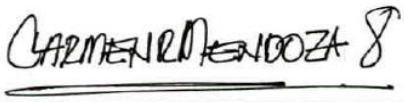
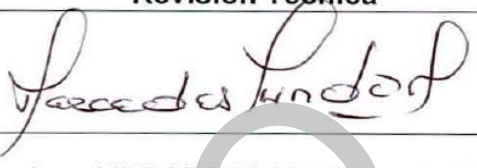
	Aprobación	Revisión Técnica
Firma:		
Nombre:	CARMEN ROSA MENDOZA SUÁREZ	**Nombre:** MERCEDES YUNDA MONROY
Cargo:	Director Técnico	**Cargo:** Director Técnico
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones	**Dependencia:** Dirección de Planeación
R.R. No. 047	**Fecha**	28 DIC. 2018

1. OBJETIVO

Proteger la información por medio de la gestión y aseguramiento de los servicios de red de la Contraloría de Bogotá D.C., así como el establecimiento de actividades para el uso de mecanismos criptográficos para garantizar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Inicia con la verificación y análisis de los registros (logs) de auditoria y eventos de los elementos de red (Routers, switches, firewall, controladores inalámbricos, otros) información y equipos informáticos, y finaliza con la actualización del inventario de los distintos mecanismos criptográficos.

3. BASE LEGAL

NORMA	FECHA	DESCRIPCIÓN
Ley 527	19-ago-1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 599	24-jul-2000	Por la cual se expide el Código Penal. Título III capítulo séptimo de la violación a la intimidad, reserva e interceptación de comunicaciones. Art 192, 193, 194,196 y 197.

Ley 1273	5-ene-2009	Por medio de la cual se modifica el Código Penal. Título VII Bis "De la protección de la información y de los datos". Artículos 269A a 269J.
Ley 1341	30-jul-2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Ley 1581	17-oct-2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712	06-mar-2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1377	27-jun-2013	Por la cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886	13-may-2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074	26-may-2015	Por medio del cual se expide el Decreto único Reglamentario del Sector Comercio, Industria y Turismo.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Capítulo 1, Título 9, Libro 2, Parte 2 subrogado por el Decreto 1008 de 2018.
Decreto 1081	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Presidencia de la República. Parte 1, Titulo 1.
Decreto 1008	14-jun-2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Política de Gobierno Digital.
Acuerdo 658	21-dic-2016	Por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Acuerdo 664	28-mar-2017	Por el cual se modifica parcialmente el Acuerdo 658 del 21 de diciembre de 2016, por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.

Resolución 305	20-oct-2008	Comisión Distrital de Sistemas. Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
Resolución 004	28-nov-2017	Por la cual se modifica la Resolución 305 de 2008 de la CDS.
CONPES 3701-2011	14 - jul - 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2016	11-abr-2016	Política nacional de seguridad digital.
NTC-ISO/IEC COLOMBIANA 27001:2013	11-dic-2013	Norma Técnica Colombiana NTC-ISO-IEC 27001.Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
Guía No 3	25-abr-2016	Procedimientos de Seguridad de la Información, MINTIC.

4. DEFINICIONES

Activo de información: Es una pieza de información definible e identificable, almacenada en cualquier medio.

Criptografía: Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

Enrutador: (Router) Dispositivo de comunicaciones encargado de enviar paquetes de datos de una red a otra de acuerdo con las reglas implementadas en la red de la entidad.

Hardening o endurecimiento: Es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuanto más funciones desempeña; el proceso de cerrar las vías para los ataques más típicos incluye el cambio de claves por defecto, desinstalar el software y dar de baja usuarios y accesos innecesarios; también deshabilitar servicios que no serán usados y fortalecer las configuraciones de aquellos que estarán en uso.

Hash: Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Información: Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.

Logs: Huellas o rastros de los sucesos que se han presentado en un equipo de cómputo o de comunicaciones de red con el fin de dar a proteger los equipos que conforman la red de la entidad.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Segmentación de red: proceso a través del cual se divide la red LAN en segmentos o grupos más pequeños con el fin de conseguir un mejor aprovechamiento del ancho de banda, evitar congestión de tráfico.

Transferencia de información: Proceso a través del cual se entrega información en formato digital al interior de la entidad o entidades externas de acuerdo con la solicitud presentada.

5. DESCRIPCION DEL PROCEDIMIENTO

5.1. Aseguramiento de Servicios en la Red

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
1	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la	Verifica y analiza los registros (logs) de auditoria y eventos de los elementos de red (Routers, switches, firewall, controladores inalámbricos, otros)		

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
	infraestructura de redes de TI.	En caso de encontrar alertas que comprometan la red o su seguridad, se inicia con las actividades del Procedimiento Gestión de Incidentes de Seguridad – PGTI-10.		
2	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Realiza actividades de administración y gestión de privilegios de usuarios con acceso al dispositivo de acuerdo a lo descrito en el procedimiento Control de Accesos a Usuarios – PGTI-07 y efectúa acciones de hardening o endurecimiento de dispositivos de ser requerido. Registra actividades en SICEINFO .	Sistema de Información de Control de Elementos Informáticos SICEINFO	
3	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Segmenta redes de acuerdo con las necesidades de distribución y seguridad de la información de la entidad, establece la segmentación de la red. Si existen, revisa y evalúa solicitudes de cambios en temas de organización, segmentación nuevos o	Diagramación y documentación de la segmentación de la red de la Contraloría de Bogotá.	

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		modificación de accesos y se inicia el procedimiento Gestión de Cambios y Capacidad Tecnológica – PGTI-08		
4	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Gestiona y/o configura las redes Inalámbricas autorizadas según la necesidad.		
5	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Configura y gestiona las conexiones de VPN autorizadas según la necesidad.	Registro de VPN	**Observación:** Revisa los parámetros técnicos para la conexión segura sección 5.3 controles criptográficos de este procedimiento en conjunto con el Oficial de Seguridad.
6	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Establece los protocolos de trasmisión y transferencia de información que se manejaran en las diferentes redes.		**Observación:** Teniendo en cuenta el nivel de confidencialidad de la información, a transmitir por las redes establecidas en la Contraloría de Bogotá, se iniciarán las

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
				actividades 5.3. Gestión de Controles criptográficos de este procedimiento
7	Profesional Especializado, Profesional Universitario responsable de administrar algún elemento de la infraestructura de redes de TI.	Supervisa y controla cuatrimestralmente los aspectos de configuración en los equipos y sistemas operativos de los elementos de la red que permitan asegurar la disponibilidad, integridad y confidencialidad de la información de acuerdo con las necesidades de la entidad.	Informe de administración y gestión de conexiones de red.	
8	Subdirector de Recursos Tecnológicos	Revisa informe de administración y gestión de conexiones de red.		

5.2. Transferencia de información digital

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
1	Servidores públicos de la Contraloría de Bogotá Propietario del activo de información	Reporta la solicitud de transferencia o transmisión de información, siguiendo las actividades del numeral 5.1. del procedimiento PGTI-04 - “Registro y atención	Registro en el Sistema de Mesa de Servicios	**Punto de Control:** Para solicitudes de transferencia de información con entidades externas debe ser solicitado por el jefe de la dependencia

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		de requerimientos de soporte a los sistemas de información y equipos informáticos".		propietario de la información. **Observaciones**: Tener en cuenta los acuerdos de confidencialidad establecidos por la Entidad Los servidores públicos de la Contraloría de Bogotá, que traten temas o información clasificada como información pública reservada o información pública clasificada (privada o semiprivada), lo deberán hacer en lugares seguros y/o por medios de comunicación establecidos por la Entidad.
2	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios la Dirección TIC – responsable del	Verifica la necesidad de transferencia de información, establecerá sí es transferencia de información al interior de la entidad o fuera de ella y escala el requerimiento.	Sistema de Mesa de Servicios por número de caso.	**Observación**: La transferencia de información al interior de la Entidad se realizará a través de los medios oficiales de comunicación establecidos por la entidad.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
	registro en el Sistema de Mesa de Servicios			
3	Profesional Especializado, Profesional Universitario – responsable de atención de la solicitud (Asignado)	Complementa la solicitud de transferencia de información teniendo en cuenta los siguientes aspectos en caso que se requiera: **Si es Transferencia a terceros:** • Establecer el acuerdo de transferencia de información con terceros, el cual deberá contener cláusulas donde se establezcan las herramientas a utilizar para asegurar la transferencia de información. • Incluir acuerdos de confidencialidad de la información, compromiso y reserva, el cumplimiento de la normatividad vigente nacional e internacional para el tratamiento de la información, en caso que se requiera.	Sistema de Mesa de Servicios por número de caso. Acuerdo de transferencia y confidencialidad de información con terceros.	**Punto de Control:** El Director y subdirectores de Tecnologías de la Información y las comunicaciones, revisan y aprueban la solicitud antes de ser realizada. **Observaciones**: La transferencia de información digital será liderada por la Dirección de Tecnologías de la Información y las comunicaciones así como el control del uso de sistemas de transferencia en coordinación con la dependencia y/o funcionario que manifieste la necesidad. La Dirección de TIC se reservará el derecho de suspender de manera unilateral los servicios que

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		• Método de enrutado y autenticación detallada para la transferencia de información. • Tiempo aproximado de utilización de la herramienta para el traspaso de la información. • Especificaciones técnicas especiales como llaves digitales o técnicas de encriptación de acuerdo con la entidad que se esté trabajando y la clasificación de la información Pasa a la actividad No.4 **Si la transferencia es interna:** • Valida que este autorizado por el jefe inmediato. • Evalúa la necesidad y establecer la herramienta apropiada para la atención de la solicitud. • Verifica la clasificación de la información a transferir de ser		hacen parte del objeto del acuerdo, así como la terminación unilateral del mismo, si llegaré a detectar algún incidente de seguridad que ponga en riesgo la Información de la Contraloría de Bogotá. La Entidad realizará transferencia de información con organizaciones gubernamentales y privadas, basada en la necesidad planteada por la Contraloría de Bogotá.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		necesario da inicio a las actividades descritas en la sección 5.3 – Gestión de Controles Criptográficos de este procedimiento. Pasa a la actividad No.5		
4	Profesional Especializado, Profesional Universitario de la Dirección TIC – responsable de atención de la solicitud (Asignada)	**Transferencia de información a terceros** Si la transferencia de información obedece a la ejecución de una función de la entidad, se procede a coordinar con la entidad interesada el método de transferencia y si se requiere un cambio en la infraestructura de red, se inicia el procedimiento Gestión de Cambios y Capacidad Tecnológica – PGTI-08.	Sistema de Mesa de Servicios por número de caso	**Punto de control**: Verifica si la transferencia de información hace parte del desarrollo de un contrato, para lo cual deberá verificar que se tenga total claridad del acuerdo de confidencialidad de la información que firmo.
5	Profesional Especializado, Profesional Universitario de la Dirección TIC – responsable de atención de la solicitud (Asignada)	**Transferencia de información interna** Realiza las actividades de transferencia de información interna; para lo cual sí se requiere un cambio en la infraestructura de red, se inicia el procedimiento Gestión	Registro en el Sistema de Mesa de Servicios	**Observación:** La Dirección de Tecnologías de la Información y las comunicaciones, implementará las herramientas, y controles para asegurar la transferencia de información al

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		de Cambios y Capacidad Tecnológica – PGTI-08. De lo contrario realiza las actividades del procedimiento Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos – PGTI-04, que apliquen de acuerdo a la naturaleza de la solicitud.		interior de la Entidad.
6	Profesional Especializado, Profesional Universitario de la Dirección TIC – responsable de atención de la solicitud (Asignada)	Valida el método de transferencia. En caso de ser por el protocolo de transferencia de archivos FTP o almacenamiento en la nube o correo electrónico, se inicia las actividades descritas en la sección 5.3 – Gestión de Controles Criptográficos de este procedimiento en caso que aplique. En caso de ser por medio extraíble (USB, DISCO EXTERNO u OTRO) realiza las actividades del procedimiento Registro y atención de	Registro en el Sistema de Mesa de Servicios	**Punto de Control:** Informa a Director y Subdirectores de Tecnologías de la Información y las comunicaciones que los servicios abiertos para atender la solicitud fueron cerrados.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		requerimientos de soporte a los sistemas de información y equipos informáticos – PGTI-04, que apliquen de acuerdo a la naturaleza de la solicitud. Finaliza la atención como se indica en el procedimiento Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos – PGTI-04 y cierra o desactiva los servicios autorizados temporalmente para la atención del requerimiento.		

5.3. Procedimiento de Criptografía

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
1	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, Asesor, Gerente, Profesional, Técnico, Secretario o Auxiliar.	Revisa la clasificación del activo en el registro de activos de información contenido en los Instrumentos de Gestión de Información Pública, sí el activo de información no se encuentra registrado se activa Procedimiento		**Observación:** Resultado de la clasificación de los activos de información, surge la necesidad de aplicación de controles criptográficos para

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
		PGD-08 – "Actualización de los Instrumentos de Gestión de Información Pública". Numeral 5.1 Actualización, aprobación y divulgación de Instrumentos: Registro de Activos de Información, Índice de Información Clasificada y Reservada o Esquema de Publicación de Información. Identifica si el activo de información se encuentra calificado como público clasificado o publico reservado.		la gestión de la información.
2	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, asesor, gerente, profesional, técnico, secretaria, auxiliar, (Funcionario perteneciente a la dependencia propietario del activo de información).	Registra el requerimiento de aplicación de controles criptográficos al activo a través de la mesa de servicio, se activa procedimiento PGTI-04 - "Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos".	Registro en el Sistema de Mesa de Servicios	**Observación**: Informa el nombre del funcionario y tiempo de utilización del control criptográfico.

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
3	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información.	Revisa los riesgos de seguridad digital del activo de información establecidos en el mapa de riegos, en caso no existir registro éste y según evaluación solicita a dueño de proceso su incorporación en el mapa de riesgos de seguridad digital.		**Punto de Control:** Valida la clasificación según el nivel de confidencialidad y privilegios de acceso a la información y define si continua con la ejecución del procedimiento o si la información no requiere controles criptográficos termina el procedimiento y se registra en el Sistema de Mesa de Servicios.
4	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información.	Determina los mecanismos criptográficos a implementar, basado en lo descrito en el Anexo 1 “Mecanismos Criptográficos”.		Observación: Se utilizarán controles criptográficos en los siguientes casos: 1. En la protección de claves de acceso a sistemas, datos y/o servicios. 2. Para la transmisión de información Reservada o Clasificada, fuera de la Entidad. 3. En la protección de la información a

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
				custodiar, cuando así lo establezca el dueño de la información o Oficial de Seguridad de la Información.
5	Contralor Auxiliar, Director, Subdirector, Jefe de Oficina, asesor, gerente, profesional, técnico, secretaria, auxiliar, (Funcionario perteneciente a la dependencia propietario del activo de información).	Asigna la clave para el cifrado de la información, debe ser establecida por el usuario que administra dicha información utilizando para ello protocolos para generar llaves seguras y teniendo siempre presente que en caso de olvidar la clave, la información cifrada no es recuperable.		**Observación**: Para la generación de llaves y/o claves seguras, tener presente lo descrito en el Anexo 5. "Instructivo para la gestión de contraseñas seguras", del PGTI-07 – Procedimiento De control de acceso a usuarios
6	Asesor, Profesional Especializado con funciones de Oficial de Seguridad de la Información.	Realiza el aprovisionamiento o alistamiento de hardware, software, y demás recursos necesarios para poner en marcha los controles criptográficos que serán utilizados.		**Observación**: Teniendo presente los controles que se implementaran se da inicio al procedimiento PGTI-08 "Procedimiento para la Gestión de cambios y capacidad tecnológica"

N°	RESPONSABLE	ACTIVIDAD	REGISTRO	PUNTOS DE CONTROL/ OBSERVACIONES
7	Asesor, Profesional Especializado con funciones de Oficial de Seguridad de la Información.	Actualiza el inventario de los mecanismos criptográficos controlando, fechas de expiración, asignaciones realizadas, activo custodiado y así poder renovar oportunamente y/o revocar los controles que ya no son requeridos.	Inventario de mecanismos criptográficos	**Observación:** Para gestionar el ciclo de vida de las llaves criptográficas debe tener presente lo descrito en el Anexo 2. "Lineamiento Gestión de llaves criptográfica".

6. ANEXOS

Anexo 1. Mecanismos Criptográficos

Dentro de los mecanismos criptográficos que la Contraloría de Bogotá puede implementar se encuentran:

- **Certificado Digital:** o certificado electrónico es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital.
- **Certificados SSL**: Sirve para brindar seguridad al visitante de un sitio web, es una manera de indicarle a los usuarios que el sitio es auténtico, real y confiable para ingresar datos personales. Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que los datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada.
- **Certifirma:** Aplicativo desarrollado por Certicámara S.A., en donde el usuario interactúa para realizar los procesos de firma de documentos en diferentes formatos ej. (Doc, jpeg, PDF). este aplicativo tiene un tipo de licencia freeware.
- **Cifrado de archivos y carpetas**: Es un procedimiento que vuelve completamente ilegibles los datos de un documento o de cualquier archivo. De esta manera, el archivo se vuelve prácticamente inservible para un usuario no autorizado a leerlo,

ya que incluso si lo ha interceptado o lo ha copiado, si no cuenta con la clave correspondiente, no podrá leerlo o visualizarlo.

- **Clave:** conjunto finito de caracteres alfanuméricos necesarios para el uso del certificado digital, el cual debe ser conocido únicamente por el titular del certificado.
- **Correo Electrónico Certificado**: Permite a los suscriptores tener las notificaciones electrónicas de los correos electrónicos demostrando que reproduce con exactitud la información generada, enviada o recibida, a su vez es posible determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje aportando validez jurídica y probatoria.
- **Dispositivos Criptográficos**: Hace referencia a mecanismos por ejemplo para doble autenticación como es el uso del Token.
- **Estampado Cronológico**: Estampar cronológicamente, consiste en certificar que un conjunto de datos o documentos ha existido e incorpora la fecha y la hora en que ocurre dicho evento, específicamente cuando fue creado, modificado, recibido, etc., en un sistema de cómputo.
- **Firma Digital**: Es un método criptográfico que asocia una identidad ya sea de una persona en particular o de un equipo a un mensaje enviado a través de transmisión por la red. Su uso puede ser diferente dependiendo de lo que se requiera hacer con la firma como por ejemplo, expresar conformidad con algún documento de tipo legal como podría ser la firma de un contrato laboral e incluso asegurar que no podrá modificarse el contenido del mensaje. La firma digital es el resultado de aplicar a un documento, en línea, un procedimiento matemático que requiere datos que exclusivamente conoce la persona que firma, encontrándose ésta bajo su absoluto control.
- **Generación de Firmas Digitales**: Es un servicio que integra la firma digital a una plataforma de acceso seguro en la cual se puede firmar y enviar documentos a usuarios internos o externos de la entidad a través de circuitos de firma y flujos de trabajo.
- **Token de seguridad** (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Anexo 2. Lineamientos Gestión de Llaves Criptográfica

Dentro de la gestión de los controles criptográficos, se debe administrar el ciclo de vida de los mecanismos utilizados donde se deben contemplar mínimamente las siguientes fases:

- **Generación de contraseñas:** Aplicar buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y un medio para establecer

derechos de acceso. Anexo 5. “Instructivo para la gestión de contraseñas seguras”, del PGTI-07 –Procedimiento De control de acceso a usuarios.

- **Distribución**: Disponer adecuadamente de mecanismo criptográfico: Comprende la forma como llega y se autentica el mecanismo criptográfico en el banco o base de datos que autoriza el acceso a la plataforma.
- **Políticas de Uso:** Aplicar políticas para generar, emplear, recuperar, reemplazar y disponer de las claves y contraseñas. Determinar los límites de uso, y esto incluye tipo de caracteres; longitud de la contraseña; políticas de almacenamiento en la base de datos; políticas de recuperación de clave o contraseña olvidada; y caducidad u obsolescencia (“vencimiento”) de las claves.
- **Almacenamiento en Base de datos: D**ebe almacenar o alojar la información de las claves o contraseñas en una Base de Datos; y restringir el acceso a ella, la cual se basa en los siguientes controles de seguridad:
  - Encripción de los archivos que contienen las claves y contraseñas.
  - Activación del control de acceso al sistema operativo de la Base de Datos.
  - Almacenamiento de hashes criptográficos para claves y contraseñas.
  - Verificación del dispositivo (capacidades de seguridad, amenazas y/o requerimientos de autenticación).
- **Obsolescencia:** En esta etapa final del ciclo de vida de claves y contraseñas, se debe dar disposición final adecuada a las claves o contraseñas cuando caen en desuso, no deben usarse por tiempo indefinido. Existen dos tipos de disposición de las claves y contraseñas una vez se hacen obsoletas:
  - Disposición por Expiración: Establecer el tiempo máximo de vida útil de claves y contraseñas. Esto da una ventana de tiempo predeterminada para que las mismas caigan en desuso, y sea necesario crear una nueva clave o contraseña para el acceso seguro.
  - Disposición por Revocación: Ocurre cuando se detecta compromiso en las claves y contraseñas, y para asegurar la integridad de las mismas, procede a su descontinuación inmediata. También se revoca una clave o contraseña por fuerza mayor (despido, deceso o redefinición de privilegios de usuario; actualizaciones; restructuraciones, entre otros).

    Cuando las claves y contraseñas se hacen obsoletas, se deberá determinar los parámetros de su destrucción y disposición final. Generalmente, los controles más comunes para adelantar esta destrucción son los siguientes:
    - Borrado seguro.
    - Destrucción física por desmagnetización o trituración de medios magnéticos.

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0		Versión Inicial