HOJA DE APROBACIÓN

	Preparado Por:	Revisado Por:	Aprobado Por:
Nombre:	Juan Pablo Vanegas	Alberto Mario Solano Jiménez Wilmack Sánchez	Darleny Consuelo Fajardo Cuadrado
Cargo:	Profesional Especializado Dirección de Seguimiento y Mejoramiento de Procesos	Oficial de Seguridad de la Información Contratista Asesor Seguridad TICs	Directora Seguimiento y Mejoramiento de Procesos
Fecha:	9 de Junio de 2017	13 de Junio de 2017	20 de Junio de 2017

HOJA DE CONTROL DE CAMBIOS

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
1.0	Creación	31/07/2011	Creación del documento	Todos	Alberto Solano
2.0	Modificación	29/07/2016	Modificación del numeral 5.3, en donde se asocia la política específica para la gestión de logs de seguridad de la información y se establece el alcance de activación de logs de seguridad a los sistemas de información según niveles de riesgo y concepto de seguridad de la información.	5.3	Samuel Córdoba
3.0	Modificación	20/06/2017	En el numeral 4, se adiciona el literal h). En el numeral 5.2 Control de Acceso, se modifica literal e, para relacionarlo con la POLÍTICA ESPECÍFICA DE GESTIÓN DE ACCESO LÓGICO AP-PIT-001 En el numeral 5.2 Control de Acceso, se modifica el literal g). Se modifica el numeral 5.3 literal a) para relacionarlo con la POLÍTICA ESPECÍFICA PARA LA GESTIÓN DE LOGS DE SEGURIDAD DE LA INFORMACIÓN (AP-PIT-007).	4 h. 5.2, e. g. 5.3. a.	Juan Pablo Vanegas

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 Protección de la información....4
5.2 Control de acceso....4
5.3 Registro y auditoria....6
5.4 Evaluación y atención de vulnerabilidades....6
5.5 Manejo de Sesión....6
5.6 Planes de restauración....7

6 GLOSARIO....7

1 OBJETIVO

Establecer los lineamientos y estándares de seguridad de la información para el desarrollo y/o adquisición de sistemas de información en La Unidad.

2 PROCESO O SUBPROCESO AL CUAL PERTENECE

AP-SUB-007 Subproceso Gestionar Seguridad de la Información

3 ALCANCE

La política aplica para todos los proyectos de desarrollo y/o adquisición de sistemas de información que se adelanten en La Unidad. Para el caso de sistemas de información recibidos de otras entidades, estos deberán cumplir con esta política, en la medida en que su nivel de criticidad así lo requiera.

4 NORMAS GENERALES

a. El dueño de esta política es el Oficial de Seguridad de la Información, quien es el responsable de garantizar el mejoramiento continuo y autorizar cualquier cambio sobre la misma.

b. Los lineamientos establecidos en este documento, se deben observar en la fase de diseño o evaluación de los sistemas de información y se deben mantener durante su ciclo de vida sin importar la arquitectura tecnológica o metodología de desarrollo aplicada.

c. La definición de los requisitos de seguridad de los sistemas de información se debe realizar con la participación de los responsables del tratamiento de la información, siguiendo los lineamientos expuestos en este documento.

d. Si no es posible implementar o dar cumplimiento a alguno de los requerimientos expuestos en este documento dadas las restricciones tecnológicas del sistema de información o de la plataforma tecnológica de La Unidad, se debe documentar la excepción, los riesgos generados —estos analizados y evaluados por el Oficial de Seguridad de la Información— y se deben implementar medidas o controles complementarios que permitan dar el tratamiento apropiado a dichos riesgos, los cuales deben ser aceptados expresamente por el responsable del tratamiento, por el no cumplimiento del requerimiento de seguridad.

e. La documentación de diseño de la arquitectura tecnológica de los sistemas de información, los casos de uso de seguridad y de los controles seguridad, se deben encontrar disponibles para análisis y evaluación por parte del Equipo de Seguridad de la Información.

f. El acceso a la documentación de diseño e implementación de los sistemas de información (código fuente, documentos de diseño, especificaciones funcionales, etc.) debe ser restringido y únicamente autorizado para el personal que por una necesidad de negocio, requiera conocerla. En tal sentido, el único responsable para autorizar el acceso a esta información, es el Director de Gestión de Tecnologías de la Información.

g. El despliegue de sistemas de información en el ambiente productivo debe acatar lo definido en los procesos definidos por la Dirección de Gestión de Tecnologías de la Información para tal propósito. Asimismo, se requiere validación y concepto expreso del cumplimiento de los requisitos de seguridad por parte del Equipo de Seguridad de la Información.

h. Antes de que un sistema de información nuevo entre a producción, éste deberá ser puesto en conocimiento de la Oficina de Seguridad de la Información por parte de la Dirección de Gestión de Tecnologías de la Información, con el fin de realizar el análisis de vulnerabilidades y de penetración pertinentes.

5 NORMAS ESPECÍFICAS

5.1 Protección de la información.

En cuanto a la protección de la información gestionada en los sistemas de información, como mínimo se deben cumplir y documentar los siguientes requisitos:

a. El sistema de información debe ser clasificado por el responsable del tratamiento, en términos de confidencialidad, integridad y disponibilidad, según la Metodología para la Gestión de Activos de Información AP-INS-005.

b. Se debe identificar el requerimiento de respaldo de la información, de acuerdo al proceso de respaldo definido por la Dirección de Gestión de Tecnologías de la Información, considerando aspectos tales como: tipo de respaldo, frecuencia de toma, tiempo de retención, rutas a respaldar, entre otros.

c. Se deben implementar mecanismos seguros de comunicación entre los componentes (aplicación, bases de datos, sistemas operativos) de los sistemas de información, que permitan contar con niveles adecuados de confidencialidad, integridad y no repudio de la información.

5.2 Control de acceso.

Se deben considerar los siguientes lineamientos de control de acceso en los sistemas de información:

a. La capa de autenticación debe ser integrada con el servicio de Controlador de Dominio (Directorio Activo), a fin de manejar un repositorio único de usuarios y aplicar las políticas allí disponibles. En caso de que la arquitectura requiera el manejo de un repositorio independiente de usuarios, los usuarios se deben crear a nivel de aplicación y no de bases de datos. Si la arquitectura de la aplicación requiere la creación de usuarios directos en la base de datos, el acceso de inicio de sesión y/o permisos a tablas deberán ser restringidos en su totalidad, a fin de evitar inconsistencias entre los controles a nivel de aplicación y de bases de datos.

b. Los sistemas de información deben basar su capa de autorización en roles, de manera que cada usuario pueda ser asociado a uno —o varios roles— (grupo de actividades), a los que a su vez se asocian perfiles (funcionalidades, programas, etc.) y permisos (lectura, escritura, modificación, y eliminación).

c. Para el acceso a los sistemas de información se debe acatar lo definido en l*a POLÍTICA ESPECÍFICA DE GESTIÓN DE ACCESO LÓGICO AP-PIT-001,* la cual define las directrices para la creación, modificación, inactivación y monitoreo de usuarios y roles en La Unidad.

d. Previo al paso a producción de un sistema de información se debe definir lo siguiente:

   - Áreas usuarias (áreas de La Unidad con derecho de acceso al sistema de información).
   - Roles de acceso de usuarios funcionales segregados dentro de la aplicación, de acuerdo a la necesidad de acceso a la información.
   - Roles de acceso de usuarios administradores segregados por función (por ejemplo, parametrización, administración de usuarios, y administrador de roles).
   - Responsable del tratamiento.

e. Los sistemas de información deben implementar los parámetros de contraseñas establecidas en el numeral 6.3.2 del documento *AP-PIT-001 POLÍTICA ESPECÍFICA DE GESTIÓN DE ACCESO LÓGICO,* ya sea que la capa de autenticación se encuentre localmente en la aplicación o se realice a través del Directorio Activo.

f. Se deben considerar mecanismos de autenticación fuerte, tales como tokens, tarjetas inteligentes, lectores biométricos, entre otros, dependiendo de la criticidad de la información a la cual se controla el acceso.

   - Los sistemas de información deben incluir funcionalidades que permitan restringir el acceso por horarios, de acuerdo a la criticidad de la información que estos manejen y las necesidades puntuales de La Unidad.

g. El desarrollo de sistemas de información deberá considerar prácticas de desarrollo seguro que permita minimizar riesgos asociados a las vulnerabilidades más comunes en los aplicativos web, tales como: (a) inyección de código (SQL, LDAP, HTML, OS), (b) gestión de sesiones, (c) ataques de Cross-Site Scripting (XSS), (d) parámetros de configuración insegura, (e) exposición de datos sensibles, (f) problemas de acceso

restringido a funciones y (g) al uso de componentes con vulnerabilidades conocidas (versiones, parches y sistema operativo). Un ejemplo, el proyecto TOP10 de OWASP (Open Web Application Security Project), por medio del cual se busca identificar y remediar las 10 vulnerabilidades más comunes de las aplicaciones web.

5.3 Registro y auditoria.

a. Los componentes de la infraestructura tecnológica de la Unidad deberían generar y almacenar registros de las actividades, acciones, operaciones, y/o transacciones sobre la información, la plataforma y sobre su administración, con el fin de garantizar el principio de Auditabilidad, de forma tal que no se ejecute ninguna acción si no se puede consignar el registro que establezca el usuario responsable de la acción. Lo anterior, según concepto expreso por la Oficina de Seguridad de la Información, considerando los niveles de riesgos asociados al sistema de información, para lo cual, dichos registros deben cumplir con lo establecido en el documento*AP-PIT-007 Política Específica para la Gestión de Logs de Seguridad de la Información*

b. Los registros de auditoría deben ser de solo lectura (sin excepción) y expresados en lenguaje funcional comprensible.

5.4 Evaluación y atención de vulnerabilidades.

a. Antes de dar el paso a producción de un sistema de información, se deben realizar análisis de vulnerabilidades y pruebas de penetración sobre cada uno de los componentes tecnológicos del mismo tales como: (sistemas operativos, base de datos, aplicación). Las vulnerabilidades identificadas y reportadas como críticas deben ser remediadas antes del paso a producción.

b. Durante el tiempo en producción de los sistemas de información, la Dirección de Gestión de Tecnologías de la Información y la Oficina de Seguridad de la Información deberán realizar análisis de vulnerabilidades y pruebas de penetración de forma periódica sobre cada uno de los componentes tecnológicos de los mismos y así mismo, las vulnerabilidades identificadas y reportadas como críticas deberán ser remediadas para mantener los niveles adecuados de seguridad.

5.5 Manejo de Sesión

Los sistemas de información deben incluir los siguientes controles en el manejo de las sesiones:

a. Los intentos de inicio de sesión simultáneos deberán ser bloqueados, cuando estos se originen desde equipos diferentes, de lo cual se deberá guardar un registro de auditoría del evento, bajo la categoría de inicio de sesión. Se entiende entonces que únicamente se permite una (1) sesión activa por cada usuario.

b. Cuando el tiempo de inactividad de la sesión supere los cinco (5) minutos, esta se mantendrá activa, no obstante, se deberá exigir la repetición del proceso de autenticación (digitación de la contraseña). Asimismo, cuando el tiempo de inactividad de la sesión supere los quince (15) minutos, esta deberá ser finalizada automáticamente. Cabe anotar que esta característica debe ser parametrizable en los sistemas, por si llegasen a cambiar las necesidades de la entidad.

5.6 Planes de restauración.

Los sistemas de información que pasen al ambiente productivo deben contar con un manual de restauración y recuperación ante fallas, alineado con el Plan de Contingencia Tecnológica definido por la Dirección de Gestión de Tecnologías de la Información.

6 GLOSARIO

- **Autenticación:** Proceso de verificación de la identidad de un sujeto que solicita el uso de un sistema de información y/o acceso a recursos de red.
- **Autorización:** Otorgar acceso a un objeto después de que un sujeto ha sido identificado y autenticado.
- **Auditabilidad:** Principio de seguridad que indica la posibilidad de que un individuo sea identificable y responsabilizado por sus acciones**.**
- **Vulnerabilidad:** Ausencia o debilidad de un control, que puede ser explotada.
- **Análisis de Vulnerabilidades:** Es un método pasivo de evaluación de la seguridad de un sistema informático o red, en la que se identifican posibles vulnerabilidades, pero en el que no se emplean técnicas para explotarlas.
- **Prueba de Penetración:** Es un método de evaluación de la seguridad de un sistema informático o red, simulando las técnicas empleadas por un atacante, con el fin de identificar vulnerabilidades.
- **Responsable del Tratamiento:** Es el director o subdirector responsable según la Ley 1581 de 2012 de velar por que las limitaciones aprobadas por el comité del SIG se mantengan para cada activo de información, aprobar las operaciones que cada rol de cada sistema informático puede realizar sobre el activo entregado en custodia, y aprobar los usuarios que están autorizados para pertenecer a cada rol informático.
- **Encargado del Tratamiento**: El responsable según la ley 1581 de 2012 de realizar el tratamiento de la información. En la UGPP es el Director de Gestión de Tecnologías de la Información (DGTI).
- **Usuario de la Información**: Es responsable de usar los activos de información bajo los parámetros del Sistema de Gestión de Seguridad de la Información —SGSI.