HOJA DE APROBACIÓN

	Preparado Por:	Revisado Por:	Aprobado Por:
Nombre:	Leidy Lorena Urbano Ardila	Alberto Mario Solano Wilmack Sánchez Juan Pablo Vanegas Samuel Córdoba Grace Jiménez	Darleny Consuelo Fajardo Cuadrado José Fernando Castillo Canon
Cargo:	Profesional Especializado Dirección de Seguimiento y Mejoramiento de Procesos	Oficial Seguridad de la Información Asesor Seguridad Informática Profesionales Especializados Dirección de Seguimiento y Mejoramiento de Procesos	Directora de Seguimiento y Mejoramiento de Procesos Director de Gestión de Tecnologías de la Información
Fecha:	30 de Junio de 2016	27 de Julio de 2016	28 de Julio de 2016

HOJA DE CONTROL DE CAMBIOS

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
1.0	Creación	28/07/2016	Creación del documento	Todos	Leidy Lorena Urbano

TABLA DE CONTENIDO

1 OBJETIVO 3
2 PROCESO O SUBPROCESO AL CUAL PERTENECE 3
3 ALCANCE 3
4 NORMAS GENERALES 3
5 NORMAS ESPECÍFICAS 4
5.1 Responsabilidades 4
5.1.1 Dirección de Gestión de Tecnologías de la Información. 4
5.1.2 Seguridad de la Información 5
5.2 Estándar de activación de Logs de seguridad de la información. 5
5.3 Criterio de activación de Logs de diagnóstico de los componentes de infraestructura tecnológicos. 6
5.4 Criterio de activación de Logs de acceso físico 6
5.5 Almacenamiento, transporte y consulta de Logs. 6
5.6 Acceso a los Logs 7
5.7 Eliminación de Logs 7
5.8 Monitoreo y revisión de Logs. 7
6 GLOSARIO 7

1 OBJETIVO

Establecer las directrices para la gestión de los registros de operación (logs de seguridad de la información, logs de diagnóstico y logs de acceso físico), su generación, almacenamiento, análisis, diagnóstico y la ejecución de las acciones de monitoreo periódico y/o de investigaciones, que permitan garantizar el principio de Auditabilidad ante la ocurrencia de eventos de Seguridad de la Información sobre los activos de información de La Unidad.

2 PROCESO O SUBPROCESO AL CUAL PERTENECE

AP-SUB-007 Subproceso Gestionar Seguridad de la Información

3 ALCANCE

Esta política solo contempla la gestión de logs de seguridad, de diagnóstico, de acceso físico y aplica para los activos de información de La Unidad a cargo de funcionarios, contratistas, proveedores, entendiendo como:

- Funcionario: Personal vinculado a la planta de personal de la UGPP.
- Contratista: Persona natural contratada por La Unidad para la ejecución de tareas específicas.
- Proveedor: Persona Jurídica contratada por La Unidad para la prestación de servicios.

4 NORMAS GENERALES

a) El responsable de esta política es el Oficial de Seguridad de la Información, quien es el encargado de garantizar el mejoramiento continuo de la misma.

b) Esta política considera como *log*, todo rastro almacenado sobre un registro de la plataforma tecnológica de las acciones concernientes a operaciones y/o acontecimientos que ocurren sobre un activo de información o sistema de información tecnológico de La Unidad, cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar.

c) Los componentes de la infraestructura tecnológica de la UGPP (v.gr. sistemas operativos, bases de datos, servicios, aplicativos, equipos de telecomunicaciones), deberían generar y almacenar registros de las actividades, acciones, operaciones, y/o transacciones que se ejecuten en ellos. Lo anterior, según concepto expreso por la Oficina de Seguridad de la Información, considerando los niveles de riesgos asociados a dichos componentes.

d) Las directrices dispuestas en esta política, se deben tener presentes para la fase de diseño de nuevos sistemas de información para La Unidad y deberán mantenerse

durante su ciclo de vida, sin importar la arquitectura tecnológica o metodología de desarrollo aplicadas.

e) En aquellos casos en que no se pueda implementar o cumplir alguno de los lineamientos expuestos en el presente documento por restricciones tecnológicas, la Dirección de Gestión de Tecnologías de la Información deberá documentar la excepción y presentar un plan para dar tratamiento alternativo que incluya la descripción de las actividades, fechas y responsables, de manera que los riesgos asociados se mantengan en niveles aceptables. Este plan de tratamiento se deberá presentar al Oficial de Seguridad de la Información para su correspondiente análisis y evaluación y recomendaciones en caso que el riesgo se mantenga en un nivel no aceptable.

f) El acceso de cada usuario a los sistemas de información de La Unidad, debería ser registrado, al igual que las actividades, acciones, operaciones, y/o transacciones que ejecute sobre los mismos, según el nivel de riesgo identificado por parte de la Oficina de Seguridad de la Información.

5 NORMAS ESPECÍFICAS

5.1 Responsabilidades

5.1.1 Dirección de Gestión de Tecnologías de la Información.

a) Facilitar y garantizar las condiciones tecnológicas que permitan el registro, tratamiento, almacenamiento y gestión de los Logs expuestos en esta política (Numerales 5.2, 5.3 y 5.4), en la infraestructura de La Unidad o a través de un servicio contratado, alineándose a lo dispuesto en la "*Política Específica de Seguridad de la Información para Proveedores y Terceros AP-PIT-005*".
b) Establecer los mecanismos (físicos y/o lógicos) de control de acceso a la información contenida de los Logs, para que solo sean consultados por el personal autorizado de La Unidad.
c) Hacer uso de la presente política como parte de sus herramientas de gobierno y de gestión, así como definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento sobre los servicios contratados con terceros, en donde se encuentren alojados los activos de información de La Unidad.
d) Cuando un proveedor sea el responsable de la administración de la infraestructura tecnológica de la UGPP o de sistemas de información o componentes, es responsabilidad de la DGTI asegurar que el provedor atienda las solicitudes de explotación y tratamiento de Logs de seguridad de la información y de diagnóstico de los componentes de infraestructura tecnológica.

5.1.2 Seguridad de la Información

a) Conceptuar a partir de los riesgos identificados para cada activo de información sobre la viabilidad técnica para la implementación de registros de auditoria de cada uno de los mismos.
b) Generar directrices y actividades de monitoreo sobre los sistemas de información, administrados por La Unidad y por los proveedores contratados.
c) Ejecutar actividades de monitoreo a partir de los registros generados por los distintos componentes tecnológicos para la identificación de eventuales incidentes de seguridad de la información.
d) Solicitar la generación y configuración de registros de auditoría en los distintos componentes de la infraestructura tecnológica de La Unidad.

5.2 Estándar de activación de Logs de seguridad de la información.

Las operaciones desarrolladas sobre los activos de información o componentes tecnológicos, deben mantener el registro y la trazabilidad de las acciones o eventos realizados sobre la información y su administración. Por lo cual los eventos deberían ser registrados con las siguientes características:

a) Para la gestión de Usuarios en los sistemas de información es necesario contar con la siguiente información del Evento:
   - Inserción. (Usuario, Permiso, Rol, Perfil).
   - Modificación. (Usuario, Permisos, Roles, Perfiles).
   - Inactivación (Usuario, Permiso, Rol, Perfil).
   - Inicio de sesión (Exitoso, Fallido).
   - Fecha y hora exacta de ejecución de la acción.
   - Usuario que ejecuta la acción.
   - Equipo desde el que se ejecuta la acción (Hostname, dirección IP).
   - Operación realizada.
   - Estado anterior y estado nuevo del registro modificado.
   - Identificación del sistema de información.

b) Para la gestión de la información almacenada en los sistemas de información, es necesario contar con los siguientes datos del Evento:
   - Inserción/Modificación/Eliminación (por ejemplo: inserción de reglas de filtrado, de IDPS, FW o cambios de configuración de un aplicativo, BD, repositorio)
   - Consulta información de la aplicación y/o plataforma.
   - Fecha y hora exacta del evento.
   - Usuario que ejecuta la acción.
   - Equipo desde el que se ejecuta la acción (Hostname, dirección IP).
   - Operación realizada (descripción del evento).
   - Estado anterior y estado nuevo del registro modificado.
   - Código del sistema de información.
   - Versión del sistema de información.

5.3 Criterio de activación de Logs de diagnóstico de los componentes de infraestructura tecnológicos.

La Dirección de Gestión de Tecnología de Información debe realizar las configuraciones necesarias para que los distintos componentes tecnológicos generen registros que permitan realizar diagnósticos sobre el desempeño de los mismos (v.gr. almacenamiento, procesamiento, recurrencia de conexiones, entre otros), los cuales podrán ser consultados por la Oficina de Seguridad de la Información.

5.4 Criterio de activación de Logs de acceso físico

Para la Gestión de control de acceso físico de personas a áreas en donde se encuentren sistemas de información de La Unidad, es necesario contar con la siguiente información del Evento, registrando los datos de forma manual en medios físicos:

- Nombre y apellidos del visitante (Funcionario, Contratista, Proveedor, Tercero, Subcontratista).
- Número de documento del visitante (Funcionario, Contratista, Proveedor, Tercero, Subcontratista).
- Área de la Unidad en la que labora o Empresa proveedora a la que pertenece.
- Motivo del acceso.
- Fecha y Hora exacta del ingreso al sitio.
- Fecha y Hora exacta de Salida del sitio.
- Firma del visitante. (Funcionario, Contratista, Proveedor, Tercero, Subcontratista)
- Nombre y apellidos del funcionario de la UGPP que autoriza el acceso físico del visitante, si aplica.
- Firma del funcionario de la UGPP que autoriza el acceso físico del visitante, si aplica.

5.5 Almacenamiento, transporte y consulta de Logs.

a) Los Logs de seguridad de la información y de diagnóstico de los componentes de infraestructura tecnológica, estarán conservados y disponibles de acuerdo al tiempo definido entre la Dirección de Gestión de Tecnología de Información y la Oficina de Seguridad de la Información.

b) Todo Log debe ser protegido en su trasmisión y almacenamiento acorde a los lineamientos dispuestos en la "*Política Específica de Seguridad para el tratamiento y protección de información clasificada AP-PIT-008*", empleando los mecanismos de cifrado descritos en la "*Política Específica para la implementación y uso de controles criptográficos AP-PIT-009*".

5.6 Acceso a los Logs

La Dirección de Gestión de Tecnología de Información debe restringir el acceso a registros de los componentes de infraestructura tecnológica que contengan sistemas de información de la entidad, con el propósito de que solo esta información sea accedida por el personal autorizado (Administradores de plataforma y/o servicios, Oficina de Seguridad de la Información y entes de control).

5.7 Eliminación de Logs

Los Logs de seguridad de la información y de diagnóstico de los componentes de infraestructura tecnológicos antigüedad sea mayor a dos (2) años, deben ser eliminados de manera segura aplicando los lineamientos de la "*Política Específica de Seguridad para el Tratamiento y Protección de Información Clasificada AP-PIT-008*", con excepción de:

- Logs correspondientes a los aplicativos que soportan los negocios misionales y/o hayan sido catalogados como críticos para La Unidad.
- Logs correspondientes a los casos o eventos que se estén investigando por parte de entes judiciales o al interior de la entidad.

5.8 Monitoreo y revisión de Logs.

Para el monitoreo de Logs de seguridad de la información y de diagnóstico de los componentes de infraestructura tecnológicos, se debe dar cumplimiento a los lineamientos definidos en la "*Caracterización de Monitoreo de Políticas de Seguridad de la Información*" y para el monitoreo de usuarios y roles se debe considerar lo establecido en la "*Política Específica de Gestión de Acceso Lógico AP-PIT-001*".

La Oficina de Seguridad de la Información realizará revisiones con el fin de investigar, reportar incidentes y mitigar riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información de los distintos procesos de La Unidad.

6 GLOSARIO

- **Activo de Información:** Toda la información en formato físico o digital y todo aquel elemento lógico o físico, mediante el cual se pueda procesar, almacenar, visualizar, crear o transmitir información y que tiene valor para la entidad.

- **Análisis:** Es el procedimiento en el cual se examinan los registros en bruto del sistema de información con el propósito de determinar qué tipo de acciones se efectuaron sobre el activo de información de interés.

- **Borrado seguro:** Método para sobrescribir la información a través de herramientas especializadas, no permitiendo que ésta se pueda recuperar posteriormente.

- **Cifrado de archivos:** Proceso por el que una información legible se transforma mediante un algoritmo en información ilegible, para evitar ser leída por sistemas o personas no autorizadas.

- **Contratista:** Persona natural contratada por la UGPP para la ejecución de tareas específicas.

- **Componentes de la infraestructura tecnológica:** Activos de información referentes a plataformas tecnológicas tales como bases de datos, servidores de aplicaciones, dispositivos de red, plataformas tecnológicas, etc.

- **Diagnóstico:** Se define como el o los resultados entregados a partir de un estudio, evaluación o análisis sobre determinados registros de los activos y/o sistemas de información. El diagnóstico tiene como propósito reflejar con claridad un escenario para luego proceder a elaborar y ejecutar una acción o tratamiento para sanear la situación, si aplica.

- **Información privada:** Activo de información restringido, disponible sólo para un grupo de personas dentro o fuera de La Unidad (definido por el propietario) y que en caso de ser conocido por terceros sin autorización puede conllevar un impacto negativo para el ciudadano, operativo, económico, de imagen, y/o legal para la entidad.

- **IDS / IPS:** Control para la detección y prevención de accesos no autorizados a un equipo o a una red.

- **Logs de control de acceso físico:** Este tipo de Logs registra los datos del personal que accede de manera física a zonas de acceso restringido.

- **Logs de Seguridad:** Este tipo de Log registra sucesos que tengan relación directa con la disponibilidad, confidencialidad, e integridad de la información.

- **Proveedor:** Persona Jurídica contratada por la UGPP para la prestación de servicios.

- **Software malicioso**: Programas malintencionados que tienen como objetivo infiltrase o dañar el sistema de información.

- **Subcontratista:** Empresa o persona natural subcontratada para realizar tareas específicas a nombre del Proveedor originalmente contratado.

- **Tercero:** Personal contratado por una empresa proveedora para la ejecución del servicio contratado.