**Identificación, gestión y monitoreo de vulnerabilidades en una Entidad Financiera**

John Wilson Morales Rivera
Andrea Marcela Tejada Ome
Universidad de Los Andes
Proyecto Final

## Introducción

La entidad estudiada en este trabajo es una entidad financiera presente en Latinoamérica. Adicionalmente, en Colombia tiene más de 5.000 colaboradores activos, 570.000 clientes en más de 23 ciudades e inversión anual en tecnología de aproximadamente 70.000 millones de dólares.

Es importante mencionar que, durante la pandemia de COVID-19, a nivel mundial, se ha evidenciado un aumento alarmante de los ciberataques hacia las entidades financieras, lo que conlleva a que las empresas realicen grandes inversiones y desplieguen rápidamente diferentes controles para proteger los datos que viajan constantemente de un sistema a otro. [1]

Teniendo en cuenta lo mencionado anteriormente, se busca en este proyecto disminuir o controlar los diferentes riesgos a los cuales está expuesto la organización por la ausencia en la identificación, gestión y monitoreo de las vulnerabilidades en los servidores y estaciones de trabajo.

Para poder llevar a cabo las tres etapas indicadas en el párrafo anterior, se deberá realizar un análisis profundo, en donde se tengan en cuenta diferentes aspectos como: Recursos de personal, tecnológicos, económicos y físicos. Adicionalmente, investigar qué herramientas se tienen en el mercado con sus respectivos pros y contras, riesgos de seguridad de la información a los cuales se podría estar expuesto a la hora de ir desarrollando el proyecto y una vez sea implementado.

### 1. Definición del Problema

Durante la pandemia de COVID-19, a nivel mundial, se ha evidenciado un aumento alarmante de los ciberataques hacia las entidades financieras, lo que conlleva a que las empresas realicen grandes inversiones y desplieguen rápidamente diferentes controles para proteger los datos que viajan constantemente de un sistema a otro.

En cuanto a las vulnerabilidades en Colombia, durante el año 2020, se vieron ataques a diferentes sectores privados y públicos con un gran impacto (afectación a estructuras críticas), los cuales están relacionados con el hurto, violación de datos personales, acceso abusivo a sistema informático, transferencia no consentida de activos y uso de software malicioso. [1]

Si bien, en esta Entidad Financiera hoy en día tiene el servicio de escaneo trimestral de vulnerabilidades con un tercero, se identifican diferentes oportunidades de mejora en la entidad, las cuales están relacionadas con la confidencialidad, disponibilidad e integridad de la información. Dentro de estas mejoras, están la falta de identificación y gestión oportuna de vulnerabilidades de los activos críticos de la organización (Servidores y portátiles del área de Seguridad de la Información, Tecnología y Ciberseguridad), debido a que al realizar el escaneo cada tres meses, no se tendrían tiempos de respuestas apropiados para solucionar las vulnerabilidades una vez son identificadas, y tanto el CORE como la información sensible de los clientes, se pueden ver afectadas por la explotación de alguna vulnerabilidad por parte de un atacante interno o externo a la entidad dentro de ese tiempo de los tres meses que no se han detectado nuevas vulnerabilidades en los activos.

Es importante resaltar que, este tiempo que se tiene actualmente con el tercero para obtener los resultados de las vulnerabilidades en los diferentes activos del Banco, es bastante alto. Adicionalmente, no se tiene establecido internamente que antes de proporcionar este listado de activos al tercero, en una reunión se integren las áreas de Tecnología, Seguridad de la Información y Ciberseguridad, y se deje el acta correspondiente de las respectivas novedades en el inventario de activos. Tampoco se tiene asignada una correcta criticidad de los activos, la cual sea analizada en conjunto entre la Vicepresidencia de Riesgo Operativo y la de Tecnología, lo cual no permite identificar realmente qué tan crítico puede ser el activo para la entidad, porque para Tecnología puede tener una criticidad media, pero para Operaciones alto porque se tiene interacción con el CORE.

Por lo tanto, se pueden generar diferentes riesgos/impactos a nivel de organización, dentro de los cuales están: Afectación de los servicios ofrecidos a los clientes; degradación de la imagen corporativa por mala reputación; comprometer, alterar y exponer información sensible de los clientes; incurrir en sanciones ante la Superintendencia Financiera de Colombia; generar grandes pérdidas económicas por indisponibilidad de algunos de los servicios, durante un tiempo superior a los 60 minutos.

El rango de indisponibilidad en minutos que se tiene dentro de esta Entidad Financiera se presenta a continuación:

| Rango de Indisponibilidad (Minutos) | | Nivel | Boletín Informativo |
|---|---|---|---|
| Desde | Hasta | | |
| 0Min | 10Min | N1 | Interno IT |
| 11Min | 20Min | N2 | Interno IT |
| 21Min | 30Min | N3 - Proveedores | Interno IT |
| 31Min | 45Min | Auditoría Interna | Informe Comité de Riesgo |
| 45Min | 60Min | Comité Ejecutivo | Informe Ejecutivo |

*Tabla 1. Rango de Indisponibilidad del servicio en minutos.*

## 2. Justificación del Problema

Actualmente, a nivel mundial se ha evidenciado un aumento considerable de los ataques a estas entidades, como por ejemplo al Banco Davivienda a finales del 2021, en donde los atacantes para este caso utilizaron la suplantación de identidad de la Periodista Jessica de la Peña, quien, mientras descansaba, los atacantes desocupaban su cuenta de ahorros. [2]

Con el pasar de los años, se ha evidenciado que gran parte de los ataques realizados, pueden ocasionar una indisponibilidad de los servicios ofrecidos por la entidad, secuestrar información confidencial de los clientes y/o colaboradores, cobro de grandes sumas de dinero para no hacer pública la información recolectada y en el peor de los casos la información nunca se recupera, impactando el acervo documental, backups o snapshot.

Un ejemplo de lo anterior es la vulnerabilidad Log4j, la cual acababa de ser descubierta y no tenía un parche que la solucionara. Esta vulnerabilidad monitorea la actividad en las aplicaciones que están bajo el lenguaje de programación Java, permitiendo que un atacante pueda robar-cifrar información y causar indisponibilidad del servicio como ocurrió en el Banco Itaú Chile. [3]

Adicionalmente, Asobancaria en el último resumen ejecutivo presentó indicadores de vulnerabilidades para el sector financiero, en donde, publica alertas tempranas sobre el crecimiento deliberado de ataques Troyanos Bancarios, diseñados para atacar ordenadores y arquitecturas desactualizadas. En cuanto a los

Remoto Access Trojan (RAT), estos tuvieron un incremento en su uso, debido al aumento del uso de herramientas de acceso remoto por el teletrabajo. [4]

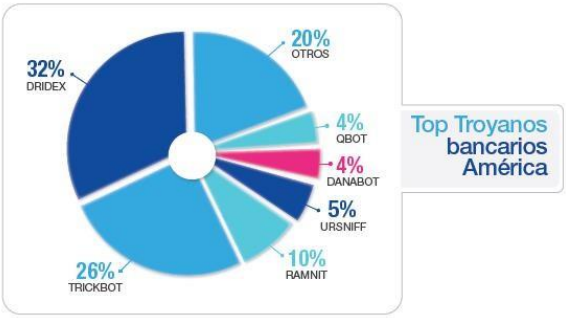


*Figura 2. Resumen Ejecutivo Memoria Anual CSIRT ASOBANCARIA. [4]*

De igual forma, en el mismo informe del resumen ejecutivo de Asobancaria se identifican las acciones con mayor porcentaje de efectividad al momento de un ciberataque, las cuales son:

- Ransomware como carga final y doble extorsión.
- Explotación de vulnerabilidades, derivado de la situación de teletrabajo.
- Vulnerabilidades de loT que permiten recoger información durante el teletrabajo.
- Ataques más sofisticados, prolongados y silenciosos por parte de un software diseñado para evadir controles de seguridad convencionales (APT).

Es importante mencionar que, actualmente esta Entidad Financiera tiene un documento de Políticas y normas de Seguridad de la Información y Ciberseguridad, en donde se mencionan diferentes aspectos para tener en cuenta, dentro de los cuales están:

- Administración de la política y procedimiento de cambio
  - Protección de la información, asegurando la confidencialidad, integridad, disponibilidad, auditabilidad, efectividad, eficiencia y confidencialidad, en la manipulación, custodia y correcto uso de la información utilizada por los usuarios internos y externos.
  - El cumplimiento de las normas y marcos legales a través del conocimiento, acatamiento y alineación de nuestra actuación, conforme a las disposiciones legales emitidas por entes de control nacional e internacional y los acuerdos contractuales establecidos con terceras partes.
  - La protección de los recursos tecnológicos implementando medidas para asegurar los componentes de la infraestructura tecnológica empleados para la prestación de servicios de TI.
  - La continuidad del negocio gestionando los riesgos asociados a los activos de información, velando por la continuidad de los procesos críticos ante incidentes

- Propiedad y actualización del documento
  - La Vicepresidencia de Riesgos del Banco ha delegado la propiedad de este documento a la Gerencia de Riesgo Operativo y el área de Seguridad de la Información responsables de mantenerlo actualizado.
  - El área de Seguridad de la Información debe realizar la revisión de este documento mínimo una vez al año y en caso de realizar ajustes de fondo, deberá presentarlo ante el Comité de Riesgo Operacional.

- Aprobación – Esta política debe ser aprobada por la Junta Directiva del Banco

Sin embargo, se tiene una problemática interna en dicha Entidad Financiera, en donde se han evidenciado las siguientes situaciones:

1. Ausencia o inoportuna actualización del proceso y documentación relacionada con la identificación, gestión y remediación de vulnerabilidades.
2. No se tiene definida una matriz de asignación de responsabilidades (RACI) ni cobertura mínima del porcentaje de activos que van a ser escaneados.
3. Ausencia de planes de escaneos de vulnerabilidades mensuales como mínimo a los activos críticos del Banco.
4. No asignación de la criticidad a los activos del Banco.
5. No gestión de las vulnerabilidades más críticas y de los aplicativos/servicios/activos obsoletos, especialmente, las relacionadas con los activos críticos del Banco.
6. No asunción de riesgos de las vulnerabilidades que no pueden ser remediadas.
7. No contar con un análisis de riesgos para los activos de información que tiene el Banco, el cual consolide el punto de vista de la Vicepresidencia de Riesgos y la Vicepresidencia de Tecnología. [5]

De igual forma, en la organización se realizan escaneos a los activos cada trimestre por parte de un proveedor, en donde a se tienen más de 5.072 dispositivos (servidores, estaciones de trabajo, cámaras de video, impresoras, routers, switches y teléfonos). Es importante mencionar que, el 12 de agosto del 2021, el área de seguridad TI de la sede principal logró explotar una vulnerabilidad a la sede de Colombia a través de la ejecución de una prueba no controlada. Dicha vulnerabilidad, estaba relacionada con el servidor que soportaba los servicios de la página web, ocasionando indisponibilidad del servicio de aproximadamente 10 minutos en la página web pública de la Entidad Financiera en Colombia. Como resultado de dicha explotación, la Sede Principal logró descargar información confidencial de los clientes de Colombia.

Teniendo en cuenta lo mencionado en el párrafo anterior, se evidenció que no se tiene una identificación, gestión y remediación oportuna de vulnerabilidades, por lo tanto, se procedió a realizar las siguientes actividades para solucionar el problema:

- El jueves 12 de agosto, se desactivaron los servicios que generaban la vulnerabilidad y se aplicaron bloqueos a la firma que se personalizó para el IPS.
- El viernes 13 de agosto, se inició el proceso de validación, con apoyo de Chile y Brasil, para determinar si esta vulnerabilidad pudo haber sido aprovechada por un atacante durante el periodo que estuvo activa.
- El sábado 14 de agosto, se actualizó Weblogic, hasta llevar al mayor nivel de actualización posible.
- Se instalaron herramientas de seguridad Trendmicro en los servidores de análisis.
- Se realizó una revisión exhaustiva de todas las vulnerabilidades existentes en el servidor.
- Se realizó la revisión del firewall y no se encuentran reglas que puedan facilitar el compromiso de estos servidores

## 3. Propuesta

Diseñar e implementar una herramienta que permita gestionar de manera oportuna y adecuadamente las vulnerabilidades presentes en los servidores y estaciones de trabajo del área de Tecnología, Seguridad de la Información y Ciberseguridad para una Entidad Financiera.

### 3.1 Objetivos específicos

- Identificar el inventario de activos que tiene el Banco con respecto a servidores y portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad.
- Identificar los servidores y portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad que están obsoletos en el Banco para disminuir la probabilidad de que se exploten vulnerabilidades con mayor efectividad y se esté menos expuesto ante diferentes amenazas.
- Definir los criterios para asignar los niveles de criticidad de los activos que tiene el Banco.

- Aplicar los criterios para identificar los activos críticos que tiene la entidad para comprender cuáles requieren de atención inmediata y cuáles pueden esperar en caso de algún ataque cibernético.
- Validar la criticidad que se tiene definida internamente en la Entidad Financiera para los diferentes activos.
- Seleccionar la herramienta con la cual se escanearán las vulnerabilidades, a través del análisis financiero, cantidad de activos que podrán ser escaneados, la información mínima requerida que se arrojará como resultado del escaneo y el tiempo que se tardará en entregar al Banco la información.
- Identificar semiautomáticamente las vulnerabilidades en los activos críticos en el Banco y tanto clasificar automáticamente la criticidad/severidad como enviar por correo electrónico al equipo/colaborador responsable la información de los servidores y estaciones de trabajo priorizados.
- Identificar las áreas y los responsables de los activos que serán monitoreados para informarles automáticamente la prioridad asignada a sus activos con sus respectivas vulnerabilidades.
- Definir e implementar un procedimiento para monitorear la gestión que se está realizando a los activos más críticos con vulnerabilidades presentes.
- Validar si las vulnerabilidades que no pueden ser remediadas se están llevando para asunción de riesgos, justificando las herramientas que se tienen de contención, controles compensatorios y riesgo al cual está expuesto el banco.
- Identificar el porcentaje de cubrimiento del escaneo de vulnerabilidades que se está realizando a los activos del Banco, a través de la alimentación automática de los dashboards para realizar un monitoreo en línea de los equipos atendidos y su criticidad/severidad.

**4. Diseño e implementación**

La herramienta para gestión de vulnerabilidades para la Entidad Financiera debe responder a tres fases: Identificar, Gestionar y Monitorear. De igual forma, es importante realizar un comparativo del antes de diseñar y el después de implementar el proyecto:

| Antes - Identificación, gestión y monitoreo de vulnerabilidades | Después - Identificación, gestión y monitoreo de vulnerabilidades |
|---|---|
| No se integran las áreas/gerencias/coordinaciones de Tecnología, Seguridad de la Información y Ciberseguridad (dejando un acta), en donde se deje el acta correspondiente de las respectivas novedades en el inventario de activos. | Se integran las áreas/gerencias/coordinaciones de Tecnología, Seguridad de la Información y Ciberseguridad (dejando un acta), en donde se deje el acta correspondiente de las respectivas novedades en el inventario de activos. |
| No hay correcta asignación de la criticidad del activo porque ésta es asignada por la Vicepresidencia de Riesgo Operativo. | Hay una correcta asignación de la criticidad del activo, debido a que ésta asignación se realiza en conjunto con la Vicepresidencia de Riesgo Operativo y la Vicepresidencia de Tecnología. |
| La prioridad con la cual se debían atender las vulnerabilidades se valida de forma manual por un colaborador de la Vicepresidencia de Tecnología. | La prioridad con la cual se debían atender las vulnerabilidades se realiza de forma automática cada semana mediante la ejecución de un script. Dicha herramienta está en la Vicepresidencia de Tecnología. |
| Escaneo de vulnerabilidades: Trimestral. | Escaneo de vulnerabilidades: Semanal. |
| Escaneo realizado por el tercero/proveedor. | Escaneo realizado por un colaborador del Banco. |
| Tercero/ Proveedor descarga los resultados de los escaneos realizados y los entregaba a un colaborador del Banco en formato Excel | Colaborador del Banco descarga los resultados de los escaneos realizados en formato Excel. |

| | |
|---|---|
| Se podía validar si una vulnerabilidad en un activo del Banco fue remediada hasta el siguiente ciclo del escaneo, es decir, a los tres meses. | El colaborador del Banco encargado de realizar los escaneos puede validar si una vulnerabilidad en un activo del Banco fue remediada cuando desee. |
| La información entregada por el tercero/proveedor es consolidada por un colaborador del Banco y la deja en el servidor junto con los archivos generados de forma individual, es decir, sube tres archivos: Consolidado, resultado de escaneo de servidores y resultado de escaneo de las estaciones de trabajo. | La información de los resultados de los escaneos realizados por el colaborador es consolidada por esta misma persona y la deja en el servidor junto con los archivos generados de forma individual, es decir, sube tres archivos: Consolidado, resultado de escaneo de servidores y resultado de escaneo de las estaciones de trabajo. |
| No se gestionan a tiempo las vulnerabilidades más críticas a tiempo, porque se tenía un reporte por parte del tercero/proveedor cada tres meses. | Se gestionan a tiempo las vulnerabilidades más críticas, porque éste reporte se genera semanalmente de forma automática los lunes por medio de la ejecución de un script. |
| No se realiza el monitoreo de las vulnerabilidades que han sido gestionadas, no han sido gestionadas, han sido remediadas y no han sido remediadas. | Por medio de la herramienta de Power BI, se realiza el monitoreo de las vulnerabilidades que han sido gestionadas, no han sido gestionadas, han sido remediadas y no han sido remediadas. En esta herramienta, la Vicepresidencia de Riesgos, Vicepresidencia de Tecnología, Vicepresidencia de Auditoría Interna y miembros del Comité de Riesgo Operativo tendrán permisos de consulta para observar lo relacionado con vulnerabilidades gestionadas, no gestionadas, remediadas y no remediadas en cualquier momento. |
| Actualmente con el tercero/proveedor se evidencia un riesgo latente en la atención de casos, debido a la lentitud en la comunicación y validación (Ejemplo: Explotación de vulnerabilidad el pasado 12 de agosto de 2021 – indisponibilidad de cincuenta (50) minutos), lo cual puede generar pérdidas para la Compañía. | Con las acciones de implementación del proyecto y la mejora de los tiempos en la respuesta a una vulnerabilidad, al momento de presentarse una incidencia de BlackOut y de pérdida económica, será menor, teniendo en cuenta las acciones de identificación, gestión y monitoreo de vulnerabilidades. |

*Tabla 3. Identificación, gestión y monitoreo de vulnerabilidades antes y después de la implementación del proyecto.*

Adicionalmente, la siguiente figura presenta un esquema de las tareas que implementan cada una de las fases, las cuales son identificar, gestionar y monitorear. En cada una de las fases se podrá observar las diferentes actividades que se llevan a cabo y antes de entrar a la fase de identificación, es necesario ejecutar cinco actividades. La información indicada anteriormente, se observa a continuación:

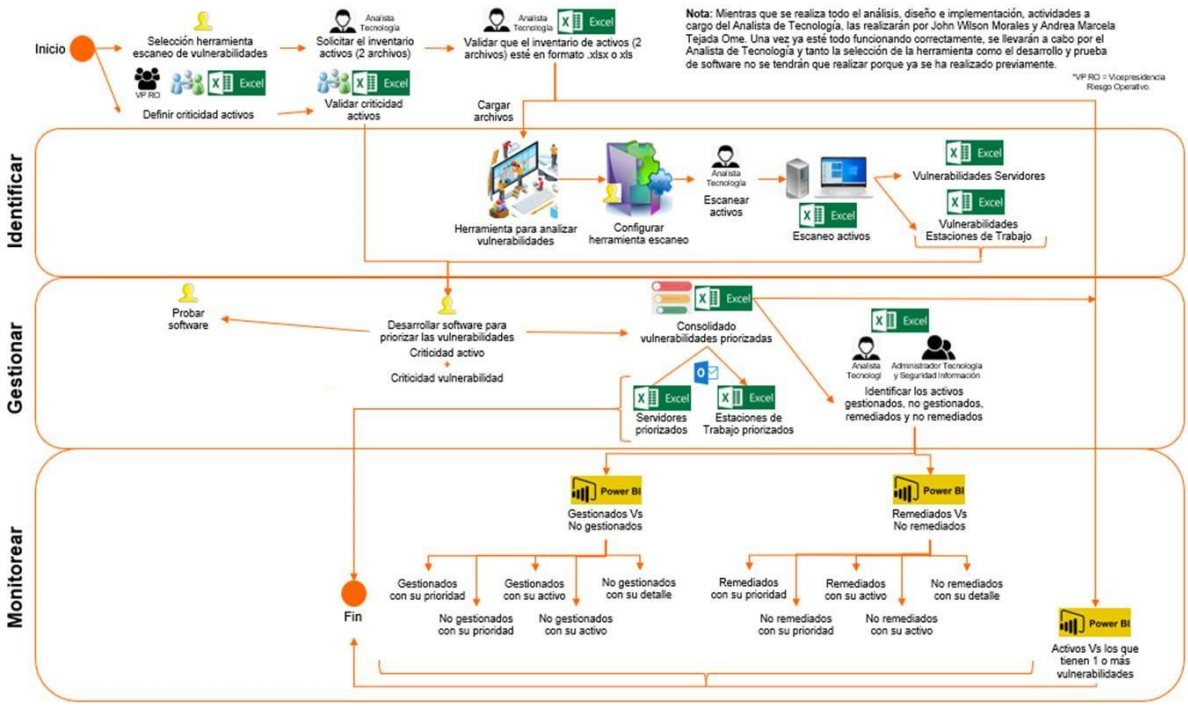


*Figura 4. Diagrama de diseño e implementación.*

Es importante mencionar que, las estaciones de trabajo hacen referencia a las relacionadas con portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad.

Antes de entrar a cada una de las fases, es importante llevar a cabo las siguientes actividades:

**Duración: 4 semanas y 5 días.**

Seleccionar la herramienta que realizará el escaneo de vulnerabilidades, teniendo en cuenta: El presupuesto que tiene la Vicepresidencia de Tecnología (Encargada de la identificación de vulnerabilidades); la cantidad de activos que se alcanzarán para escanear; si admite el formato .xlsx o .xls y si lo toma de una ruta o una persona debe realizarlo manualmente; la cantidad y el costo de cada licencia; los resultados que arrojará la herramienta, tales como, fecha del escaneo de vulnerabilidades, nivel de severidad de la vulnerabilidad, la dirección IP del activo que presentó la vulnerabilidad, la dirección MAC del activo, el puerto, el nombre del activo, el nombre del archivo que se cargó en la herramienta, el CVE de la vulnerabilidad, el título de la vulnerabilidad, el Sistema Operativo (SO) del activo, y si se tiene algún exploit.

Una vez seleccionada la herramienta, el Analista de Tecnología va a solicitar al administrador del área de Tecnología el inventario de los servidores (Un archivo) y al administrador de Seguridad de la Información el de los portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad (Un archivo). Éstos dos archivos entregados siempre los tienen en formato .xlsx o xls, sin embargo, esta misma persona deberá validar que estén en cualquiera de esos dos formatos y la identificación de los activos se realizará cada mes por la Vicepresidencia de Tecnología.

**Duración: 2 semanas.**

En una reunión con la Vicepresidencia de Riesgo Operativo (Enfocado en el Negocio) y de Tecnología, definir en un documento de Excel la criticidad de los activos y estaciones de trabajo del Banco (Portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad), luego validar con estas dos Vicepresidencias si están de acuerdo con las criticidades definidas y dejarlas en el mismo formato que se

tenía (Excel). Es importante mencionar que, la criticidad de los activos se validará mensualmente (solo se revisarán los que hayan cambiado su criticidad) o cada vez que ingrese o se cambie un activo en la entidad.

El archivo Excel relacionado con la criticidad del activo, tendrá lo siguiente: Dirección IP, el nombre, la dirección MAC de la máquina y su respectiva criticidad (Alta, media y baja). Dicha criticidad no es asignada bajo alguna metodología, sino que se realiza en conjunto con la Vicepresidencia de Riesgos y la Vicepresidencia de Tecnología.

A continuación, se describirán cada una de las fases:

**Identificar (Duración: 2 semanas).**

Con base en el inventario de servidores y portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad, los cuales fueron validados que estén en formato .xlsx o .xls, realizar lo siguiente: El Analista de Tecnología cargará manualmente los archivos a la herramienta de vulnerabilidades que se seleccionó previamente y será adquirida por la Entidad Financiera; luego, configurarla (una única vez) y el Analista de Tecnología dará la opción de escanear activos para que de forma automática se tengan tanto los activos escaneados como los dos archivos con las respectivas vulnerabilidades, en donde uno estará relacionado con los servidores y el otro con las estaciones de trabajo. Estos dos archivos de las vulnerabilidades tienen la respectiva criticidad y serán insumo para el software que se desarrollará para gestionar las vulnerabilidades.
Cabe resaltar que, actualmente en el Banco no se tiene una herramienta que maneje el inventario, sino que se tiene disponible en la ruta de un servidor de la Vicepresidencia de Tecnología y por el momento no lo ven necesario, pero si como un gran gasto.

**Gestionar (Duración: 5 semanas).**

Teniendo en cuenta el archivo Excel resultado de la validación de la criticidad de los activos y la criticidad de la vulnerabilidad presentes en los dos archivos Excel (Vulnerabilidades Servidores y Vulnerabilidades Estaciones de Trabajo), desarrollar un software nuevo que permita priorizar las vulnerabilidades. Dicho software será Python y se ejecutará de forma automática por medio del programador de tareas.

Una vez terminado el software, probar que realmente está arrojando automáticamente un archivo Excel consolidado con las vulnerabilidades priorizadas como se requiere.

Posteriormente, el software arrojará automáticamente tres archivos Excel, uno relacionado con los servidores priorizados, otro con las estaciones de trabajo priorizadas y otro con el consolidado tanto de los servidores como estaciones de trabajo priorizados. El archivo relacionado con las estaciones de trabajo priorizadas y los servidores priorizados se enviarán automáticamente desde Python al correo del Analista de Tecnología. Para enviar estos dos archivos, se utilizará un correo que sea únicamente para lo relacionado con vulnerabilidades y tenga dominio del Banco para enviarlos.

Del archivo Excel que tiene el consolidado de las vulnerabilidades priorizadas, el Analista de Tecnología junto con los administradores de Tecnología y Seguridad de la Información, identificarán manualmente las vulnerabilidades de los activos que fueron gestionadas, las que no fueron gestionadas, las que no fueron remediadas y las que fueron remediadas. El resultado de lo mencionado anteriormente, lo almacenarán en un archivo de Excel. Las vulnerabilidades que no fueron gestionadas ni remediadas se tendrán que reportar al Comité mensual de Riesgo Operativo que se realiza mensualmente en conjunto con la Vicepresidencia de Tecnología con su respectiva justificación (Ejemplo: No hay suficiente personal, no hay suficiente presupuesto, etc) y/o asunción del riesgo.

**Monitorear (Duración: 5 días).**

De los dos archivos Excel obtenidos en la fase de Gestionar, los cuales corresponden a los servidores y estaciones de trabajo (Portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad)

priorizados, el Analista de Tecnología junto con los administradores de Tecnología y Seguridad de la Información, identificarán aquellos activos que no se podrán remediar y después se creará un dashboard en donde se mostrarán estos resultados.

De los dos archivos Excel que se obtuvieron de la validación del inventario de activos (Actividad realizada antes de pasar a la fase de Identificar) y el archivo Excel con la información de los activos que fueron escaneados, se creará un dashboard para mostrar el comparativo entre los activos que tiene el Banco y la cantidad de activos que fueron escaneados.

Adicionalmente, con el archivo Excel en donde están los activos gestionados y no gestionados (De la fase Gestionar), se crearán dos dashboard:

- Un dashboard mostrará un comparativo entre los activos gestionados y los no gestionados.
- El otro dashboard reflejará un comparativo entre los gestionados y los no gestionados por administrador, es decir, los relacionados con Tecnología (Servidores) y Seguridad de la
- Información (Estaciones de Trabajo: Portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad).

El cronograma con las actividades o fases a nivel general, se pueden evidenciar a continuación:

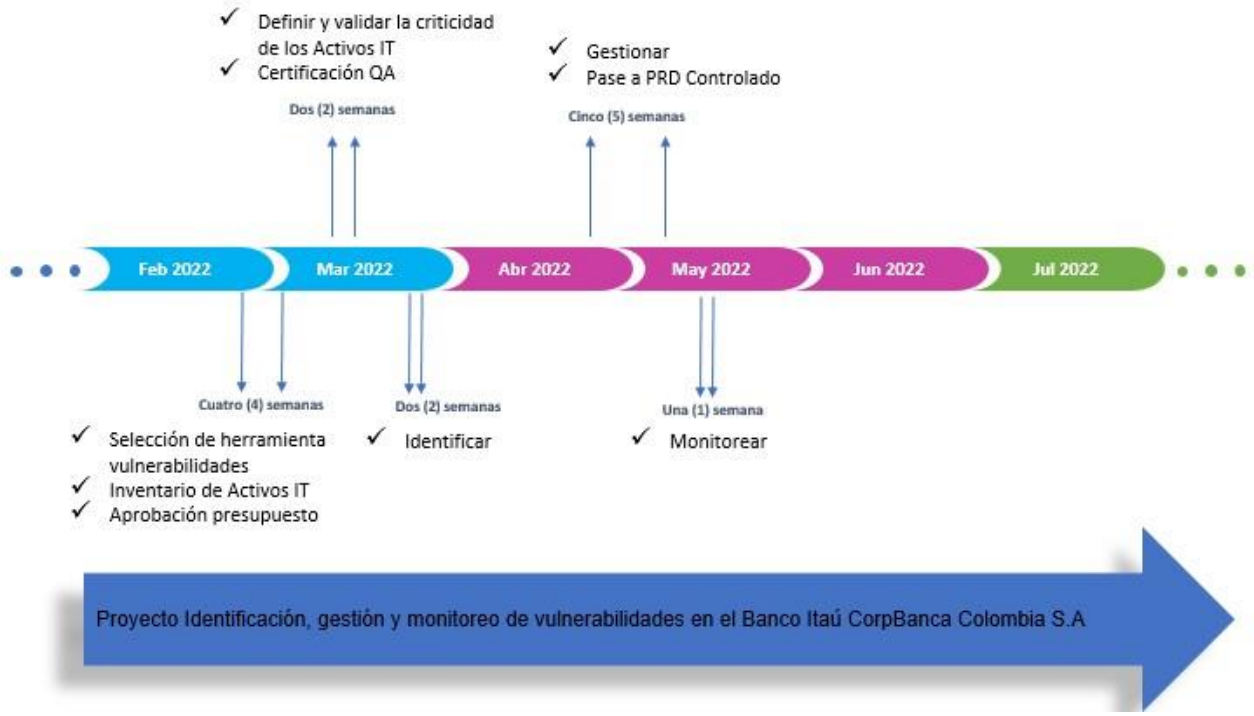


*Figura 5. Línea de Tiempo actividades/fases.*

La información presentada en los dashboards, podrá observarse por parte del Analista de Tecnología, el administrador del área de Seguridad de la Información y el administrador del área de Tecnología.

Una vez ya estén maduras las fases de monitorear, gestionar e identificar, es posible analizar, diseñar e implementar para los demás activos que tiene el Banco (Routers, switchs, teléfonos IP, entre otros). Llevar a cabo lo anterior, podría tardar aproximadamente siete meses más.

**5. Requerimientos**

- Funcionales

La herramienta seleccionada para identificar vulnerabilidades deberá:

- Permitir la carga de los dos archivos que tienen los activos del Banco relacionados con los servidores y las estaciones de trabajo (Portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad).
- Permitir que se configure, de acuerdo con lo que requiera observar como resultado la Vicepresidencia de Tecnología en cuanto a las vulnerabilidades identificadas.
- Arrojar automáticamente en un archivo Excel, las vulnerabilidades identificadas en los servidores, en donde se logre evidenciar como mínimo la fecha del escaneo de vulnerabilidades, nivel de severidad de la vulnerabilidad, la dirección IP del activo que presentó la vulnerabilidad, la dirección MAC del activo, el puerto, el nombre del activo, el nombre del archivo que se cargó en la herramienta, el CVE de la vulnerabilidad, el título de la vulnerabilidad, el Sistema Operativo (SO) del activo, y si se tiene algún exploit.
- Arrojar automáticamente en un archivo Excel, las vulnerabilidades identificadas en las estaciones de trabajo (Portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad), en donde se logre evidenciar como mínimo la fecha del escaneo de vulnerabilidades, nivel de severidad de la vulnerabilidad, la dirección IP del activo que presentó la vulnerabilidad, la dirección MAC del activo, el puerto, el nombre del activo, el nombre del archivo que se cargó en la herramienta, el CVE de la vulnerabilidad, el título de la vulnerabilidad, el Sistema Operativo (SO) del activo, y si se tiene algún exploit.
- La herramienta seleccionada para identificar vulnerabilidades deberá configurarse y tenerse en el portátil asignado al Analista de Tecnología y en el portátil backup que está en el Banco.

- El software que será desarrollado deberá:
- Arrojar automáticamente en un archivo Excel el consolidado con las vulnerabilidades priorizadas.
- Arrojar automáticamente en un archivo Excel los servidores priorizados.
- Contar con un módulo de ayuda en línea, el cual tendrá un glosario para guiar al usuario final, al momento de una duda con respecto al funcionamiento del software.
- Entregar los documentos Excel con una clave para poder ver la información contenida en cada uno.
- Arrojar automáticamente en un archivo Excel las estaciones de trabajo (Portátiles del área de Tecnología, Seguridad de la Información y Ciberseguridad) priorizadas.

- El dashboard que permitirá monitorear lo relacionado con la gestión de vulnerabilidades:
- Permitirá la carga de los siguientes archivos en formato Excel. Dichos archivos corresponden a: Activos sin poderse remediar, inventario de activos, activos escaneados, activos que fueron gestionados y los que no se gestionaron.
- Permitirá como mínimo observar cuatro gráficos diferentes en una misma hoja de diseño (Ejemplo: Gráfico de barras, torta, líneas y dispersión).
- Observar el histórico (mes a mes) de las vulnerabilidades identificadas.

- No funcionales
- La herramienta seleccionada para identificar vulnerabilidades deberá arrojar los resultados en un tiempo inferior a 1 hora.
- El software que será desarrollado deberá:
- Respaldarse en la nube (AWS) cada 24 horas.
- Proporcionar mensajes de error que sean informativos y orientados al usuario final.
- Disponible cuando se requiera, es decir, se puede ejecutar en cualquier momento.
- Soportar más de 5.000 registros para analizar.

- El dashboard que permitirá monitorear lo relacionado con la gestión de vulnerabilidades:
- Podrá ser visualizado a cualquier hora y día.
- La información de los gráficos (barras, tortas, líneas y/o dispersión) se podrá ver por día y año a año.

6. **Selección de la Herramienta de Monitoreo Vulnerabilidades: Comparativo entre herramienta de Nexpose y Nessus**

Teniendo en cuenta que, actualmente la entidad Financiera en Colombia cuenta con la herramienta de Nexpose para la identificación de las vulnerabilidades con un tercero y es utilizada en la Sede Principal de Brasil, se contempla mantener el mismo estándar para una fácil administración de los Equipos de TI, resulta ser más económico, más fácil de usar, visualizar los datos y es más completa.

A continuación, se detallará un cuadro comparativo de las ventajas y desventajas contra la herramienta Nessus "competencia en el mercado", con el fin de dar una radiografía a lo que se tiene en la Organización.

**Comparativo entre herramienta de Nexpose y Nessus**

| ***Parámetro*** | ***Nexpose*** | ***Nessus*** |
|---|---|---|
| **Prueba** | Disponible por 30 días. | Disponible por 7 días. |
| **Escaneo** | Disponible: Autenticación de clave pública SSH, basada en contraseña, escaneo autenticado Kerberos, autenticación LDAP, etc. | Disponible: Autenticación de clave pública SSH, basada en contraseña, etc. |
| **Sistema operativo compatible** | Se puede instalar en Ubuntu Linux 20.04 LTS, Ubuntu Linux 18.04 LTS, Ubuntu Linux 16.04 LTS, Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows 8.1, Red Hat Enterprise Linux Server 8, Red Hat Enterprise Linux Server 7, Red Hat Enterprise Linux Server 6, CentOS 7, Oracle Linux 7, SUSE Linux Enterprise Server 12. | Se puede instalar en Debian/Kali Linux, Red Hat/CentOS/Oracle Linux, Fedora, FreeBSD, Ubuntu, Mac OS X, Windows Server 2008 y Windows Server 2012, SUSE Linux, Windows 7, 8 y 10. |
| **Comprobaciones de cumplimiento** | Compatibilidad con SOC 2 tipo II, competencia de seguridad de Amazon Web Services (AWS), Ley SarbanesOxley (SOX), Reglamento general de protección de datos de la UE (GDPR), etc. | Guía de mejores prácticas y políticas de seguridad, como puntos de referencia CIS, SOX, FISMA, HIPAA, etc. |
| **Escaneo externo** | Disponible. | La opción de escaneo remoto está disponible. |

| | | |
|---|---|---|
| **IPv6** | Soporte de escaneo IPv6. | Soporte de escaneo IPv6. |
| **Comparativo entre herramienta de Nexpose y Nessus** | | |
| ***Parámetro*** | ***Nexpose*** | ***Nessus*** |
| **Solución de hardware** | Disponible. | No disponible. |
| **Vulnerabilidades conocidas de aplicaciones web** | Vectores de ataque de escritorio (Adobe Reader, Acrobat, Quicktime, navegadores, Flash, Java), identificación de vulnerabilidades de proveedores (Adobe, Apple, Microsoft), Web (Apache, IIS, OWASP Top 10, PHP, XSS, SQL Injection, navegadores), funcionamiento Sistemas (Microsoft Windows, Linux, Mac OS X), Bases de datos (Oracle, Microsoft SQL Server, MySQL). | Identificar vulnerabilidades conocidas de aplicaciones web. |
| **Informe de auditoría** | Informe de problemas prioritarios disponible. | Resultados de cumplimiento en Nessus: Aprobado, fallido y advertencia. |
| **Costos (Aprox)** | Hasta 128 IP´s cuesta alrededor de USD 2.000 – (15 USD cada Licencia). | 1 Año: USD 2.999.<br>2 Años: USD 5.830.<br>3 Años USD 8.520. |

*Tabla 6. Comparativo Nexpose con Nessus.*

Teniendo en cuenta las ventajas y desventajas en el comparativo anterior, sumado a que la Sede Principal tiene implementado Nexpose como herramienta de análisis de vulnerabilidad, se toma la decisión de continuar con la homologación en su CORE de TI.

**7. Creación de gráficas para realizar el monitoreo de vulnerabilidades en Power BI**

A través de la herramienta de Office Power BI, se realiza el monitoreo de las vulnerabilidades que han sido gestionadas, no gestionadas, han sido remediadas y no remediadas, por medio de un dashboard en tiempo real al cual podrán tener permiso de consulta la Vicepresidencia de Riesgos, Vicepresidencia de Tecnología, Vicepresidencia de Auditoría Interna y miembros del Comité de Riesgo Operativo. Lo anterior, permitirá realizar un seguimiento y análisis cada vez que se desee por parte de las Vicepresidencias mencionadas, tener un mayor control, gestión de las vulnerabilidades y visualización de los datos más importantes.

La información presentada en la herramienta, será traída de forma automática desde una ruta del servidor de la Vicepresidencia de Tecnología, en donde se tendrá el inventario de activos, los activos que tienen una o más vulnerabilidades, los activos gestionados, no gestionados, remediados y no remediados, los cuales se podrán observar en una torta, un diagrama de barras, un anillo y una tabla con su respectivo detalle.

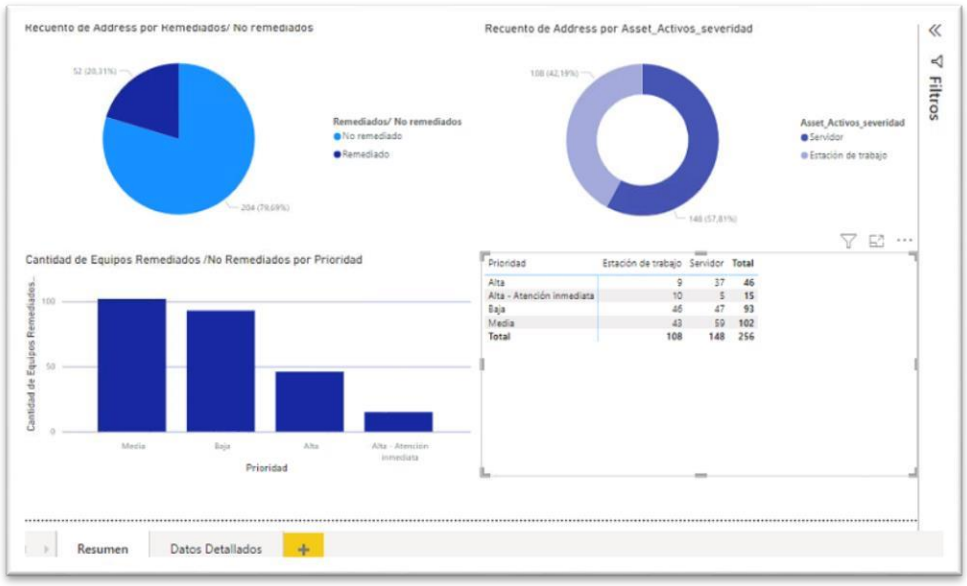


*Figura 6. Dashboard PowerBI.*

## 8. Conclusiones

La clave del éxito para este proyecto correspondió al saber llevar el ciclo de: Identificar, gestionar y monitorear. Toda vez que en la actualidad el flujo llegaba hasta la identificación. “Actividad que estaba bajo la gestión de un tercero”, los últimos dos no se aplicaban en la Entidad Financiera.

Una vez es diseñado el proyecto In-house, se toma el control y se articula desde Identificar, Gestionar y Monitorear; optimizándose el seguimiento a través de herramientas que permiten estar en tiempo real midiendo la salud de los Equipo de TI.

Ahora, en el marco del presupuesto: El caso de negocio presentado a la Junta Directiva de la Entidad Bancaria, se destaca la reducción de los costos fijos “honorarios profesionales al actual proveedor”. Es decir, con la ejecución del proyecto In-house, el balance en la proyección y rentabilidad del proyecto empezaría a dar frutos desde el primer semestre de la implementación.

Sobre el Punto de Equilibrio del Proyecto, tendríamos dos vías: Reducir los minutos de indisponibilidad a un 50% de lo que hoy nos entrega el proveedor actual. Sumado a que, en el peor de los escenarios, podemos tener una indisponibilidad de noventa (90) minutos. Es decir, superando casi un 30% de lo que hoy pagamos; aun el proyecto en mención seguiría dando un balance positivo a la organización.

**Referencias**

[1] Ciberseguridad – Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020 – BID & OEA https://observatoriociberseguridad.org/#/final-report

[2] Suplantación de Identidad Periodista Jessica de la Peña (10 de octubre de 2021) – Articulo Revista Semana https://www.semana.com/nacion/articulo/son-unos-desgraciados-jessica-de-la-pena-cuentacomo-le-desocuparon-sus-cuentas-de-davivienda/202135/

[3] Copyright – Apache Logging, Apache Log4j, Log4j, Apache, the Apache feather logo, and the Apache Logging project logo are trademarks of The Apache Software Foundation (23-02-22) https://logging.apache.org/log4j/2.x/

[4] Asobancaria, “DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA.” Oct. 2019, [Online]. Available: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-087/19

[5] Resumen Ejecutivo Memoria Anual ASOBANCARIA – (01 de junio de 2021) – Mediante el CSIRT de esta entidad, se le comunica al ecosistema financiero el modus operandi de los piratas informativos https://csirtasobancaria.com/publicaciones?year=2021&month=6.