1. **NOMBRE DEL PROCEDIMIENTO:** Gestión De Llaves Criptográficas
2. **PROCESO AL QUE PERTENECE:** Gestión Tecnológica
3. **UBICACIÓN Y COBERTURA DEL PROCEDIMIENTO:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NIVEL** |  |  | **COBERTURA** |  |
| Estratégico |  |  | Central |  |
| Misional |  |  | Nacional | **X** |
| Apoyo | **X** |  | Seccional |  |

1. **OBJETIVO DEL PROCEDIMIENTO**

Establecer actividades en cuanto a gestión de llaves criptográficas durante su ciclo de vida, para la protección de la información sensible de la Rama Judicial.

1. **MARCO NORMATIVO**

* Ley 270 de 1996 – Ley Estatutaria de la Administración de Justicia.
* Ley 872 de 2003 – Creó el Sistema de Gestión de la Calidad en la Rama Ejecutiva y en otras entidades prestadoras de servicios.
* NTC ISO 9001:2015 – Norma Técnica de Calidad.
* NTC ISO 14001:2015 – Norma Técnica de Sistema de Gestión Ambiental.
* NTC OHSAS 18001:2007 – Norma Técnica de Seguridad y Salud en el Trabajo.
* ACUERDO No. PSAA14-10161 (junio 12 de 2014) - “Por el cual se actualiza el Sistema Integrado de Gestión y Control de la Calidad creado mediante Acuerdo PSAA07-3926 de 2007 y se establece el Sistema Integrado de Gestión y Control de la Calidad y el Medio Ambiente – SIGCMA”.
* ACUERDO No. PSAA14-10279 (Diciembre 22 de 2014) - “Por el cual se aprueban las políticas y procedimientos de Seguridad de la Información para la Rama Judicial”.

1. **ALCANCE DEL PROCEDIMIENTO**

Este procedimiento aplica para todas las llaves criptográficas de la Rama Judicial.

1. **LÍDER DEL PROCEDIMIENTO**

|  |  |
| --- | --- |
| **CARGO** | **DEPENDENCIA** |
| Director de Unidad | Unidad de Informática  Grupo de Proyectos Especiales |

1. **RESPONSABLES DEL PROCEDIMIENTO**

|  |  |
| --- | --- |
| **CARGO** | **DEPENDENCIA** |
| Profesional designado | Unidad Informática  Grupo de Proyectos Especiales de Tecnología |

1. **PROVEEDORES E INSUMOS**

|  |  |
| --- | --- |
| **PROVEEDORES** | **ENTRADA/INSUMOS EXTERNOS** |
| Colombia Compra Eficiente | Acuerdos Marco de Precio. |
| Usuarios y Servidores Judiciales | Solicitudes de llaves criptográficas. |

1. **CONTROLES DEL PROCEDIMIENTO**

|  |  |
| --- | --- |
| **NOMBRE DEL CONTROL** | **DESCRIPCIÓN DEL CONTROL** |
| Documento de diseño de las llaves | Documento donde se selecciona el algoritmo, tipo de llave, tamaño de la llave, funcionalidad, criptoperiodo, garantías antes de su uso y emisión. |
| Documento gestión de incidentes | Documento con acciones en caso de que se comprometan las llaves. |
| Inventario de llaves | Listado de llaves criptográficas que incluye tipo de llave, tamaño de la llave, funcionalidad, criptoperiodo y responsable. |
| Acta de destrucción de las llaves | Soporte de la destrucción autorizada de una llave criptográfica. |
| Recuperación de las llaves | Mecanismos de respaldo o como se realiza la recuperación de las llaves en caso de perdida. |
| Acta de responsabilidad de llaves criptográficas. | Documento donde se detalla el responsable de una llave criptográfica. |
| Documento de lecciones aprendidas. | Detalle de los eventos ocurridos durante la gestión de las llaves criptográficas y las actividades realizadas para dar solución. |

1. **DESCRIPCIÓN DEL PROCEDIMIENTO (Ciclo PHVA)**

| **Etapa** | **Actividad** | **Descripción** | **Producto** | **Responsable** |
| --- | --- | --- | --- | --- |
| P | Planear la adquisición/generación de llaves criptográficas | Realizar plan de adquisiciones, renovaciones y/o generación de llaves criptográficas con base en los requerimientos y en el inventario de llaves existentes. | Plan de llaves criptográficas | Profesional designado |
| H | Solicitud de llaves | Realizar la solicitud de llaves que cumplan los requisitos de acuerdo a su uso. | Evidencia solicitud de llaves | \* Usuario Interesado |
| H | Realizar la planeación de la Generación de llaves | \* Selección de Algoritmo de acuerdo a la necesidad y servicio donde se va a usar.  \* Seleccionar el Tipo de llave y su funcionalidad  \* Establecer el Criptoperiodo.  \* Especificar las llaves o parámetros y las garantías antes de su uso y emisión  \* Definir la longitud del Tamaño de la llave.  \* Definir acciones en caso de que se comprometan las llaves. | Configuración para la generación de las llaves | \* Director de Unidad  \* Coordinador de Ciberseguridad  \* Proveedor |
| H | Generación de llaves | Realizar la generación de las llaves en concordancia a las siguientes especificaciones:  \* Llaves criptográficas sólidas (AES-256) con una longitud de 256 bits como mínimo  \* Las llaves de cifrado utilizada en entornos de pruebas y desarrollo no debe ser instaladas en producción. | Llaves criptográficas | \* Director de Unidad  \* Coordinador de Ciberseguridad  \* Proveedor |
| H | Distribución de llaves | Definir los métodos de distribución de las llaves (Automático o Manual) o como se distribuye. | Documento técnico | \* Coordinador de Ciberseguridad  \* Usuario Interesado  \* Proveedor |
| H | Almacenamiento de llaves | Definir los medios de almacenamiento de las llaves generadas y controlar su acceso, modificación para garantizar su integridad y confidencialidad. | Documento técnico | \* Coordinador de ciberseguridad  \* Usuario interesado  \* Proveedor |
| H | Destrucción de llaves | Establecer cómo se va a realizar la destrucción una vez se genera una nueva. | Documento técnico | \* Coordinador de ciberseguridad  \* Usuario interesado  \* Proveedor |
| H | Recuperación de llaves | Establecer mecanismos de respaldo o como se realiza la recuperación de las llaves en caso de perdida | Documento técnico | \* Coordinador de ciberseguridad  \* Usuario interesado  \* Proveedor |
| H | Entregar Llaves | Realizar la entrega de las llaves de acuerdo a la solicitud entregando el Acta de responsabilidad de Llaves Criptográficas. | Acta de responsabilidad de llaves criptográficas | \* Coordinador de ciberseguridad  \* Usuario interesado  \* Proveedor |
| H | Validación de funcionamiento | Realizar la validación del funcionamiento. | Documento técnico | \* Coordinador de ciberseguridad  \* Usuario interesado  \* Proveedor |
| H | Identificar lecciones aprendidas | Generar lecciones aprendidas. | Documento técnico | \* Coordinador de ciberseguridad  \* Usuario interesado  \* Proveedor |
| H | Ejecutar acciones mejora | Analizar y planear siguientes pasos | Evidencia de seguimiento | \* Coordinador de ciberseguridad  \* Usuario interesado  \* Proveedor |
| V | Verificar la implementación correcta del procedimiento | Revisar que todas las actividades para la implementación en la gestión de usuarios se hayan ejecutado y cumplido. | Evidencia de la revisión | Director(a) de la Unidad Informática  Profesional Unidad de Informática |
| A | Ejecutar acciones de mejora | Aplicar las acciones necesarias para corregir desviaciones en la gestión de usuarios | Documento que evidencia las acciones de mejora implementadas y lecciones aprendidas | Profesional Unidad de Informática |

1. **ANEXOS (Formatos, Guías, Instructivos, Planes)**

* Documento de diseño de las llaves
* Documento gestión de incidentes
* Inventario de llaves
* Acta de destrucción de las llaves
* Recuperación de las llaves
* Acta de responsabilidad de llaves criptográficas.
* Documento de lecciones aprendidas.

1. **CONTROL DE REGISTROS**

Ver tabla de retención documental validada por el Comité Nacional del SIGCMA.

1. **TÉRMINOS Y DEFINICIONES**

Los términos y definiciones se pueden observar en el documento *“Glosario del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y protección de Datos Personales”.*