|  |  |  |
| --- | --- | --- |
| logo | ***Rama Judicial del Poder Público*****PROCEDIMIENTO DE GESTION DE VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLIGICA** |  |
|  |

|  |
| --- |
| 1. **OBJETIVO**
 |
| Establecer el método para identificar, analizar, priorizar y remediar las vulnerabilidades tecnológicas presentes en las diferentes áreas y componentes tecnológicos que soportan los procesos del negocio de la Rama Judicial, minimizando los riesgos a los que está expuesta la información. Así mismo, cumplir con los requerimientos regulatorios aplicables a la organización. |
| 1. **ALCANCE**
 |
| El alcance de este procedimiento aplica para todos los componentes de infraestructura tecnológica de la Rama Judicial. Asimismo, este procedimiento debe ser aplicado por todos los funcionarios y terceros que tengan acceso a la administración de los activos tecnológicos de la organización.  |
| 1. **RESPONSABLE**
 |
| El responsable de proceso, área o sistema de información debe garantizar la adecuada implementación del presente procedimiento de gestión de cambios |
| 1. **DEFINICIONES**
 |
| * **Sistema de información**

Cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales así como el software, firmware o hardware que forme parte del sistema. * **Software**

Programa de computador* **Solución de errores conocidos.**

Serie de pasos previamente establecidos que permiten resolver un problema en un equipo tecnológico o un Software* **Activo**

Componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa. La entidad asigna un valor a cada activo que representa el nivel de importancia que tiene el activo en el proceso del negocio.* **Vulnerabilidad**

Debilidad o defecto en las Tecnologías de Información que hace que la seguridad (en términos de Confidencialidad, Integridad y Disponibilidad) de un activo sea susceptible de ser comprometida.* **Vulnerabilidades Potenciales**

Vulnerabilidades potenciales incluyen todas las vulnerabilidades que no podemos confirmar existir. La única manera de verificar la existencia de estas vulnerabilidades sería llevar a cabo una exploración intrusiva en su red, lo que podría resultar en una denegación de servicio. Esto está totalmente en contra de nuestra política.* **Amenaza**

Un agente representa una amenaza para un sistema cuando dicho sistema tiene una vulnerabilidad que un atacante puede explotar para obtener un beneficio.* **Riesgo**

Probable ocurrencia de que un atacante explote un fallo de seguridad en un activo determinado, en base a las amenazas existentes y al impacto potencial que representaría para el negocio de la compañía.* **Confidencialidad**

Garantía de que únicamente accederán a la información los elementos autorizados para ello, y que dichos elementos no van a convertir esa información en disponible para otras entidades.* **Integridad**

Garantía de que la información únicamente puede ser modificada por elementos autorizados asegurando métodos de proceso exactos y completos.* **Disponibilidad**

Garantía de que la información y los activos relacionados deben estar accesibles a elementos autorizados en tiempo, modo y lugar adecuado. |
| 1. **NORMATIVIDAD**
 |
| Norma Técnica Colombiana NTC ISO/IEC 27001:2013 Anexo A12.1.2 Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afecten la seguridad de la información.Manual Políticas seguridad de la información Rama Judicial.Se debe dar cumplimiento a la “POLÍTICA GESTIÓN DE VULNERABILIDADES EN LOS COMPONENTE DE INFRAESTRUCTURA TECNOLÓGICA”Norma técnica Colombiana NTC ISO/IEC 20000-2 primera edición del 15 de diciembre de 2005 Sistemas de Gestión de Información y Tecnología, sección 9 gestión de cambios |

| 1. **ACTIVIDADES**
 |
| --- |
| **PASO** | **ACTIVIDAD** | **DESCRIPCIÓN DE LA ACTIVIDAD** | **RESPONSABLE** |
| ELABORACIÓN Y MANTENIMIENTO DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN |
|  | Planeación | El objetivo de la etapa de planeación es identificar todos los requerimientos de análisis y definir el alcance teniendo en cuenta aspectos como: * Las ubicaciones desde donde se ejecutaran las pruebas.
* Cantidad de seccionales, numero de dispositivos por cada seccional o tecnologías empleadas.
* Tipo de pruebas que se ejecutaran (Escaneos con credenciales, pruebas de penetración caja negra, caja gris o caja blanca).
* Las solicitudes explicitas de escaneo de vulnerabilidades (solicitud del área responsable, cumplimientos regulatorios, solicitudes de auditoría, apoyo a proyectos previo a su puesta en producción, etc.)
* Resultados de análisis de vulnerabilidades o pruebas de penetración realizados con anterioridad.

Los responsables del área de seguridad de la información deben validar con cada uno de los administradores de los sistemas el alcance de las pruebas, con el fin de determinar los tiempos de ejecución, horarios o cualquier tema relacionado a la disponibilidad o criticidad de los dispositivos seleccionados.Se debe elaborar un plan de trabajo y un cronograma los cuales están sujetos a aprobación por parte de las partes involucradas, así mismo se debe notificar y difundir el cronograma a las partes interesadas.  | Área de seguridad / Oficial de seguridad de la información |
|  | Ejecución | Previo al inicio de las actividades de escaneo de vulnerabilidades y/o penetración se notificará al responsable/administrador de los activos tecnológicos involucrados vía correo electrónico, para el respectivo monitoreo.Posterior a la notificación del inicio de las actividades se debe definir el perfil de análisis sobre las herramientas involucradas por parte del Área de seguridad o el tercero involucrado, dando inicio al descubrimiento de los componentes tecnológicos.Si durante la etapa de planeación se definido realizar pruebas de penetración se deben aclarar si se van a realizar ataques de denegación de servicio y el horario provisto para esto. | Área de seguridad / Oficial de seguridad de la información / Tercero |
|  | Análisis y reportes | Basado en los resultados de las diferentes herramientas utilizadas sobre las pruebas y/o la extracción de información obtenida de las mismas, se deben desarrollar informes tanto técnicos como ejecutivos teniendo en cuenta aspectos definidos en el plan de trabajo y aspectos como los descritos a continuación: * Se debe analizar cada uno de los resultados teniendo en cuenta los activos de información y el nivel de criticidad establecidos por el Consejo Superior de la Judicatura.
* Se debe realizar análisis y validación de resultados con el objetivo de identificar falsos positivos este ítem aplica exclusivamente sobre el análisis de vulnerabilidades debido a que las pruebas de penetración garantizan la confirmación de la vulnerabilidad.
* Realizar comparaciones con los análisis anteriormente realizados.
* Se deben organizar las vulnerabilidades de acuerdo a su nivel de criticidad conforme a la escala mostrada a continuación y el impacto para el negocio de lo cual se obtiene la priorización de las vulnerabilidades más críticas.
	+ **Urgente (5):** Intrusos pueden fácilmente obtener el control de un dispositivo lo cual puede conducir al compromiso de toda la red de seguridad.
* **Critico (4):** Los intrusos pueden posiblemente obtener el control del dispositivo o estos posiblemente pueden tener fugas de información altamente sensible.
* **Serio (3):** Los intrusos pueden tener acceso a información específica almacena sobre el dispositivo, incluyendo configuraciones de seguridad. Esto puede resultar en el aprovechamiento de esta falencia por parte de un atacante.
* **Medio (2):** Los intrusos pueden ser capaces de recolectar información sensible desde un dispositivo como por ejemplo la versión especifica de un software instalado posibilitando la explotación de vulnerabilidades conocidas de este software.
* **Mínimo (1):** Los intrusos pueden reunir información acerca de puertos abiertos y servicios y puede ser capaz con esta información de buscar otras vulnerabilidades.
* Realizar recomendaciones y elaboración de informes para cada una de los grupos o seccionales identificadas en el plan de trabajo.
* Realizar presentaciones y entrega de informes con las partes interesadas.
 | Área de seguridad / Oficial de seguridad de la información / Tercero |
|  | Remediación | Cada uno de los administradores de las diferentes plataformas o administradores de las seccionales deben entender el informe técnico en el cual se describen los problemas de seguridad concernientes a la plataforma, y de esa menara elaborar un plan de remediación de dichos problemas de seguridad en el cual se tengan contempladas estrategias como:* Instalación masiva de parches de seguridad que estén presentes en el informe y que afecten en gran porcentaje a los activos.
* Clasificación y agrupar de los problemas de seguridad a nivel de sistemas operativos, software específico, aplicaciones web, bases de datos etc.
* Top de dispositivos con la mayor cantidad de vulnerabilidades.
* Top de vulnerabilidades más comunes.

Posterior a la selección de la estrategia de remediación se procederá a ejecutar la solución de seguridad, sin embargo para sistemas que sean críticos para la organización se deben implementar ambientes de prueba.Estos ambientes de prueba serán instalados en sistemas virtualizados y en ambientes semejantes al de producción de tal forma que las versiones de software instaladas en el ambiente de producción serán las mismas que en el ambiente de pruebas.En caso de existir incompatibilidad con la implementación de la solución de seguridad se debe informar al área de seguridad de dicha incompatibilidad, el área de riesgos y seguridad deberán tomar la decisión sobre los controles alternativos y deben llegar a un acuerdo sobre el riesgo expuesto, así mismo para futuros análisis, estos casos puntuales deberán ser tenidos en cuenta para las respectivas excepciones sobre las herramientas utilizadas. | Área de seguridad / Administrador del sistema / Tercero |
|  | Re-test | Finalizado el plan de remediación y la implementación de los respectivos cambios sobre las plataformas evaluadas, se ejecutaran las pruebas de validación o Re-test con el objetivo de identificar la correcta implementación de la solución de seguridad o la aparición de nuevas vulnerabilidades.Sobre la validación se deben tener en cuenta las excepciones de las vulnerabilidades acordadas con el área de seguridad de la información.  | Área de seguridad / Oficial de seguridad de la información / Tercero |
|  | Fin del procedimiento. |

| 1. **REGISTROS**
 |
| --- |
| **CÓDIGO** | **NOMBRE** | **RESPONSABLE DE DILIGENCIARLO** | **LUGAR DE ARCHIVO** | **CRITERIO DE ARCHIVO** | **TIEMPO DE RETENCIÓN** | **DISPOSICIÓN** |
|  | Registro de control de cambiosCSJ\_RG\_Solicitud\_Cambio | Funcionario Responsable proceso, área o sistema de información la Rama Judicial | Ver tabla de retención documental | Ver tabla de retención documental | Ver tabla de retención documental | Ver tabla de retención documental |

|  |
| --- |
| 1. **DOCUMENTOS ASOCIADOS**
 |
| [Manual de Políticas de Seguridad](../../Manual%20de%20Politicas/CSJ_Manual%20de%20politicas_v1.2.DOCX) |
| 1. **ANEXOS**
 |
| **Terceros:** En determinados casos es posible que la ejecución del procedimiento, este encargado a un tercero calificado para este fin. En el momento en que esto se presente, el tercero debe garantizar el cumplimiento del presente proceso, así como de las políticas internas de la organización que apliquen según el caso.**Anexo:** Caracterización del Procedimiento Gestión de vulnerabilidades.xlsx  |
| 1. **CONTROL DE CAMBIOS**
 |
| N.A. |