadas en la matriz. Se revisan el estado, alertas, informes de incidentes, logs y demás variables a gestionar conforme a los elementos y periodicidad de la "matriz de monitoreo activos y servicios" e "Instructivos de herramientas de monitoreo" y se verifica la disponibilidad de los activos en el mapa de estado, mediante observaciones periodicas en tiempo real. Durante el monitoreo al detectarse una incidencia se debe abrir un nuevo caso en la mesa de ayuda, estebleciendo criticidad y prioridad. Si las incidencias son de seguridad o ciberseguridad, de acuerdo al análisis preliminar deben ser clasificadas según las categorias de criticidad e impacto descritas en el documento “metodología y procedimiento para la gestión de incidentes de seguridad y ciberseguridad”	Registro de cada Monitoreo de servicios Tic en el aplicativo Mesa de Ayuda Registro de incidente en aplicativo Mesa de ayuda	Profesional Especializado / Profesional Universitario de TIC	12
7		Realizar al final de cada cuatrimestre o cuando se requiera, el seguimiento y medición de la gestión y generar los informes del servicio. **AC**	Informes	Profesional Especializado de TIC	1
8		Almacenar las matrices de monitoreo, los instructivos y el plan de monitorieo en la carpeta de documentos digitales del proceso. Almacenar los los registros de la solicitud, seguimientos de las actividades del procedimiento.y anexos de la atención en la base de datos del aplicativo Mesa de ayuda GLPI, el cual es asegurado y respaldado periodicamente. Y puede ser consultado según sea requerido	Carpeta de red en servidor de archivos. Registro en el aplicativo Mesa de ayuda Respaldos (back ups) del aplicativo Mesa de ayuda	Profesional Especializado / Profesional Universitario de TIC	1
9		¿Se materializó algun incidente o evento de riesgo? SI: Pasar a la actividad 10 NO: FIN			

No.	FLUJOGRAMA	ACTIVIDAD	REGISTRO	RESPONSABLE	TIEMPO TOTAL HORAS
10		Reportar los eventos y/o incidentes que afecten los sistemas de administración de riesgos (SARO, SARC,SARL, SARM, SGSI, SIPLAFT, de Corrupción) materializados en cualquiera de las actividades del procedimiento.	Aplicativo DARUMA Módulo Situaciones	Líder del proceso	1
11		FIN			

ELABORÓ:	Ruby Dalila Sánchez Posada	Cargo: Profesional Especializado PS
REVISÓ:	Fredy Alexander Guerrero Vega	Cargo: Profesional Especializado de TIC
APROBÓ:	Comité Institucional de Gestión y Desempeño	Cargo: No Aplica