HOJA DE APROBACIÓN

	Preparado Por:	Revisado Por:	Aprobado Por:
Nombre:	Juan Pablo Vanegas	Alberto Mario Solano Wilmack Sánchez 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 de Seguridad Informática Profesional Especializado Dirección de Seguimiento y Mejoramiento de Procesos	Directora de Seguimiento y Mejoramiento de Procesos Director de Gestión de Tecnologías de la Información
Fecha:	22 de Julio de 2016	27 de Julio de 2016	29 de Julio de 2016

HOJA DE CONTROL DE CAMBIOS

Versión	Acción	Fecha	Descripción de la Acción	Numeral	Responsable
1.0	Creación	29/07/2016	Creación del documento	Todos	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 Administración de firmas y certificados digitales 4

6 ESTÁNDARES 5

6.1 Algoritmos aceptados para las llaves de las firmas y certificados digitales 5
6.2 Canales cifrados VPN. 5
6.2.1 VPN-IPSec 5
6.2.2 VPN-SSL 5
6.3 Almacenamiento seguro de la información 6
6.3.1 Cifrado con criptografía asimétrica 6
6.3.2 Cifrado con criptografía simétrica 6
6.4 Seguridad en redes inalámbricas 6

7 ROLES Y RESPONSABILIDADES 6

7.1 Oficina de Seguridad de la Información 6
7.2 Dirección de Gestión de Tecnologías de la Información 6
7.3 Custodios de las firmas digitales 7

8 REFERENCIAS 7

9 GLOSARIO 7

1 OBJETIVO

Establecer los lineamientos y directrices de seguridad de la información que se deben cumplir para el almacenamiento y transferencia segura de los activos de información de La Unidad en formato digital.

2 PROCESO O SUBPROCESO AL CUAL PERTENECE

AP-SUB-007 Subproceso Gestionar Seguridad de la Información

3 ALCANCE

Esta política aplica a los activos de información en formato digital de La Unidad, de acuerdo a la POLITICA ESPECIFICA DE SEGURIDAD PARA EL TRATAMIENTO Y PROTECCIÓN DE INFORMACIÓN CLASIFICADA (AP-PIT-008), teniendo en cuenta su almacenamiento, acceso, distribución y movilidad.

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) La presente política se rige por la Ley 527 de 1999.

c) Toda la información de La Unidad clasificada como privada se debe proteger con técnicas de cifrado de acuerdo a la POLÍTICA ESPECÍFICA DE SEGURIDAD PARA EL TRATAMIENTO Y PROTECCIÓN DE INFORMACIÓN CLASIFICADA (AP-PIT-008).

d) Todas las comunicaciones desde redes públicas hacia infraestructura interna de La Unidad se deben realizar a través de canales cifrados.

e) Para aquellas aplicaciones cuyo análisis de riesgo indique se deba proteger la confidencialidad, integridad y autenticidad de la información que a través de ésta se almacene o distribuya, debe contar con la implementación de controles criptográficos de acuerdo a la presente política.

f) Solo el Oficial de Seguridad de la Información podrá aceptar excepciones a la presente política.

5 NORMAS ESPECÍFICAS

5.1 Administración de firmas y certificados digitales

a) Los certificados digitales se deben gestionar a través de una entidad certificadora de confianza. No se encuentra permitido el uso de certificados digitales que no permitan confirmar su autenticidad.

b) La custodia y uso de los certificados para las firmas digitales es personal e intransferible. Se encuentra prohibido el préstamo y uso por parte de personal no asignado para ello.

c) El custodio del certificado digital debe velar por la confidencialidad y disponibilidad de éste. Una vez se pierda la confidencialidad del certificado, el custodio deberá notificar a la Dirección de Gestión de Tecnologías de la Información para su revocación y expedición de una nueva.

d) Todo acto que altere la integridad, autenticidad y/o confidencialidad de los certificados y firmas digitales se tratará de acuerdo a la POLÍTICA ESPECÍFICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (AP-PIT-003) y a las disposiciones legales vigentes.

e) Toda aplicación que requiera el uso de firmas digitales debe registrar el evento de log cuando se firme digitalmente un documento. Este log debe registrar, como mínimo, quién firmó, cuando lo firmó y que se firmó.

f) El tiempo de vigencia para los certificados digitales no debe exceder dos (2) años.

6 ESTÁNDARES TÉCNICOS

6.1 Algoritmos aceptados para las llaves de las firmas y certificados digitales

Los protocolos y algoritmos aceptados para la generación de firmas y certificados digitales deben contar con al menos los siguientes parámetros de seguridad:

- Algoritmo de Firma: RSA >= 2048 bits, ECDSA >= 224 bits, DSA >=112 bits, algoritmos que ofrezcan igual o superior nivel de seguridad.
- Algoritmo hash de la firma: sha256 o superior.
- Algoritmo de cifrado de clave pública: RSA superior a 2048 bits; ECDSA o algoritmos que ofrezcan igual o superior nivel de seguridad.
- Algoritmo de identificación: sha1 o superior.

6.2 Canales cifrados VPN.

En La Unidad se encuentran permitidos los canales VPN de tipo IPsec y SSL.

6.2.1 VPN-IPSec

Los túneles VPN-IPsec deben contar al menos con la siguiente configuración:

- Los algoritmos aceptados son los siguientes
  - AES-CBC con longitud de llave de 128 o superior (Recomendado).
  - 3DES-CBC
- El algoritmo DES no se encuentra aceptados para el uso de cifrado en redes VPN.
- Para la protección de integridad se debe usar HMAC-SHA-1, no se acepta HMAC-MD5.
- Para IKEv1, el tiempo de las SAs de IKE no debe ser mayor a 24 horas. El tiempo de las SAs de IPsec debe no debe ser mayor a 8 horas.
- Para IKEv2, el tiempo re-key de las SA de IKE no debe ser mayor a 24 horas, en cuanto el tiempo de re-key de las SAs de IPsec no debe superar las 8 horas.
- El grupo de Diffie-Hellman usado para el establecimiento de las llaves de IKE y IPsec debe ser al menos del grupo 2 con 3DES o AES128 de DH. Para una mayor seguridad, se debe usar DH grupo 5 o DH grupo 14, dependiendo de la disponibilidad y capacidades de procesamiento de los equipos, integrado con cifrado AES.

6.2.2 VPN-SSL

Los túneles VPN-SSL deben contar al menos con la siguiente configuración:

- La versión de cifrado debe ser TLSv1.0 o superior. Debido al nivel de seguridad que brinda SSLv3.0 o inferior, este no se encuentra permitido.
- Los certificados digitales usados para el establecimiento del túnel deben implementar función hash SHA-256 junto con RSA o DSS para el algoritmo de firmas.
- La longitud de las llaves debe ser al menos de 2048 bits.

6.3 Almacenamiento seguro de la información

6.3.1 Cifrado con criptografía asimétrica

El par de llaves para el almacenamiento con cifrado asimétrico debe contar al menos con las siguientes características:

- Algoritmo de Firma: RSA >= 2048 bits, ECDSA >= 224 bits, DSA >=112 bits, algoritmos que ofrezcan igual o superior nivel de seguridad.
- Algoritmo hash de la firma: sha256 o superior.
- Algoritmo de cifrado de clave pública: RSA superior a 2048 bits; ECDSA o algoritmos que ofrezcan igual o superior nivel de seguridad.
- Algoritmo de identificación: sha1 o superior.

6.3.2 Cifrado con criptografía simétrica

Los algoritmos autorizados para el cifrado simétrico son los siguientes:

- Algoritmo de cifrado: AES con longitud de llave de 128 bits o superior
- Algoritmo hash: SHA-256 o superior.

6.4 Seguridad en redes inalámbricas

Solamente está permitido el uso de los siguientes protocolos criptográficos para el acceso a redes inalámbricas Wi-Fi:

- Tipo de autenticación y cifrado: WPA2-AES.
- Los mecanismos de autenticación a la red permitidos son:
  - PSK (Pre Shared Key): Autenticación a través de llave compartida. Esta debe ser asignada de acuerdo a la POLÍTICA ESPECÍFICA DE GESTIÓN DE ACCESO LÓGICO
  - EAP (Extensible Authentication Protocol): Permite la autenticación a través de diferentes mecanismos, como token, Smart card, certificado digital, entre otros. Se debe implementar a través de protocolo seguro.

7 RESPONSABILIDADES

7.1 Oficina de Seguridad de la Información

a) Actualizar esta política.

b) Ejecutar actividades de monitoreo para el cumplimiento de la política

7.2 Dirección de Gestión de Tecnologías de la Información

a) Coordinar la implementación de las directrices de la presente política en los diferentes componentes tecnológicos.

b) Hacer uso de la presente política como parte de sus herramientas de gobierno y de gestión, y definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento sobre los servicios brindados por parte de terceros.

c) Contar con los respectivos procedimientos para la generación, recuperación y revocación de los certificados digitales

d) Mantener un inventario de los servicios y/o personal que utiliza certificados digitales u otros mecanismos criptográficos

7.3 Custodios de las firmas digitales

a) Garantizar la confidencialidad y disponibilidad de las llaves privadas de las firmas digitales asignadas.

8 REFERENCIAS

- Ley 527 de 1999
- NIST SP 800-97 Establishing Wireless Robust Security Networks: A guide to IEEE 802.11i
- FIPS 140-2 Security Requeriments for Cryptographic modules
- NIST 800-111 Guide to Storage Encryption Technologies for End User Devices
- NIST 800-77 Guide to IPsec VPNs
- NIST SP 800-113 Guide to SSL VPNs
- FIPS PUB 186-4 Digital Signature Standard
- NIST SP 800-131Ar1 Recommendation for Transitioning the Use of cryptographic Algorithms and Key Lengths
- NIST 800-57pt4r4 Recommendation for Key Management Part 1: General
- NIST 800-32 Introduction to Public Key Technology and the Federal PKI Infrastructure

9 GLOSARIO

- **Autenticidad:** Propiedad que determina que la información es de quien indica ser
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **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.
- **Cifrado de disco:** Alterar los datos para que estos sean ilegibles para cualquier otro usuario que no posea la clave de acceso al equipo.
- **Custodio de las firmas digitales:** Persona asignada y autorizada para el uso de una firma digital.

- **Certificado digital:** Archivo digital generado por una entidad certificadora en la que se relacionan los datos de identidad de una persona o empresa. A través del certificado se puede autenticar la identidad, firmar electrónicamente o cifrar la información.

- **Disponibilidad de la información:** Propiedad que determina que la información sea accesible en el momento de ser requerida

- **Entidad certificadora:** Entidad autorizada para prestar servicios de certificación digital. La entidad certificadora debe ser reconocida en internet o al interior de una empresa (entidad certificadora local).

- **Entidad certificadora local**: Entidad certificadora ubicada al interior de una empresa para la expedición de certificados digitales internos.

- **Firma digital:** Mecanismo equivalente a la firma manuscrita que garantiza la identidad y responsabilidad del autor de un documento o transacción electrónica, así como permite comprobar la integridad del mismo.

- **Integridad de la información:** Propiedad que determina que solo el personal autorizado puede modificar la información

- **Llave privada y llave pública**: En la criptografía asimétrica, el par de llaves (pública y privada) se usan para cifrar información, de tal manera que si ésta se cifra por medio de una de las llaves, solamente la otra llave puede descifrarla.