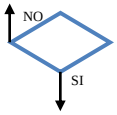
| PROCEDIMIENTO: GESTIÓN DE ANÁLISIS DE VULNERABILIDADES EN LA SNR | | |
|---|---|---|
| **OBJETIVO:** | | Establecer lineamientos para la gestión de vulnerabilidades de seguridad técnica de los sistemas de información y equipos informáticos, a través de herramientas de pentesting, con el fin de mantener un nivel de aseguramiento adecuado en las plataformas tecnológicas y sistemas de información de la SNR para mitigar los riesgos asociados. |
| **ALCANCE:** | **Limite Inicial:** | Definir alcance de la prueba. |
| | **Limite Final:** | Comunicar a los responsables de la oficina OTI el estado de los riesgos. |
| **PRODUCTOS:** | | Reporte de herramienta Nessus, Cuadro de mando, Informe ejecutivo de vulnerabilidades, plan de acción, Bitácoras de información (históricos). |
| **RESPONSABLE:** | | Profesional Especializado - Oficial de Seguridad de la Información y Equipo de respuesta de tecnología de la OTI. |

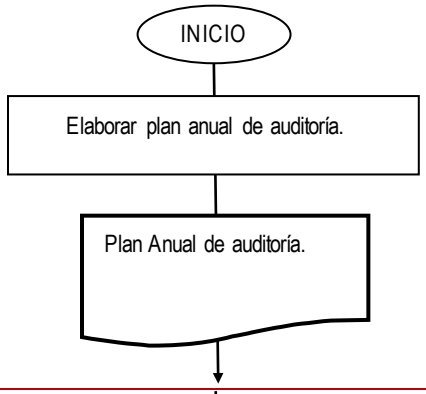
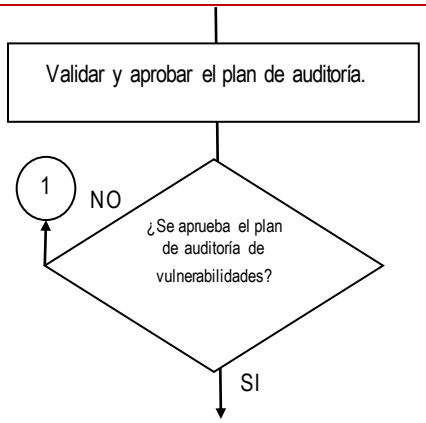
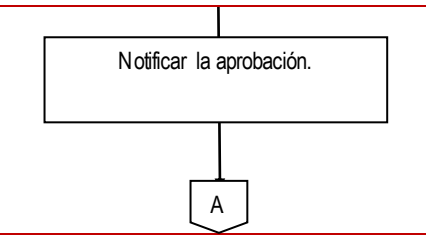
**CUADRO DE CONVENCIÓN FLUJOGRAMA:**

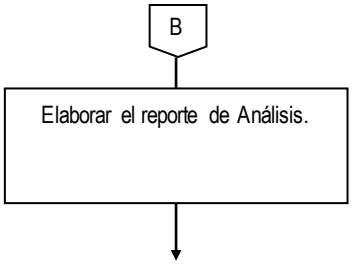
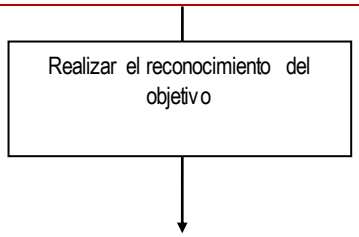
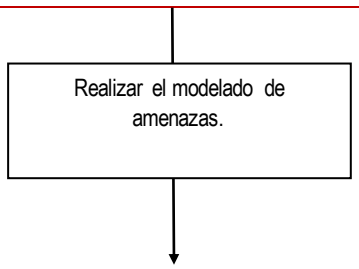
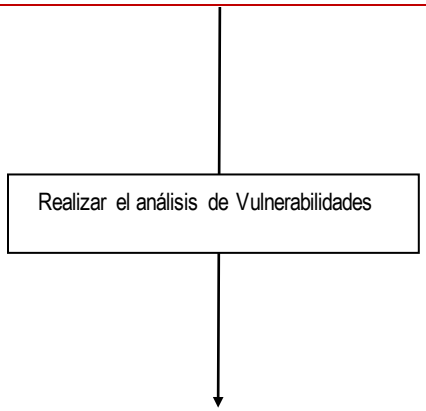
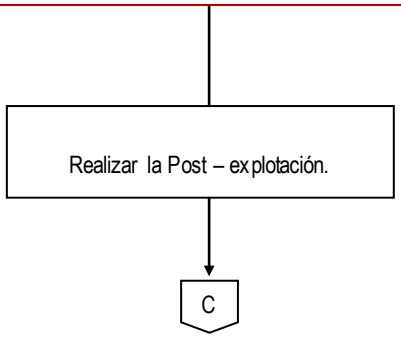
| SÍMBOLO | SIGNIFICADO | USO |
|---|---|---|
|  | Inicio / Fin | Indica el Inicio y el Final del Diagrama de Flujo. |
|  | Operación Actividad | Símbolo de proceso, representa la realización de una operación o actividad. Esta debe ser concreta y en verbo infinitivo. |
|  | Documento | Representa cualquier tipo de documento que se cree dentro de la actividad y que sirva de insumo para otra actividad del mismo procedimiento (Diferente Proceso y/o procedimiento). |
|   | Punto de Control o de Decisión | Un rombo con una pregunta en su interior indica una decisión que tiene normalmente dos alternativas. En las líneas de conexión que salen del rombo se indican las respuestas a la pregunta, que dan lugar a los caminos seguidos en función de estas respuestas, dependiendo de que la condición se cumpla o que no se cumpla. Implica un retroceso o una continuidad en la tarea. (Ver **numeral 2.4.4.4** aclaración uso símbolo de rombo). |
|  | Conector de dirección de flujo (Flecha) | Todos los símbolos deben ir enlazados entre sí, por flechas que indican cómo se realiza la secuencia. Las flechas indican el camino o flujo que sigue el ordenador desde el comienzo hasta la finalización, a través de todas las tareas. Para casos que la flecha genere trazos muy largos o que se cruzan con otras se puede utilizar un conector de círculo. |
|  | Conector | Representa la continuidad del diagrama dentro de la misma página o en distinta página. Enlaza dos pasos no consecutivos y se identifica con números. **Para el caso de la SNR** el conector de círculo referenciará el número de la actividad de la columna "número de actividad" al cual se debe direccionar para dar continuidad al flujo. |
|  | Conector de Página | Representa la continuidad del diagrama en otra página, conexión o enlace con otra hoja diferente en la que continua el diagrama de flujo, este se identifica con letras mayúsculas del abecedario, **se mantiene la misma letra inicialmente utilizada** siempre y cuando en el cambio de página se esté hablando de la misma actividad, **de lo contrario cambia de** letra. Ajustado a la SNR |
|  | Conector de Procedimiento | Procedimiento predefinido: Se utiliza para identificar un documento con el cual interactúa el procedimiento, este símbolo se utiliza de manera opcional ya que el formato en la casilla de "Descripción de la actividad" se describen las interacciones de los procedimientos. Dentro del símbolo se debe citar el nombre del procedimiento. |

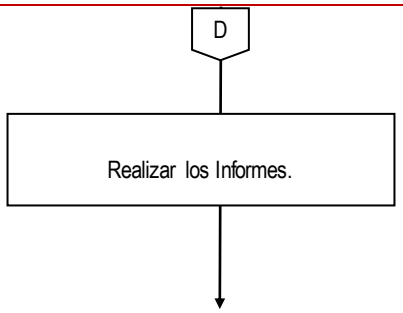
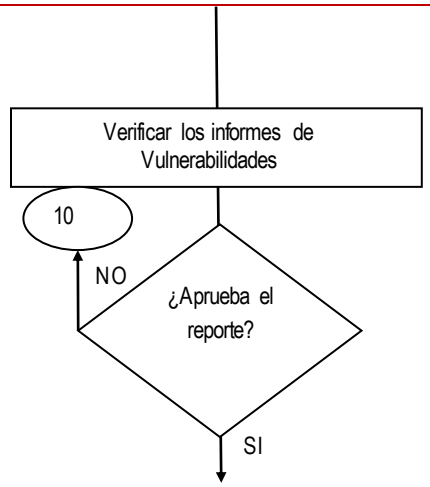
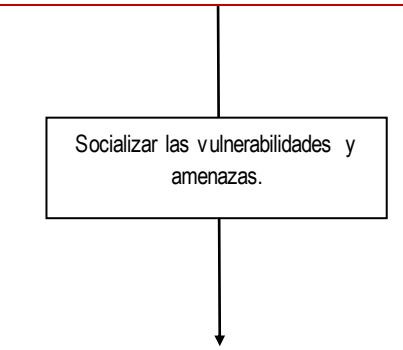
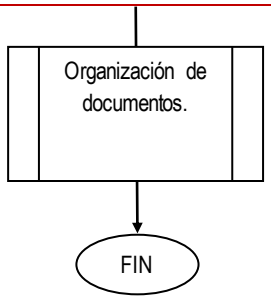
| POLÍTICAS OPERACIONALES |
|---|
| 1. **Todos los procesos deberán tener en cuenta a política general y especifica de la SNR que incluye la política de Vulnerabilidades.** |
| 2. **Los encargados de realizar los análisis de vulnerabilidades deben realizarse mensualmente con todos los procesos de la SNR.** |
| 3. **Las políticas, directrices, manuales y/o cualquier documento generado en el marco del Sistema de Seguridad de la Información, serán de estricto cumplimiento por parte de funcionarios, contratistas y/o terceros.** |
| 4. **Por ningún motivo se pueden realizar análisis de vulnerabilidades o pruebas de intrusión, sin antes tener una autorización escrita diligenciada previamente por la OTI y Grupo de seguridad de la Información, en caso contrario la persona que incumpla puede acarrear sanciones civiles, penales, económicas y sancionatorias de acuerno a la Ley vigente, lo anterior aplica para funcionarios, contratistas y terceros.** |
| 5. **En las pruebas de penetración, actualmente se contratan servicios tecnológicos por proveedores para el análisis en la infraestructura de la Entidad y en donde se considere necesario de acuerdo a la criticidad de los activos de información afectados.** |
| 6. **Las pruebas de intrusión deben realizarse en un ambiente controlado. El proveedor de seguridad por ningún motivo puede generar** |

**denegación de servicio en ninguna plataforma, sistema de información, página web y tampoco puede verse afectado ningún activo de información, en cuanto a confidencialidad, integridad y/o disponibilidad, en caso contrario deberá asumir todos los costos de la resiliencia y debe responder civil, penal y económicamente.**

7. **Las herramientas utilizadas para el escaneo deben cumplir con el estándar de OWASP en su evaluación, toda vez que es una práctica líder el cual fue creado para combatir las causas que hacen que el software sea inseguro así como el Herramientas para la gestión y análisis de Vulnerabilidades actualizadas.**
8. **Los informes, evidencias y de las etapas de descubrimiento, escaneo deben ser confidenciales, por ningún motivo se deben divulgar, salvo estricta autorización por escrito del jefe de la OTI.**
9. **Cualquier evento e incidente de seguridad de la información que genere la explotación de una vulnerabilidad critica debe registrarse en la Mesa de Ayuda (ServiceDesk) gestionada por el Oficial de Seguridad de la Información responsable de responder en un nivel 2 con apoyo del Administrador del sistema y el líder de seguridad de la SNR.**
10. **Para el reconocimiento del activo, se debe hacer un análisis de puertos abiertos definiendo los servicios que se ejecutan en esa IP evidenciando el listado de IPs públicas, balanceadas y servidores locales.**
11. **Definir la arquitectura que tiene cada una las aplicaciones misionales y validar las capas de seguridad con las que cuenta en ese momento.**

| N° | FLUJOGRAMA | DESCRIPCIÓN DE LA ACTIVIDAD | RESPONSABLE | CONTROL DE REGISTROS |
|---|---|---|---|---|
| 1 |  | Elaborar plan anual de auditoria pentest de vulnerabilidades donde se establece: alcance, contexto, cronograma, metodología, responsables y reportes. | Profesional Especializado Administrador del sistema OTI / / Profesional especializado Oficial de seguridad de la OTI / Profesional especializado Líder de Seguridad de la OTI | Plan Anual de auditoria pentest de Vulnerabilidades. |
| 2 |  | Validar y aprobar el plan de auditoría de vulnerabilidades donde debe contener: alcance, contexto, cronograma, metodología, responsables y reportes, dicho plan es actualizado anualmente.<br><br>¿Se aprueba el plan de auditoría de vulnerabilidades?<br><br>**Sí:** Notificar. Actividad 3.<br><br>**No:** Volver a la actividad 1 solicitar correcciones mediante correo electrónico. | Profesional especializado jefe OTI. | E-mail |
| 3 |  | Notificar la aprobación a la empresa a cargo, que cumpla con el Plan Anual de auditoria pentest de Vulnerabilidades.<br>**Nota**: Tener en cuenta los activos que se van a proteger según su criticidad. | Profesional Especializado Administrador del sistema OTI | E-mail. |

| | | | | |
|---|---|---|---|---|
| 4 |  | Elaborar el reporte de Análisis de vulnerabilidades por parte de la empresa a cargo. | Empresa generadora de reporte de vulnerabilidades. | Reporte de Análisis de Vulnerabilidades inicial Empresa a cargo. |
| 5 |  | Realizar la recolección de la información activa, pasiva o semi-pasiva de la mayor cantidad de activos del objetivo, para ser utilizada en las siguientes fases.<br><br>Nota: De acuerdo con el diligenciamiento del cuadro de mando tener en cuenta el Numeral 6 de la guía de Gestión de Análisis de Vulnerabilidades en la SNR. | Profesional Especializado Administrador del sistema OTI / Profesional especializado Líder de Seguridad de la OTI | Cuadro de mando de vulnerabilidades inicial. |
| 6 |  | Definir qué beneficios se pueden obtener si se logran los objetivos de penetrar el sistema para conocer su funcionamiento y mirar los vectores de ataque que puede tener en una exposición tanto atacantes internos como externos, para realizar el modelado de amenazas. | Profesional Especializado Administrador del sistema OTI / Profesional especializado Líder de Seguridad de la OTI | Cuadro de mando de vulnerabilidades actualizado |
| 7 |  | Realizar el análisis de Vulnerabilidades con las herramientas que se contraten donde se definan los niveles de criticidad Altas, Medias y Bajas para plasmar en el cuadro de mando. | Empresa generadora de reporte de vulnerabilidades<br><br>Profesional Especializado Administrador del sistema OTI / Profesional especializado Líder de Seguridad de la OTI. | Cuadro de mando de vulnerabilidades actualizado |
| 8 |  | Realizar la Post – explotación por parte de la empresa a cargo donde se identifique qué información se puede obtener y a qué otros sistemas de información se puede acceder.<br><br>**Nota**: Se crean informes por parte de la empresa contratada que evidencie actividades que permita mitigar las vulnerabilidades para entregar a los administradores y coordinadores de la OTI. | Empresa generadora de reporte de vulnerabilidades. | Cuadro de mando de vulnerabilidades Final<br><br>E-mail. |

| | | | | |
|---|---|---|---|---|
| 9 |  | Realizar los Informes de los resultados obtenidos de todas las fases, teniendo en cuenta las partes interesadas.<br><br>**Nota**: En estos reportes lista las recomendaciones de remediación por cada amenaza o vulnerabilidad evidenciada. | Profesional Especializado Administrador del sistema OTI / Profesional especializado Líder de Seguridad de la OTI. | Informe ejecutivo de vulnerabilidades.<br><br>informe técnico análisis de vulnerabilidades SNR<br><br>Bitácoras de información (históricos). |
| 10 |  | Verificar los informes de Vulnerabilidades, luego de tener los planes de remediación y el control de cambios para hacer el parchados o mejoras en las configuraciones, se realiza la fase de re-test de vulnerabilidades para comprobar que se mitigaron las vulnerabilidades.<br><br>¿Aprueba el reporte?<br><br>**Si:** Avanza a la actividad 12.<br><br>**No:** Ir actividad 10. Realizar los ajustes necesarios, devolver mediante correo electrónico. | Jefe OTI. | E-mail. |
| 11 |  | Socializar las vulnerabilidades y amenazas al jefe de la oficina OTI y al comité de gestión, dueños de los controles para evaluar el riesgo y realizar los planes de mejora para mitigar dichas vulnerabilidades presentes.<br><br>**Nota**: Es una fase en conjunto por parte de los responsables del proceso de vulnerabilidades de la SNR con el fin de mostrar resultados de las fases anteriores con las partes interesadas de la OTI. | Profesional Especializado Administrador del sistema OTI / Profesional especializado Oficial de seguridad de la OTI / Profesional Líder especializado de Seguridad de la OTI | E-mail<br><br>Reunión con las partes interesadas de la OTI. |
| 12 |  | Organizar los documentos en el archivo físico o digital de la OTI de la SNR.<br><br>**Nota**: Cargar en el repositorio definido para tal fin. | Responsable de la documentación | Documentos del proceso.<br><br>Repositorio. |

| **VERSION DE CAMBIOS** | | | |
|---|---|---|---|
| **Código:** | **Versión:** | **Fecha:** | **Motivo de la actualización:** |
| | | | |

| **ELABORACIÓN Y APROBACIÓN** | | | | | |
|---|---|---|---|---|---|
| **ELABORÓ** | **REVISIÓN METODOLOGICA** | **APROBÓ** | | **Vo.Bo Oficina Asesora de Planeación** | |
| Jorge Armando Silva Pineda<br><br>Jorge Alberto Echeverri | Jeiffe Jubelly Muñoz Robayo | Leyla Zoraya Guzmán Rodríguez | Oficina de Tecnología de la Información | Juan Carlos Torres Rodríguez | Coordinador del Grupo de Arquitectura Organizacional Mejoramiento Continuo o quien haga sus veces |
| Oficina de Tecnología de la Información – Sistema de Gestión de Seguridad y Privacidad de la información | Oficina Asesora de Planeación. | | | | |
| Fecha: 03 de Noviembre de 2022 | Fecha: 29 de Noviembre de 2022 | Fecha: 30 de Noviembre de 2022 | | Fecha Aprobación: **06 de Diciembre de 2022** | |