CONTROL DE CAMBIOS					
VERSIÓN	FECHA	DESCRIPCIÓN	ELABORÓ	REVISÓ	APROBÓ
01	20-02-2020	Se crea documento y se incluyen los lineamientos para la Política de Controles Criptográficos	COORDINADOR SGI	COMITÉ DE POLITICAS Y SEGURIDAD	GERENTE GENERAL
02	07/03/2024	SE REVISA LA POLITICA SIN GENERAR CAMBIOS, SE ACTUALIZA FIRMA DEL GERENTE GENERAL	COORDINADOR SGI	COMITÉ DE POLITICAS Y SEGURIDAD	GERENTE GENERAL

1. OBJETIVO

El objetivo del presente documento es definir reglas para el uso de los controles y claves criptográficas para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de la información.

2. ALCANCE

Esta política aplica para la Entidad de Certificación Digital - ECD de PKI SERVICES y los servicios de certificación digital que conforman el alcance de acreditación otorgado por el Organismo Nacional de Acreditación – ONAC.

3. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos A.10.1.1, A.10.1.2, A.18.1.5
- Criterios Específicos de Acreditación – CEA para entidades de certificación digital
- Política de seguridad de la información
- Política de Clasificación de la Información
- Lista de requisitos legales, normativos, contractuales y de otra índole, capítulo A.18

4. RESPONSABILIDADES

El responsable de implementar, administrar y mantener la PKI y los controles criptográficos particulares, es el administrador de sistemas.

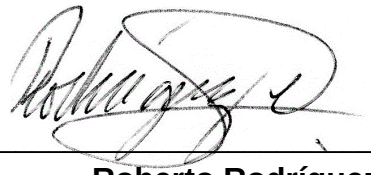
5. USO DE CRIPTOGRAFÍA

Controles criptográficos

PKI SERVICES ha implementado una Infraestructura de Llave Pública – PKI en cumplimiento de la ley y los estándares técnicos aceptados y vigentes.

Gestión de Claves criptográficas

- La PKI es implementada en dispositivos criptográficos HSM certificados fips 140-2 Level 3, mediante la ceremonia de generación de llaves, dejando
- La root de la CA debe permanecer offline una vez haya generado la subca que tendrá a cargo la función operativa.
- La creación de las lleves criptográficas de usuario final, se realiza siguiendo el ciclo de generación de llaves reglamentado
- La vigencia de las llaves debe cumplir lo reglamentado
- El almacenamiento de las llaves se puede realizar en dispositivos criptográficos llamados Token o en base de datos cumpliendo el proceso denominado generación de llaves centralizado.
- Las claves deben de estar protegidas mientras se distribuyen a todas las partes que las van a utilizar.
- La destrucción de claves se debe realiza en cumplimiento de lo que establece el reglamento o cuando la llave está comprometida.
- La llave pública está disponible para todo el mundo una vez emitido. La llave privada sólo debe estar disponible para el usuario final al que se expide el certificado digital correspondiente.
- La pérdida, robo o posible divulgación no autorizada de cualquier llave/clave de cifrado cubierto por esta política debe de ser reportado inmediatamente



Roberto Rodríguez
Gerente General
Bogotá D.C. 07-03-2024