OBJETIVO

Registrar eventos y generar trazabilidad sobre las operaciones que se realizan en los sistemas de información y sistemas operativos, con el objeto de realizar monitoreo de los servicios informáticos

RESPONSABLE

Coordinador del Grupo de Sistemas y Arquitectura de Tecnología o quien este encargue.

ALCANCE

Aplica para el acceso a la plataforma tecnológica que cuenten con Sistemas operativos, o Dispositivos de red o dispositivos de seguridad de propiedad de Integral Group Solution.

DEFINICIONES

Administración de Log: Proceso mediante el cual se realiza la generación, transmisión, almacenamiento, análisis, monitoreo y reporte de los Logs.

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: Es el registro de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar. Rastro de lo que se está ejecutando sobre la plataforma tecnológica. Recurso de Información: Término con el cual se designan las aplicaciones y datos que hacen posible el desarrollo del negocio de Integral Group Solution.

Retención de Log: Archivar los logs de eventos como parte de las actividades de administración de la infraestructura de acuerdo con las políticas de respaldo y recuperación de los mismos. Rotación de Log: Cerrar un registro de log y abrir uno nuevo de acuerdo con un periodo establecido o teniendo en cuenta la capacidad de almacenamiento disponible en el servidor (local o remoto).

CONDICIONES GENERALES

Contar con rastros de auditoria, permite que la entidad pueda realizar investigaciones especiales, cumplir con regulaciones, verificar eventos de seguridad entre otros. Se deben definir actividades que permitan contar con estos rastros de auditoria y controlar su almacenamiento.

.Activación de logs. Todos los sistemas de información, aplicativos, sistemas operacionales, bases de datos, dispositivos de comunicación, dispositivos de seguridad y servidores, deben contar con los logs o rastros de auditoria que registren las actividades de los usuarios, las excepciones, las fallas y eventos de seguridad. Es responsabilidad de los propietarios y/o líderes de TI, estar pendientes de la activación de los logs de auditoria. El encargado del aplicativo debe mantener un inventario de los registros de auditoria

existentes por aplicación y su ubicación
Verificación de eventos.

Se debe elaborar, conservar y revisar periódicamente los registros acerca de las actividades de los usuarios, excepciones, fallas, y eventos de seguridad de la información. Es responsabilidad de los propietarios de la información, solicitar y conocer que eventos se han producido sobre los sistemas de tratamiento de su información. Es responsabilidad de los líderes técnicos de infraestructura y sistemas de información, proveer la información de eventos solicitada por los usuarios.

Respaldo y restauración de archivos de auditoria.

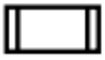
Es responsabilidad de los líderes técnicos de infraestructura y sistemas de información establecer un plan de respaldo de logs de auditoria por medio de la herramienta con que se cuente, teniendo en cuenta todos los componentes de la plataforma tecnológica de producción. Se deben establecer directrices de retención, respaldo y recuperación de los logs y registros de auditorías de los componentes de la plataforma tecnológica cuando aplique, ya que estos se constituyen en evidencia para la identificación de un incidente de seguridad. Configurar la rotación de logs automáticamente en la herramienta con que se cuente ya que ella debe consolidar la información de los logs de equipos y/o dispositivos que tenga configurados, si es posible, de lo contrario garantizar que no se pierda, ni se sobrescriba los archivos de los logs. De acuerdo con las directrices de retención, respaldo y recuperación, aplicar el borrado de los registros de logs consolidados en la herramienta utilizada para el respaldo de logs de auditoria.

Parametrización de herramienta utilizada para la gestión de logs.

El responsable de seguridad en la red será el responsable de asignar responsabilidades de parametrización de la herramienta que se utilice para el respaldo de logs de auditoria.

El responsable de seguridad en la red será el responsable de autorizar permisos de acceso a la herramienta que se utilice para el respaldo de logs de auditoria, para efectos de revisiones e investigaciones.

DESCRIPCION DE LA ACTIVIDAD

Símbolo	Nombre del símbolo	Función
	Inicio/Fin	Se utiliza para indicar en donde comienza o finaliza el procedimiento.
	Actividad	Se utiliza para representar la ejecución de una actividad al interior del proceso.
	Decisión	Se utiliza para indicar que se debe evaluar una condición y plantear la selección de una alternativa.
	Conector de actividades	Se utiliza para conectar dos actividades o puntos del flujograma (solo se emplea si las actividades o puntos están en la misma página del flujograma)
	Conector de página	Se utiliza para conectar dos actividades o puntos del flujograma (solo se emplea si las actividades o puntos están páginas diferentes del flujograma)
	Proceso predefinido	Se utiliza para indicar que hay un proceso predefinido para la ejecución de una actividad.

Flujograma	Descripción	Responsable	Documentos o formatos	Puntos de control
	Inicio			
	Activación de logs. Activar el registro de logs y auditorias de los componentes de la plataforma tecnológica para que reporten los eventos cuando aplique. Llevar inventario de logs por aplicativo	Líder de Centro de cómputo, Líder de Comunicaciones y Líder PC, impresoras y escáneres, de acuerdo a su especialidad Líderes de aplicaciones.	Inventario de logs y registros de auditoria	
	Parametrizar la Herramienta. Asignar responsable de parametrización y Autorizar acceso a logs de eventos Crear los perfiles de acceso de acuerdo con los roles requeridos en los componentes de la plataforma tecnológica que aplique.	Coordinador de sistemas y arquitectura tecnológica.	Herramienta utilizada	
	Elaborar planes de respaldo. Adicionar al plan de respaldo de información, los logs de los sistemas de información y de los dispositivos de la infraestructura. Elaborar plan de restauración Revisar periódicamente planes de respaldo y restauración de logs de auditoria	Coordinador de sistemas y arquitectura tecnológica.	Plan Acta de revisión	X
	Verificar los eventos. Solicitar informe de eventos del sistema de información. Realizar verificación de eventos e informar anomalías que se encuentren.	Propietario de información	Acta de revisión	X
	Generar mínimo una (1) vez al mes la estadística consolidada de los logs y registros de auditoria.	Funcionario asignado al proceso de respaldo de logs de auditoria	Informe estadístico	X
	FIN			

ACTIVIDAD Y ELEMENTOS CON RECOPILACION DE LOG DE AUDITORIA

Elementos de red y servidores.

Aplicativos Apolo , Vicidial/osdial/ , Software Contable, Softphnes.

Se considera registrar, entre otros, los siguientes eventos:

- Acceso, creación, borrado y actualización de información confidencial.
- Inicio y fin de conexión en la red corporativa.
- Inicio y fin de ejecución de aplicaciones y sistemas.
- Inicio y fin de sesión de usuario en aplicaciones y sistemas; intentos de inicio de sesión fallidos.
- Cambios en las configuraciones de los sistemas y aplicativos más importantes.
- Modificaciones en los permisos de acceso.
- Funcionamiento o finalización anómalos de aplicativos.
- Aproximación a los límites de uso de ciertos recursos físicos:
- Capacidad de disco; memoria.
- Ancho de banda de red
- Uso de CPU.
- Indicios de actividad sospechosa detectada por antivirus, Sistemas de Detección de Intrusos (IDS), etc.
- Transacciones relevantes dentro de los aplicativos.

Información relevante incluida en el registro. Detallaremos los elementos de información más útiles que deben ser incluidos en los distintos registros. Los más habituales son:

- Identificador del usuario que realiza la acción;
- Identificación del elemento sobre el que se realiza la acción (registros, bases de

datos, equipos, etc.);

- Identificación de dispositivos, ya sea a través de sus direcciones IP, direcciones MAC, etc.;
- Identificación de protocolos;
- Fecha y hora de ocurrencia del evento;
- Tipología del evento.

Elección del mecanismo de registro. Actualmente esta tarea la realizamos con PaperTrails, para realizar búsquedas y consultas en los logs desde varias máquinas, en una interfaz sólida tipo texto.

Protección y almacenamiento. Nos aseguraremos de que la información de registro esta convenientemente almacenada para protegerla de accesos indebidos.

Sincronización del reloj. Debemos asegurarnos de que todos nuestros sistemas están sincronizados correctamente, de este modo garantizaremos el correcto registro temporal de los eventos más relevantes

Sistemas de monitorización y alerta. Paralelamente al registro de los eventos más significativos, utilizaremos los sistemas de monitorización para que nos alerten en tiempo real de posibles errores y comportamientos anómalos, tales como:

- Proximidad de alcanzar los límites en la utilización de los recursos físicos hardware.
- Finalización o comportamientos anómalos de programas.
- Comportamientos anómalos en la red.
- Cambios en configuraciones críticas.
- Picos de rendimiento anómalos en los sistemas y redes.

CONTROL DE CAMBIOS

Revisión	Ítem Modificado	Objeto de la Modificación
Rev. 00	Creación del Documento	
Rev. 01	Actividades y elementos con recopilación de log de auditoria.	Detallar a los elementos que se recopila log de auditoria.

Brian Cortes	**Mario Pomares**	**Russell Aparicio**
Elaboró/Controló	**Revisó**	**Aprobó**