Contenido

1. OBJETIVO

Revisar los Logs de las operaciones que se efectúan en los distintos sistemas o dispositivos de misión crítica del ICETEX para buscar errores, anomalías o actividades sospechosas que infrinjan las políticas de seguridad o estándares establecidos.

2. ALCANCE

Cubre los sistemas y/o dispositivos críticos y deberán ser configuradas las alertas y revisados los Logs trimestralmente por los dueños de la información Logs

3. DEFINICIONES

- **Administrador de Base de Datos (DBA):** Persona encargada de la administración de las Bases de Datos que soportan los sistemas de información.
- **Log:** Registro de eventos presentados en los sistemas de Información y/o dispositivos que permite tener trazabilidad sobre las acciones que son ejecutadas por sistemas por usuarios en las bases de datos y dispositivos.
- **SIEM** (Security Information and Event Management)**:** se basan en detectar actividades sospechosas que amenazan los sistemas, se encargan de procesar una gran cantidad de Logs, enviando alertas sobre los fallos de seguridad encontrados en el sistema y las actividades sospechosas que están ocurriendo en tiempo real.
- **Correlacionar**: Colocar dos o más cosas en una relación recíproca o mutua, donde una o varias características coincidan con un patrón determinado.
- **Revisión de Logs:** Es el procedimiento que se ejecuta para identificar acciones y/o comportamientos, bien sea regulares o atípicos a través de la definición de patrones de revisión, criterios de verificación y reglas de correlación aplicables en las fuentes de revisión que son los registros de los sistemas o dispositivos (Logs)
- **Reglas de Correlación:** son las directrices o parámetros configurados en el SIEM para que sean disparados distintos tipos de alertamientos al coincidir con uno o más características definidas en una regla por el administrador a través de los registros (Logs) recibidos.

4. CONDICIONES GENERALES

- La revisión de los Logs de los distintos sistemas o dispositivos se debe realizar por parte de los propietarios de la información.
- El comité de Logs se realizará trimestralmente, o por demanda para casos de seguridad de la información que así lo ameriten o por casos especiales. En dicho comité se deben presentar los eventos relevantes resultados de la revisión de Logs y nuevos requerimientos o ajustes a lo que ya existe para el registro de eventos y trazabilidad de los mismos.
- Se debe generar acta de los comités de Logs que se realicen, donde se especifiquen los análisis presentados y compromisos si hubiera lugar a ello.
- El comité de Logs debe estar compuesto por un delegado de la Oficina de Riesgos y un delegado de la Dirección de Tecnología.
- Si esta información de Logs, maneja información clasificada y reservada, se debe tener en cuenta la política de retención y análisis de eventos en todas las tecnologías de la información y las telecomunicaciones de producción y contingencia, tal como se indica en el documento G212 "Requerimientos para auditoria de Logs"
- El comité de Logs, de igual forma servirá como herramienta para poder realizar análisis de las auditorias configuradas en las tablas de las bases de datos y/o usuarios que requieran depuración

Cumplir con los siguientes lineamientos:

- **Protección de Logs:** Para lograr que los Logs sean confiables y válidos en determinadas situaciones como evidencia, se debe tomar medidas por

parte de los responsables de configurar los Logs en los distintos sistemas de información o y dispositivos, que protejan la exactitud, autenticidad y accesibilidad de los archivos.

- **Exactitud**: Asegurarse de que los registros de las operaciones previstas en los Logs se estén ejecutando de forma adecuada.
- **Autenticidad:** Se puede decir que un archivo de log es auténtico si se puede probar que no han sido modificados desde que fueron originalmente registrados.
- **Movimiento de Logs:** Se debe cambiar la localización de los archivos en sí, se debe considerar trasladar los Logs a una máquina diferente a la cual los produce.
- **Trabajar con copias:** Cuando se realiza cualquier tipo de análisis sobre los archivos de Logs, nunca se debe realizar sobre el archivo original.
- **Documentación de procesos:** Establecer un proceso significa crear un documento que liste y detalle cada paso tomado, ya sea de forma manual o automático a la hora de recolectar la evidencia.
- **Accesibilidad o Control de Acceso:** Una vez el archivo del log es creado debe ser auditado y protegido para prevenir accesos no autorizados.
- **Restringir el acceso a archivos:** Un archivo de Log necesita ciertos permisos para que la aplicación o sistema que lo produce pueda enviar o almacenarlos en determinada locación para luego el registro se debe cerrar y nadie debe tener acceso a modificar el contenido de este.
- **Cadena de custodia:** Al mover los archivos desde un servidor a un dispositivo offline, o cualquier otro manejo que se ha planeado realizar, es muy importante registrar los cambios de ubicación que los archivos han tenido.
- **Temporalidad de los Logs:** Se define una retención en base de datos de un año para los Logs que se genere.

5. DESCRIPCIÓN

5.1. ACTIVIDADES

Administrador de la Herramienta / Contratista ICETEX

5.1.1. El administrador de cada sistema de información o base de datos, debe configurar el registro de eventos (auditorias) que haya solicitado el propietario de la información o por el conocimiento obtenido en el levantamiento de requerimientos.

5.1.2 El administrador de cada sistema de información o base datos debe solicitar la creación de las reglas de correlación en el SIEM que se usaran para obtener la información de acuerdo con las necesidades de configuración de alertas en dispositivos y sistemas de información determinadas por las coordinaciones de la Dirección de Tecnología o por los diferentes propietarios de la información

5.1.3 El administrador del SIEM debe configurar las reglas de correlación solicitadas por los administradores de cada sistema de información o base de datos y configurar el envío de alertas a los propietarios de la información.

5.1.4 Con base en los eventos auditados se debe verificar por parte de los propietarios de la información si existe alguna anomalía en las transacciones para implementar las medias de seguridad que eviten la materialización de incidentes de seguridad de la información.

5.1.3. ¿Se presentó alguna anomalía en los eventos auditados?

i) Si sí, continúa en punto 5.1.4.
ii) Si no, continúa en punto 5.1.5.

Administrador(es) de la(s) Herramienta(s) / Contratista ICETEX

5.1.4. Se solicita asistencia de los Administradores de los sistemas o dispositivos involucrados en los alertamientos, para implementar medidas de solución estableciendo un plan de acción que evite la materialización de incidentes de seguridad

Administrador de la Herramienta / Contratista ICETEX

5.1.5. Continua a la actividad 5.1.6.

Comité de Logs / ICETEX /Delegado de la Dirección de Tecnología

5.1.6. El delegado de la Dirección de Tecnología presenta ante el comité de Logs el informe ejecutivo (presentación) de los puntos más relevantes del análisis realizado, los escalamientos y resultados obtenidos. FIN

6. SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
Conformidad del log de transacciones	Establecer parámetros a ser auditados en el SIEM	Reglas configuradas	Coordinaciones de la Dirección de tecnología
Recepción y revisión de los hallazgos encontrados	Seguimiento a los compromisos de las actas generadas	Informe del SIEM	Administradores de Herramientas auditadas

7. DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CODIGO
Informe de casos auditados mensual	N/A
Requerimientos para auditoria de Logs	G212

Modificaciones

Descripción de cambios

Se realizan ajustes en el objetivo, alcance y condciones generaales

Se elimina el 5.2 diagama de flujo. En las actividades se realizan ajsutes a las actividades 5.1.1,5.1.2, 5.1.3, 5.1.4. 5.1.5 y 5.1.6

Se elimina la a ctividad 5.2.7.

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2021-01-15	6	Se realizan ajustes en el objetivo, alcance y condciones generaales Se elimina el 5.2 diagama de flujo. En las actividades se realizan ajsutes a las actividades 5.1.1,5.1.2, 5.1.3, 5.1.4. 5.1.5 y 5.1.6 Se elimina la a ctividad 5.2.7.
2019-12-30	5	• Se ajusta el objetivo y el alcance • En las definiciones se realizan ajustes en los conceptos de Administrador de bade de datos, log y revisión de logs • Se incluyen las definiciones de correlacionar, reglas de correlación, SIEM • Se ajustan las condiciones generales y se elimina la regla de realizar periódicamente la verificación de rotación de los Logs. • Se adiciona la regla ◦ El comité de Logs, de igual forma servirá como herramienta para poder realizar análisis de bases de datos y/o usuarios, si así se determine para algún periodo. • Se ajustan los conceptos de los lineamientos. • Cambian las actividades • Se adiciona la guía G212 Requerimientos para auditoria de Logs
2017-6-23	4	Se modifica el punto 1 objetivo ingresando "para realizar la" y "que permita". Se modifica el punto 2 alcance cambiando "mensualmente" a "trimestralmente" y se complementa ingresando "análisis de las implementaciones para la obtención de los mismos". Se modifica el punto 4 condiciones generales, en la primera viñeta se cambia periodicamente por trimestralmente. Se elimina la 4 viñeta. Se modifica la 5 viñeta. En el actividad 5.2.1. se elimina la palabra "puesta en".
2015-09-01	3	• Cambia el objetivo ingresando la verificación de los requisitos. • Cambia el nombre del procedimiento suprimiento base de datos quedando "Revisión Logs" • En el alcance se ingresa Logs y/o Tablas. • Se modifican las definiciones • Se ingresa una condición general el cual define la periodicidad de la revisión de los losg y tablas. • En las actividades se modifica el responsable cambiando el oficial de seguridad por el "Delegado de la Oficina de riesgos". • Se modifican las actividades estipulando los sistemas de información • Se modifican las actividades del punto 6 Seguimiento y control cambiando los controles. • En el punto 1 se cambia en su totalidad el objetivo estableciendo nuevos controles para la revisión de los logs. • En el punto 2 se cambia en su totalidad el alcance reflejando el tiempo del proceso. • En el punto 3 se ingresan 2 definiciones y se eliminan eventos críticos y no críticos.

2013-1-15	2	• En el punto 4 se cambian dos condiciones generales y se ingresan políticas de cumplimiento. • En el punto 5.2 se cambian en su totalidad las actividades. • En el punto 6 se suprimen y se ingresan 2 puntos de control. • En el Punto 7 se suprimen los 3 documentos relacionados y se ingresa “Revisión de logs de auditoria de los sistemas.
2010-06-24	1.0	-