ALCALDÍA MAYOR DE BOGOTÁ D.C.
MOVILIDAD
Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

FORMATO DE APROBACIÓN DOCUMENTAL

CÓDIGO: DESI-FM-008 | **VERSIÓN: 10**

FECHA DE APLICACIÓN: ENERO 2019

INFORMACIÓN DOCUMENTADA:		CÓDIGO:		VERSIÓN:		JUSTIFICACIÓN:		
TIPO	NOMBRE	ANTERIOR	VIGENTE	ANTERIOR	VIGENTE	ELABORA	ACTUALIZA	ANULA
Documento Interno	Política de Protección de Datos Personales	EGTI-DI-001	EGTI-DI-002	1	2		X	
Documento Interno	Políticas de seguridad de protección y respaldo de información	GSIT-DI-001	EGTI-DI-003	1	2		X	
Documento Interno	Política de Seguridad para la Gestión de Contraseñas	GSIT-DI-002	EGTI-DI-004	1	2		X	
Documento Interno	Políticas de escritorio limpio y bloqueo de pantallas	GSIT-DI-003	EGTI-DI-005	1	2		X	
Documento Interno	Política de Protección Contra Software Nocivo	GSIT-DI-004	EGTI-DI-006	1	2		X	
Documento Interno	Política buen uso de correo institucional	GSIT-DI-005	EGTI-DI-007	1	2		X	
Documento Interno	Política de Navegación en Internet	SIT-DI-003	EGTI-DI-008	1	2		X	
Documento Interno	Política de Seguridad para el registro histórico de actividades (LOGS)	-	EGTI-DI-009	-	1	X		

DESCRIPCIÓN DE LA JUSTIFICACIÓN:

Teniendo en cuenta el cambio de la plataforma estratégica de la Entidad, se realiza la recodificación de los documentos anteriormente citados, dado que estos anteriormente pertenecían al proceso de apoyo SIT y en la actualidad, por tratarse de políticas de seguridad de la información pasan al proceso estratégico.

Se crea la política EGTI-DI-009 Seguridad para el registro histórico de actividades (LOGS), lo cual permitirá que al tener identificados los sistemas de información y elementos de hardware que hacen parte de la infraestructura tecnológica de la Unidad, los cuales tendrán configurado el registro de eventos para que este pueda ser revisado en caso de presentarse algún incidente que afecte la continuidad de la operación de los procesos de la entidad.

AVALA: RESPONSABLE DIRECTIVO SIG	ELABORA/ACTUALIZA/ANULA: *(Colaborador del proceso en compañía del enlace)*	ACOMPAÑAMIENTO: EQUIPO TÉCNICO SIG
(Firma)	*(Firma)*	*(Firma)* Andrea del P. Zambrano
Nombre: Marcela Rocío Márquez Arenas	*Nombre: Gloria Méndez/ Omar Fernando Garzón*	*Nombre: Andrea del Pilar Zambrano*
Cargo: Secretaría General	*Cargo: Contratistas Proceso EGTI*	*Cargo: Contratista Proceso DESI*

TRÁMITE DE APROBACIÓN DOCUMENTAL (DILIGENCIADO POR LA OFICINA ASESORA DE PLANEACIÓN)	¿ES APROBADO?	FECHA DE APROBACIÓN:	RESPONSABLE DEL SISTEMA DE GESTIÓN DE CALIDAD
	SI [X] NO [ ]	29-04-19	*(Firma)*
	OBSERVACIONES:		*Martha Patricia Aguilar Copete*
	La política EGTI-DI-006, queda con el código EGTI-DI-010, dado que tal el 6 está asignado.		***REPRESENTANTE DE LA ALTA DIRECCIÓN PARA EL SIG***

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

POLÍTICA DE SEGURIDAD PARA EL REGISTRO HISTÓRICO DE ACTIVIDADES (LOGS)

Bogotá, D.C.,

(MAYO DE 2019)

CONTENIDO

1. INTRODUCCIÓN

El siguiente documento hace parte de la POLÍTICA GENERAL DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES de la entidad.

La UAERMV Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, basará la Administración de la Seguridad de los Activos de Información, en las políticas contenidas en este documento; así mismo, como las buenas prácticas y herramientas informáticas que apoyen el proceso de apoyo: "Gestión de Servicios de Infraestructura Tecnológica" (GSIT).

Los sistemas registran la actividad de los usuarios y de sus procesos internos como el inicio de sesión y cierre de sesión en un equipo de cómputo (login/logout, origen, tiempo de actividad, acciones, conexiones,) en registros de eventos o logs. La información de estos registros es esencial para elaborar informes de gestión, para monitorización o en caso de presentarse un incidente, poder realizar una auditoria.

Entre los eventos que los distintos sistemas registran están, por ejemplo: El inicio/fin de sesión, el acceso y modificación de ficheros y directorios, cambios en las configuraciones principales, ejecución de programas, etc. Los registros de actividad de los distintos sistemas y equipos son los datos a partir de los cuales es posible no sólo detectar fallos de rendimiento o mal funcionamiento, sino también detectar errores e intrusiones. Con ellos se alimentan sistemas de monitorización que configurados correctamente pueden generar alertas en tiempo real. Por otra parte, facilitan el análisis forense para el diagnóstico de las causas que originan los incidentes.

Por último, son necesarios para verificar el cumplimiento de ciertos requisitos legales o contractuales durante las auditorías.

2. GLOSARIO DE TERMINOS

- **Correlacionador de eventos:** Es una consola potente y de alto rendimiento, que reúne los datos de los eventos de seguridad, amenazas y riesgos de los aplicativos y dispositivos de hardware para proporcionar la mayor información de seguridad, lograr respuestas rápidas a los incidentes, gestionar los registros de forma sencilla y generar reportes de cumplimiento.

- **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo.
- **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.
- **IDS:** Sistema de detección de intrusos.
- **LOGS:** También conocidos como registros de actividades o de eventos en algún sistema de información.
- **MAC:** *Media Access Control*) es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (4 bits)) que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo de red.
- **NTP:** Network Time Protocol, protocolo de sincronización de tiempo.
- **Usuario:** Persona que utiliza los servicios diarios.

3. OBJETIVO GENERAL

Identificar los sistemas de información y elementos de hardware que hacen parte de la infraestructura tecnológica, los cuales deben tener configurado el registro de eventos para ser revisado en caso de presentarse algún incidente que afecte la continuidad de la operación de los procesos de la entidad.

4. OBJETIVOS ESPECIFICOS

1. Determinar los eventos más significativos dentro de los sistemas de información que deben de ser registrados, y la manera en que ha de efectuarse dicho registro.
2. Establecer mecanismos de monitorización que permitan la detección de intrusiones, errores y situaciones anómalas o potencialmente peligrosas.

5. ALCANCE

El alcance de los lineamientos que se definen en esta política da cubrimiento a los accesos que involucren:

a) Acceso a alguno de los siguientes sistemas:
   - Bases de datos.
   - Aplicativos.
   - Sistemas de información.

- Elementos de infraestructura tecnológica (Firewall, Router, Switch...).
- Equipos de cómputo.
- Servidores de datos.

Aplica para todos los Servidores Públicos de la Unidad: Empleados públicos de planta (de carrera administrativa y los provisionales), funcionarios de libre nombramiento y remoción, trabajadores oficiales, contratistas y demás personal que tenga asignado un usuario y contraseña para el ingreso a algunos de los sistemas de información, bases de datos, equipos de cómputo o aplicativos que soliciten la autenticación. Estos deberán preservar la confidencialidad de la información de la UAERMV, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de salvaguardar la información; así como están obligados a continuar protegiendo y cumpliendo los acuerdos de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la UAERMV.

Se tendrán en cuenta para esta política especifica los controles A.14.4 registro y seguimiento tomado de la norma ISO 27001:2013.

6. DECLARACIÓN

En este documento se encuentran los lineamientos que aseguran una actuación adecuada para alcanzar un alto nivel en cuanto a seguridad de la información en la UAERMV. La información es un activo importante para la entidad, tiene un alto valor para la misma, por esto mismo la unidad ha definido las directrices de seguridad para los Activos de Información, por medio de las cuales se deben orientar todas las acciones a seguir.

Estas directrices hacen parte del marco de POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE INFORMACIÓN Y COMUNICACIONES y están basadas en la NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la *International Organization for Standardization* y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013).

Por lo anterior, se busca minimizar riesgos en la información, asegurar la continuidad de la UAERMV y ayudar en el cumplimiento de los objetivos misionales.

Acuerdo de confidencialidad:

Todos los Usuarios que administran, leen, modifican o crean información en la UAERMV deben firmar un acuerdo de confidencialidad o de no divulgación como parte de sus términos y condiciones iníciales de empleo. Esta directriz también incluye a personal ocasional y los Usuarios externos no contemplados en un contrato formalizado.

7. ROLES Y RESPONSABILIDADES

7.1. Encargado de seguridad de la información: Persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información a la UAEMRV y supervisar el cumplimiento de la presente Política.

7.2. Usuarios de la información. Personas que tiene asignado un equipo de cómputo y/o escritorio de trabajo quienes deberán dar cumplimiento a los procedimientos que se deriven de esta Política.

8. POLÍTICA DE SEGURIDAD PARA LA GESTION DE LOGS

- Todos los sistemas de información y aplicativos deben estar sincronizados correctamente con un servidor de tiempo NTP con la hora legal colombiana, de este modo se garantiza el correcto registro temporal de los eventos o sucesos más relevantes.
- Se debe tener un sistema de gestión de logs adecuado, el cual puede ser un correlacionador, de eventos configurado con los dispositivos de hardware y aplicativos más importantes de la entidad el cual centralice los logs.
- Los logs o registros de eventos deben almacenarse y ser incluidos en la política de seguridad de la información y respaldo de la información de la entidad para poderla recuperar en caso de pérdida.
- Se deben definir roles y responsabilidades para el proceso de gestión de logs.

Actividades que deben ser registradas.

Para obtener la información crítica sobre el funcionamiento de los activos de información, se deben analizar las actividades mas relevantes que se deben registrar como los siguientes:

- Acceso, creación, borrado y actualización de información confidencial que repose en los sistemas de información e infraestructura tecnológica.
- Inicio y fin de conexión en los dispositivos de red de la entidad.
- 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 inesperada de los aplicativos.
- Accesos de usuario.
- Acceso privilegiado o administrativo.
- Uso de mecanismos de autenticación e identificación.
- Accesos remotos e inalámbricos.
- Cambios de privilegios de acceso.
- Uso de utilidades del sistema.
- Activación o desactivación de sistemas de seguridad.
- Accesos a registros de auditoria.
- Aproximación a los límites de uso de los recursos físicos de hardware.
    - Memoria RAM
    - Capacidad de disco.
    - Ancho de banda de red
    - Uso del procesador de la CPU.
- Indicios de actividad sospechosa detectada por los sistemas de antivirus.
- Indicios de actividad sospechosa detectada por el sistema de detección de intrusos (IDS).
- Transacciones relevantes dentro de los aplicativos.

Información relevante incluida en el registro.

Los elementos de información más útiles que deben ser incluidos en los distintos registros son:

- Identificador del usuario que realiza la acción.
- Identificación del elemento sobre el que se realiza la acción (ficheros, bases de datos, equipos, etc.).
- Identificación de dispositivos, ya sea a través de sus direcciones IP, direcciones MAC.
- Identificación de protocolos.
- Fecha y hora de ocurrencia del evento.
- Tipificación del evento.

Elaborado y/o Actualizado por EQUIPO OPERATIVO SIG del Proceso:	Validado por RESPONSABLE DIRECTIVO SIG del Proceso:	Aprobado por:
OMAR FERNANDO GARZON / GLORIA MENDEZ Contratistas / Proceso EGTI		
Acompañamiento EQUIPO TÉCNICO SIG:	Firma:	Firma:
ANDREA DEL PILAR ZAMBRANO Contratista/ Proceso DESI	MARCELA ROCIO MARQUEZ ARENAS (Secretaria General)	MARTHA PATRICIA AGUILAR COPETE Representante de la Alta Dirección

CONTROL DE CAMBIOS:

VERSIÓN	DESCRIPCIÓN	FECHA	APROBADO Representante de la Alta Dirección SIG
1	Elaborada por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), se realizó el documento de Política de seguridad para la gestión de LOGS que hace parte de la POLITICA GENERAL DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION Y COMUNICACIONES.	Mayo 2019	Jefe Oficina Asesora de Planeación