POLÍTICAS DE REGISTRO DE EVENTOS

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre y Apellido / Cargo	Firma
Elaborado por:	Ing. Geovanny Meza, Mg. **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: JORGE GEOVANNY MEZA MORALES
	Ing. Darío Braganza **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: DARIO JAVIER BRAGANZA SUAREZ
Revisado y aprobado por:	Ing. Patricio Padrón **Director de Tecnologías de la Información y Comunicación**	Firmado electrónicamente por: NARDO PATRICIO PADRON CORREA

ÍNDICE

1. Notas de Cambio

Versión	Fecha	Detalle de la modificación
1	16/11/2021	Creación del registro

2. Antecedentes

El Esquema Gubernamental de Seguridad de la Información (EGSI), establece una serie de hitos que contemplan la elaboración, implementación y difusión, de políticas, procedimientos, reglamentos, normas y demás instrumentos técnicos, que garanticen el manejo seguro de la información de las instituciones públicas.

Con el fin de garantizar la seguridad de la información institucional, entre otras acciones, el Secap viene manejando un repositorio que, mediante scripts, guarda una copia de los logs de sistemas y plataformas institucionales; y, para la verificación y control de las actividades de los usuarios y posibles eventos de sistemas operativos, se está implementando Active Directory.

3. Alcance

El registro aquí descrito es de uso exclusivo de la Dirección de Tecnologías de la Información y Comunicación; por lo que al alcance del mismo es a dicha instancia del Secap.

4. Propósito

Establecer los lineamientos para registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

5. Definiciones

- **Análisis de log:** Estudio de los logs para identificar eventos de interés o suprimir entradas de eventos insignificantes.
- **Aplicaciones de software:** Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
- **Evento:** Una alerta o notificación creada por algún componente de la plataforma tecnológica de la información o herramienta de monitoreo.

- **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.
- **Internet:** Red mundial de computadores conectadas entre sí que ofrecen acceso y comparten información a través de un lenguaje común.
- **Intranet:** Red informática interna basada en los estándares de internet.
- **Log:** Es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema. Se utiliza en muchos casos distintos, para guardar información sobre la actividad de sistemas variados.
- **Registro de eventos:** Es un documento que registra datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre en un dispositivo en particular, aplicación o sistema.
- **Seguridad del sistema:** Conjunto de medidas preventivas y correctivas que permiten resguardar y proteger la información y los sistemas de software que la procesan y almacenan.
- **Servicios:** Conjunto de aplicativos o programas informáticos y de comunicación de datos que apoyan la labor del Secap.
- **Servidor/funcionario:** Persona que presta servicios a la Administración o a nombre y por cuenta de esta, como parte de su organización, en virtud de un acto válido y eficaz de investidura, con entera independencia del carácter imperativo, representativo, remunerado, permanente o público de la actividad respectiva.
- **Sistema de software:** Programas informáticos diseñados con el propósito de facilitar a los usuarios la realización de determinadas tareas.
- **Usuario:** Nombre o identificador compuesto por una cadena de caracteres alfanuméricos, que emplea una persona para identificarse en un sistema, equipo o red, previo a ingresar la contraseña.

6. Políticas

- La Dirección de Tecnologías de la Información y Comunicación implementará las acciones necesarias para elaborar, preservar y revisar los registros de actividades de eventos (logs) de los usuarios y de los sistemas del SECAP.
- Los analistas de la Dirección de Tecnologías de la Información y Comunicación no están facultados para modificar, borrar o desactivar registros (logs) de sus equipos, ni de los usuarios de los sistemas y plataformas del SECAP. De igual forma, se deben realizar las configuraciones de seguridad necesarias para evitar la eliminación o cambios no autorizados a los registros de información.
- El acceso a los registros (logs) es restringido y está bajo la responsabilidad del administrador del Data Center.
- Para consultas por usuarios específicos, se lo hará únicamente con autorización previa del director de Tecnologías de la Información y Comunicación.
- La consulta y copia de la información de registros por personas ajenas a la institución que requieran con fines probatorios, debe ser solicitada al Director Ejecutivo para que sea evaluada por la parte legal de la institución.
- Todos los sistemas, plataformas, aplicativos, bases de datos, dispositivos de comunicación dispositivos de seguridad y servidores, deben tener activados los logs.
- Es responsabilidad de administrador del Data Center, estar pendientes de la activación de los logs en los distintos sistemas.
- El uso y la configuración de una herramienta o su generación para la gestión de logs será aprobada por el Director de Tecnologías de la Información y Comunicación, quien será responsable de asignar responsabilidades de parametrización de la herramienta que se utilice para el respaldo de logs.
- El gestor de Seguridad y Componentes de servicios de TI, será el responsable de autorizar permisos de acceso a la herramienta que se utilice para el respaldo de logs, únicamente para efectos de revisiones e investigaciones.
- La Dirección Tecnologías de la Información y Comunicación implementará la sincronización de relojes de los sistemas a un único servidor NTP (Nertwork Time Protocol –protocolo de tiempo en la red), para que la generación de logs sea coordinada.

- El encargado del Data Center generará un documento donde se indique las condiciones y tipo de almacenamiento que será usado para el resguardo de los logs y el tiempo en disco de los registros existentes, el cual dependerá de la cantidad de espacio disponible. Para el efecto, se considerará la herramienta que la institución dispone, teniendo en cuenta todos los componentes de la plataforma tecnológica del Secap, ya que estos se constituyen en evidencia para la identificación de un incidente de seguridad.
- El encargado del Data Center mantendrá un inventario de los registros existentes por aplicación en caso de una posible auditoría.
- La revisión y/o restauración de los registros será de forma periódica y aleatoria, por incidentes determinados o por requerimiento de alguna dirección especifica.
- La emisión o generación de un informe con las estadísticas, será efectuada por el encargado del Data Center, se la realizará periódicamente de acuerdo a los recursos y necesidades que tenga la institución.

7. Anexos

Ninguno.