1. OBJETIVO

Describir los pasos para realizar monitoreo, salvaguardar los eventos de seguridad y generar trazabilidad sobre las operaciones que se realizan en los servidores de aplicación, controladores de dominio, servidores de licencias, servidores de actualización, servidores de correo local, servidores de bases de datos y sistemas operativos asociados.

2. ALCANCE

Aplica para todos los accesos a la plataforma tecnológica de los servidores críticos que cuenten con Sistema Operativo Windows Server, que hacen parte de la plataforma tecnológica institucional.

3. RESPONSABLE

El profesional Especializado, responsable del Grupo de Servicios Tecnológicos será el encargado de realizar dicha tarea o a su vez delegará funciones para dicho menester.

4. GENERALIDADES

El procedimiento de Gestión de Logs se aplica sobre los eventos de seguridad de toda plataforma o servicio tecnológico alojado en los servidores que pertenecen a la Universidad del Magdalena; así como los accesos de los usuarios del personal de planta o contratistas que administren recursos y activos de información en dichos servidores. En cuanto a materia de protección, el ámbito de ejecución de este procedimiento se toman medidas de aseguramiento de los logs para futuras auditorias, detallados según normativa aplicada dependiendo de los recursos que se cuenten para establecer la Gestión de Logs.

4.1 Definiciones

Análisis de Log: Estudio de los Logs para identificar eventos de interés o suprimir entradas de eventos insignificantes.

Evento: Una alerta o notificación creada por algún componente de la plataforma tecnológica de la información o herramienta de monitoreo.

Evidencia digital: Información con valor probatorio almacenada o transmitida en forma digital.

Incidente: Es un evento o serie de eventos de seguridad de la información no deseado o no planeado, que afecte la prestación del servicio o reduzca la calidad de

la prestación del servicio o que tenga una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Log: Son registros de todos los eventos que ocurren dentro de los sistemas y redes de una organización, sistema o aplicación. Cada entrada en estos archivos contiene información relacionada a un evento específico que ocurrió dentro de un sistema o red. Rastro de lo que se está ejecutando sobre la plataforma tecnológica.

Monitoreo de Logs: Consolas que pueden ser usadas para monitorear o revisar la información de los logs o de los análisis generados de manera automática.

Ofuscación: Se refiere al acto deliberado de realizar un cambio no destructivo, ya sea en un documento o el código fuente de un programa informático, con el fin de que no sea fácil de entender o evitar divulgación de información sensible.

Script: El script es un documento que contiene instrucciones, escritas en códigos de programación. El script es un lenguaje de programación que ejecuta diversas funciones en el interior de un programa de computador.

5. DESCRIPCION

Nº	Responsable/ Dependencia	Descripción de la Actividad
01	Profesional Universitario / Grupo de Servicios Tecnológicos	**Activación de eventos de seguridad:** Activa los eventos de seguridad a través del visor de eventos del sistema en todos los servidores con Windows server.
02	Profesional Universitario / Grupo de Servicios Tecnológicos	**Asignación de Permiso:** El Profesional encargado de la infraestructura tecnológica brinda acceso sobre el(los) servidor(es) críticos que contienen Windows server y otorga permiso de ejecución para el comando de Powershell al ***Coordinador de Seguridad en Tecnología de la información***.
03	Coordinador de Seguridad en Tecnología de la información/ Grupo de Servicios Tecnológicos	**Proveer o inclusión del Script:** Ubica el script configurado de acuerdo al servidor en el disco local c del mismo, se salvaguarda en una carpeta con contraseña.
04	Coordinador de Seguridad en Tecnología de la	***Programación de Ejecución del script:*** Configura un disparador en cada servidor, donde se tomará el script creado para que se ejecute

Nº	Responsable/ Dependencia	Descripción de la Actividad
	información/ Grupo de Servicios Tecnológicos	automáticamente en un tiempo determinado no mayor a 24 horas. Esta tarea se crea con permisos de ejecución.
05	Coordinador de Seguridad en Tecnología de la información/ Grupo de Servicios Tecnológicos	***Copia de seguridad de los LOGs:*** Una vez ejecutado el script, establece un espacio dedicado en el sistema de almacenamiento, el cual estará destinado para resguardar los registros de logs de Eventos de Seguridad de los servidores con Windows server de la Universidad.
06	Coordinador de Seguridad en Tecnología de la información/ Grupo de Servicios Tecnológicos	***Verificación de Respaldo de LOGs*** Una vez se establece la ejecución del respaldo de LOGs, pasa a revisar que la tarea esté funcionando correctamente, que se esté haciendo de manera efectiva el resguardo de los eventos de seguridad y que estos cumplan con las condiciones determinadas.
07	Coordinador de Seguridad en Tecnología de la información/ Grupo de Servicios Tecnológicos	***Tiempo de Retencion de LOG´s*** Ubica en la unidad de almacenamiento un script para que se ejecute de manera automática, el cual tiene como función eliminar los registros de LOGs. Se establece como tiempo de rotación de LOGs un estimado de 30 días como límite para tratamiento y resguardo de un registro, es decir, a partir de esa fecha los LOGs con 31 días en el almacenamiento serán eliminados o en su defecto se sobrescribirán para almacenar registros nuevos.

6. MARCO LEGAL

Tipo de Norma	Entidad que Emite	Nº Identificación	Fecha de Expedición (DD/MM/AAAA)	Descripción de artículos, capítulos o partes de la Norma que aplican al documento
Ley	Congreso de Colombia	87	29/11/1993	Art.4 i. Establecimiento de sistemas modernos de información que faciliten la gestión y el control.

7. DOCUMENTOS DE REFERENCIA

G.SIS.02 Guía Técnica de Sistemas De Información-Trazabilidad / Basado en la Norma ISO 27002:2013.

8. REGISTRO

Identificación		**Almacenamiento** (Archivo de gestión)		**Protección**	**Recuperación** (clasificación para consulta)	**Disposición** (Acción cumplido el tiempo de retención)
Código Formato	**Nombre**	**Lugar y Medio**	**Tiempo de Retención**	**Responsable de Archivarlo**		
N.A	Gestión de LOGs	Grupo de Servicios Tecnológicos/ Digital	30 días	Automático en la unidad de almacenamiento	• Fecha	Eliminación automática

REGISTRO DE MODIFICACIONES

Versión	**Fecha**	**Ítem modificado**	**Descripción**

No aplica para este documento por ser la primera versión

Elaboró	***Revisó***	***Aprobó***
Equipo de trabajo del proceso de Apoyo Tecnológico TIC *28/08/2020*	*Yineth Pérez Torres* *Responsable Mejora Continua* *Grupo de Gestión de la Calidad* *31/08/2020*	*Hildemar Quintana Hernández* *Responsable del proceso* *Apoyo Tecnológico TIC* *01/09/2020*

9. ANEXOS

9.1 Flujograma