Requisitos de Seguridad y Trazabilidad de la Información Transaccional y de Logs para ser consultados desde un Módulo de Auditoria en los Sistemas de Información.

Premisa: Los administradores, clientes y usuarios que utilizarían el servicio y los diferentes sistemas de información deben estar registrados en las bases de datos de las aplicaciones, de igual manera todo cambio, registro, transacción y eventos (administrativos, técnicos y operacionales) que se realicen desde los diferentes servicios y sistemas de información a nivel de bases de datos y de capa de aplicación deben ser revisados y auditados periódicamente.

Objetivos de Control y Controles para Transacciones y eventos de la Norma ISO 27002:

12.4 REGISTRO (LOGGING)Y SEGUIMIENTO

Objetivo: Registrar eventos y generar evidencia

12.4.1 Registro de eventos

Control:

Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Guía de implementación

Los registros de eventos (Event Logs) deberían incluir Cuando es pertinente:

- a. Identificación de usuarios
- b. Actividades del sistema
- c. Fecha, hora y detalles de los eventos claves, por ejemplo, entrada y salida
- d. Identidad del dispositivo o ubicación, si es posible, identificador del sistema
- e. Registro de intentos de acceso al sistema exitosos y rechazados
- f. Registro de datos exitosos y rechazados y otros intentos de acceso a recursos;
- g. Cambio a la configuración del sistema;
- h. Uso de privilegios
- i. Uso de utilidades y aplicaciones del sistema;
- j. Archivos a los que se tuvo acceso, y el tipo de acceso;
- k. Direcciones y protocolos de red,
- l. Alarmas accionadas por el sistema de control de acceso;
- m. Activaciones y desactivación de los sistemas de protección, tales como sistemas de antivirus y sistemas de detección de intrusos;
- n. Registro de las transacciones ejecutadas por los usuarios en las aplicaciones

El registro de eventos (Events Logging) establece las bases para los sistemas de seguimiento automatizado que están en capacidad de generar informes consolidados y alertas sobre la seguridad del sistema.

Información Adicional

Los Registros de eventos (Event Logs) pueden contener datos sensibles e información identificable personalmente. Se deberían tomar medidas apropiadas para la protección de la privacidad (Véase el numeral 18.1.4).

En donde sea posible, los administradores de sistemas no deberían tener permisos para borrar o desactivar registros (Logs) de sus propias actividades (12.4.3).

12.4.2 Protección de la información de registro (Log Información)

Control:

Los Sistemas de gestión de registro (Logging Facilities) y la información de registro (Log information) se deberían proteger contra alteración y acceso no autorizado

Guía de implementación

Los controles deberían estar dirigidos a proteger contra cambios no autorizados de la información del registro (log Information) y contra los problemas operacionales con los sistemas de gestión de registro (logging faclilities, inclusive:

- a. Alteración a los tipos de mensajes que se registran;
- b. Archivos de registro (log Files) que son editados o eliminados;
- b. Se excede la capacidad de almacenamiento del medio de archivo de registro (Log File Media), lo que da como resultado fallas en el registro de eventos, o sobre escritura de eventos pasados registrados.

Puede ser necesario archivar algunos registros de auditoria (Audit Log), como parte de la política de retención de registros o debido a requisitos acerca de recolectar y retener evidencia

Los registros de sistemas (System Logs) a menudo contienen un gran volumen de información mucha de la cual es ajena al seguimiento de la seguridad de la información. Para ayudar a identificar los eventos significativos con propósitos de seguimiento de la seguridad de la información, se debería considerar el copiado automático del tipo de mensaje apropiados a un segundo registro (Log), o el uso de utilidades del sistema(System Utilities) o herramientas de auditoría adecuados para llevar a cabo la interrogación y racionalización de los archivos.

Es necesario proteger los registros de sistema (System Utilities), ya que, si los datos se pueden modificar o los datos se pueden borrar, su existencia puede crear una sensación falsa de seguridad. El copiado de registro (logs) en tiempo real a un sistema por fuera de control de un administrador u operador del sistema se puede usar para salvaguardar los registros (logs).

12.4.3 Registro (Logs) del administrador y del operador

Control:

Las actividades del administrador y del operador del sistema se deberían registrar (Logged), y los registros (logs) Se deberían proteger y revisar con regularidad

Guía de implementación

Los titulares de cuenta de usuario privilegiado pueden estar en capacidad de manipular los registros (logs) en instalaciones de procesamiento de información bajo su control directo; por esto, es necesario proteger y revisar los registros (logs) para mantener la rendición de cuentas para los usuarios privilegiados.

Información adicional

Un sistema de detección de intrusión gestionado por fuera del control del sistema y de los administradores de la red se puede usar para hacer seguimiento del sistema y de las actividades de la red se puede usar para hacer seguimiento del sistema y de las actividades de administración de la red, para determinar su cumplimiento.