ESPECIFICACIÓN DE UN MÉTODO QUE AYUDE AL BANCO POPULAR A IDENTIFICAR Y DISMINUIR LA BRECHA DE SEGURIDAD DE SU SOFTWARE ANTIVIRUS

JUAN PABLO ANTONIO SALCEDO DÍAZ

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ, D.C.

2022

ESPECIFICACIÓN DE UN METODO QUE AYUDE AL BANCO POPULAR A IDENTIFICAR Y DISMINUIR LA BRECHA DE SEGURIDAD DE SU SOFTWARE ANTIVIRUS

Presentado Por:

JUAN PABLO ANTONIO SALCEDO DÍAZ

2219450

Trabajo de grado para la titulación como Ingeniero de Telecomunicaciones

Tutor:

ING. GERALD BREEK FUENMAYOR RIVADENEIRA

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ D.C

2022

Nota de aceptación.

_____

_____

_____

_____

_____

_____

Ing. Gerald Breek Fuenmayor Rivadeneira

Tutor

_____

Jurado

_____

Jurado

_____

Fecha

Resumen

Los equipos tecnológicos como servidores, computadores portátiles, desktops, entre otros necesitan estar protegidos mediante esquemas de seguridad física en las instalaciones del banco (oficinas, regionales, casa matriz) así como seguridad de la información y seguridad informática. Es importante estos dos últimos principalmente porque es gracias a esto que el banco puede estar seguro en cuanto a fugas de información de sus clientes y/o trabajadores (claves, tarjetas de crédito, información personal, etc.) como también de ataques por parte de hackers o piratas cibernéticos que busquen comprometer los insumos de la entidad.

Teniendo en cuenta lo anterior, el Banco Popular debe ser una entidad que preste especial atención a la ciberseguridad de sus equipos, y en este presente documento se plantearán metodologías o estrategias que permitan no solo corregir las brechas de seguridad existentes sino también mejorar los procesos que se vienen haciendo para que estas no aparezcan nuevamente.

Palabras Clave

Brecha de seguridad, Antivirus, Banco, Entidad Bancaria, Sistemas de Información, Herramientas de Seguridad, Ciberseguridad, Seguridad de la Información.

Abstract

Banco Popular, belonging to the Grupo AVAL bank network, is one of the most important banking entities in the country thanks for his contribution to the provision of services to the public sector in Colombia. This banking entity has offices in 29 departments of Colombia and has in his network more than 193 offices throughout the country. These figures give an indication of the great magnitude of technological equipment that the bank has at the service of its workers.

This technological equipment needs to be protected by means of physical security schemes in the bank's facilities (Offices, Regionals, Operative Center) as well as information security and computer security. These last two are important mainly because thanks to this that the bank can be safe in terms of information leaks from its customers and/or workers (passwords, credit cards, personal information, etc.) as well attacks by hackers or cyber hackers seeking to compromise the entity's supplies.

Taking into account, Banco Popular must be an entity that pays special attention to the cybersecurity of its teams, and in this present document methodologies or strategies will be planted that allow not only to correct the existing security gaps but also to improve the processes that They are being done so that these do not appear again.

Keywords

Security breach, Antivirus, Bank, Entity Bank, Information System, Security Tools, Cybersecurity, Information Security.

Tabla de Contenidos

PARTE I 9
Capítulo 1 10
Introducción 10
1. PLANTEAMIENTO DEL PROBLEMA 11
2. JUSTIFICACIÓN 12
3. OBJETIVOS 15
3.1 OBJETIVO GENERAL 15
3.2 OBJETIVOS ESPECÍFICOS 15
4. ALCANCE 16
METODOLOGÍA 18
5.1 TIPO DE INVESTIGACIÓN 18
5.4 FUENTES 18
5.4.1 FUENTES PRIMARIAS 18
5.4.2 FUENTES SECUNDARIAS 19
5.5 INSTRUMENTOS DE CAPTURA, PROCESAMIENTO Y GENERACIÓN DE RESULTADOS 19
5.6 PASOS METODOLÓGICOS 19
5.6 CRONOGRAMA DE ACTIVIDADES 20
5.7 Diagrama de Gantt 21
PARTE II 22
Capítulo 2 23
Estado del Arte 23
Capítulo 3 26
Bases Conceptuales 26
3. MARCO CONCEPTUAL 27
3.1 BRECHA DE SEGURIDAD 27
3.2 TRIADA DE LA CIBERSEGURIDAD CIA 27
3.2.1 Confidencialidad 28
3.2.2 Integridad 29
3.2.3 Disponibilidad 29
3.3 ANTIVIRUS 29

3.3.1 ¿Cómo Funciona? 30
3.4 HERRAMIENTA CLIENT MANAGEMENT 32
Capítulo 4 35
Marco Referencial 35
4.1 NORMA ISO 27001 36
4.2 MÉTODO DELPHI 38
PARTE III 39
Desarrollo de la Investigación 39
POLÍTICA DE CONFIDENCIALIDAD CON EL BANCO POPULAR 40
Capítulo 1 41
Estado Actual de la gestión de brechas de seguridad en Antivirus 41
Capítulo 2 45
Acciones de Mejoramiento 45
2.1 RECOMENDACIONES A TENER EN CUENTA DE ACUERDO A LA NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001. 46
2.1.1 GENERALIDADES DE LA PROPUESTA 46
2.1.2 Valorar Los Riesgos De La Seguridad De La Información Dentro De La Propuesta. 46
2.1.3 Tratamiento De Los Riesgos Encontrados 47
2.2 MÉTODO PARA IDENTIFICAR Y DISMINUIR LA BRECHA DE SEGURIDAD EN SU SOFTWARE ANTIVIRUS A NIVEL NACIONAL. 47
2.2.1 Reporte de cruce de herramientas 47
2.2.2 Método Actual 49
2.3 DEFINICIÓN Y MEJORAMIENTO DEL PROCESO CON EL CUAL SE IDENTIFICAN LAS BRECHAS DE SEGURIDAD EN EL SOFTWARE ANTIVIRUS. 51
2.3 GESTIÓN DE BRECHAS DE SEGURIDAD EN ANTIVIRUS HASTA EL CIERRE TOTAL O PARCIAL. 56
2.3.1 Despliegues por medio del Client Management 57
2.3.2 Gestión de equipos por medio de soporte técnico. 59
2.3.3 Gestionamiento final de la brecha de seguridad en Antivirus. 62
2.4 PROCESO DE MEJORA CONTINUA PROPUESTO PARA QUE LA BRECHA DE SEGURIDAD EN EL SOFTWARE DE ANTIVIRUS NO SE VUELVA A REABRIR 64
2.4.1 Documentación de casos encontrados. 64
2.4.2 Plan de mejora continua 66
Capítulo 3 ..... **¡Error! Marcador no definido.**

Método Delphi 69
3.1 FORMULARIO SUMINISTRADO A LOS EXPERTOS. 69
3.2 RESPUESTA #1 ..... **¡Error! Marcador no definido.**
3.3 RESPUESTA #2 ..... **¡Error! Marcador no definido.**
3.3 Análisis de las Respuestas 73
PARTE IV 74
CONCLUSIONES 75
RECOMENDACIONES 76
Referencias Electrónicas 78

PARTE I

Introducción a la Investigación

Capítulo 1

Introducción

En este capítulo se muestran los primeros factores que se debe tener en cuenta antes de trabajar de lleno con el método a especificar. Para esto se inicia con la problemática que se quiere solucionar, la justificación donde se abordan situaciones en las que este trabajo es beneficioso y los objetivos que se deben cumplir para que la propuesta se desarrolle de la mejor manera. Por último, se expresa el alcance de la propuesta, así como la metodología del trabajo y al final todo se describe en un cronograma y diagrama de Gantt.

1. PLANTEAMIENTO DEL PROBLEMA

El Banco Popular es una entidad muy grande y está ubicado a nivel Nacional con más de 200 sedes, al ser una entidad bancaria el flujo de datos e información siempre va a ser sensible y a la vez bastante deseada por los atacantes cibernéticos por lo que sus herramientas de seguridad siempre deben estar disponibles para la prevención de ataques. Es por esto que de acuerdo a la pasantía en el Banco Popular se puede constatar que la entidad dispone de diferentes herramientas de seguridad para la protección de sus equipos, algunas de estas son (Antivirus, Software de Data Loss Prevention, Client Management, Proxy, VPN y Cifrado).

Teniendo en cuenta esto, la entidad realiza diariamente un informe detallado de la cantidad de equipos (Laptops y Computadores de mesa) protegidos por cada herramienta, resaltando el porcentaje de cobertura que se tiene en cada una de ellas, en el cual luego de pasar los datos por el cruce de herramientas en el que se puede evidenciar el porcentaje de cobertura teniendo en cuenta la cantidad de equipos en inventario, con esto en cuenta se determinó que en la herramienta Antivirus el porcentaje de cobertura es del 85% con respecto al total de equipos en inventario, mientras que en las otras herramientas supera el 98%.

Esto indica que el no solucionar este problema rápido, dejaría a un 20% de los equipos del banco vulnerables a amenazas no cubiertas por el agente de Antivirus, por lo que se necesita disminuir esa brecha a una cobertura de mínimo un 98%. Teniendo en cuenta la problemática anterior, este trabajo se enfoca en responder la siguiente pregunta ¿Qué estrategias se deben usar para disminuir la brecha de seguridad de Antivirus y que esta no vuelva a reabrirse?

2. JUSTIFICACIÓN

El presente trabajo está enfocado en especificar un método que ayude al banco a mejorar la forma en la que ellos gestionan sus brechas de seguridad priorizando en este caso la herramienta de seguridad antivirus. Sin embargo, es importante saber que más allá de la solución a esta problemática, también podríamos encontrar otros beneficios en el campo económico, técnico, operativo, académico, ambiental, legal y social.

Dentro del campo económico esta propuesta puede llegar a ser bastante beneficiosa ya que las empresas normalmente contratan licencias de sus softwares con los proveedores en este caso con antivirus, el hecho de que estas licencias no funcionen en ciertos equipos hace que sea dinero que no se está utilizando de la mejor manera y se está perdiendo, por lo que, si se logra tener un índice alto de cobertura de todas las herramientas de seguridad, el dinero se verá mejor invertido.

Con respecto al campo técnico, este método puede ayudar a mejorar los tiempos de respuesta a incidentes de brechas de seguridad, así como de alivianar la gestión realizada por parte del equipo de soporte técnico pudiendo enfocarse en otros procesos priorizados.

La operación dentro del área es otro de los temas que pueden llegar a mejorarse ya que esta gestión necesita de un apoyo mutuo entre distintas áreas operativos dentro del banco, destacando así la importancia de que las empresas trabajen más como una unión que como áreas distintas y completamente independientes. Por otra parte, la operatividad tiene una columna base y es los tiempos en los que se realizan las cosas, con este método propuesto se puede mejorar estos tiempos teniendo siempre en cuenta planes de mejora continua.

Siguiendo con el campo académico, lo que se busca con este escrito es que sea una ayuda para el interesado sobre conocer un método que se pueda implementar en muchas empresas y que

sea un soporte académico para referenciarse en caso de que logre el objetivo de ayudar. A su vez, este trabajo tiene un aporte para la universidad ya que no se tienen muchos trabajos de este tema de brechas de seguridad.

En cuanto al tema ambiental, si bien este es un trabajo sobre el manejo de softwares más que todo, uno de los puntos es conocer cómo influye un software en un hardware y a su vez como este último puede afectar el medio ambiente. En este caso la solución al gestionamiento de brechas de seguridad aporta mucho a los consumos altos de memorias RAM en los computadores si las herramientas de seguridad funcionan de manera correcta, por lo que el buen uso de la misma disminuye las temperaturas de los equipos y así se contribuye un poco más al calentamiento global.

Los temas legales siempre van a estar presentes en las compañías y dentro del manejo de la información, sin duda el hecho de que se dé una solución al mejoramiento de brechas de seguridad, es una solución directa a la protección de datos personales los cuales pueden implicar en conflictos legales en caso de que estos sean vulnerados de alguna forma. Estos problemas no solo pueden estar presentes con entidades fuera den lanco son también dentro, ya que es bien conocido la existencia de auditorías internas que, si bien están enfocadas a encontrar falencias por mejorar, el hecho de encontrar fallas en las herramientas de seguridad puede suponer de sanciones aún más graves.

Finalmente, el campo social es uno de los más importantes dentro del propósito de este trabajo, ya que se busca un aporte a la concientización de la ciberseguridad en las organizaciones y la importancia de tener las herramientas de seguridad funcionando de la mejor manera para evitar todos los problemas que ya hemos mencionado sumado a las vulnerabilidades de la misma.

Teniendo en cuenta la socialización de los puntos acordados con el equipo de brechas de seguridad, así como con el Gerente del área, la importancia de tener al 98% de cobertura la herramienta de Antivirus es evidente. No solo porque es un requerimiento del Gerente del área sino también como un problema que puede llegar a convertirse en un hallazgo de auditoría interna dentro del Banco Popular.

La herramienta de Antivirus es una de las herramientas principales y a la vez la más completa en cuanto a la protección de equipos se refiere, no solo por la revisión y protección en segundo plano a los archivos de la maquina sino también a la protección de los trabajadores en la navegación web. Se establece un 98% de cobertura como normativa siguiendo los lineamientos de las directivas de seguridad del Banco, sin embargo, este porcentaje no se debe tomar como una meta final sino como la base para tener un sistema o equipo protegido. Es decir, el 98% dentro del Banco Popular no es motivo de subir la herramienta allí y dejarla sino de partir de ese porcentaje para alcanzar el 100% de cobertura en las herramientas.

De acuerdo a lo anterior se da a entender que la metodología creada no es solo para que las herramientas a las que se pueden aplicar suban al 98% sino que estas puedan seguir aumentando su índice de cobertura basado en un plan de mejora continua hasta poder alcanzar el 100%.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

- Especificar un método que ayude al Banco Popular a identificar y disminuir la brecha de seguridad en su software Antivirus a nivel nacional.

3.2 OBJETIVOS ESPECÍFICOS

- Definir el proceso con el cual se identifican las brechas de seguridad en el software antivirus para plantear posibles mejoras.
- Plantear un procedimiento para gestionar la brecha de seguridad, desde su identificación hasta su cierre total o parcial.
- Plantear un proceso de mejora continua para que la brecha de seguridad en el software de antivirus no se vuelva a reabrir.
- Aplicar el método Delphi para validar el cumplimiento de los objetivos anteriores.

4. ALCANCE

Al momento de definir el alcance de este trabajo, se tiene en cuenta lo siguiente: Por parte de los equipos que se van a tratar no se tendrán en cuenta servidores, máquinas virtuales o demás hardware que haga parte de la entidad y esté dentro del esquema de protección de las herramientas de seguridad, exceptuando computadores portátiles y computadores de escritorio (Laptops y Desktops).

Teniendo en cuenta las herramientas de seguridad de la entidad, además de las ya mencionadas anteriormente, se tiene un servicio de mesa de ayuda o soporte técnico que para este caso sería una empresa tercerizada como lo es IBM, esto puede variar dependiendo el área de la entidad donde se vaya a realizar una gestión, sin embargo es importante tener en cuenta que para el proceso de brechas de seguridad se va a establecer el equipo de soporte como un equipo de técnicos e ingenieros encargados de realizar la tarea de gestionar los tickets de mesa de ayuda que son creados por el equipo de brechas de seguridad del banco.

Teniendo en cuenta el último punto anterior, se llama "Equipo de brecha de seguridad" al grupo de trabajadores de la entidad que se encargan día a día a gestionar tickets a soporte técnico, identificar casuísticas a los problemas en las herramientas de seguridad, validar reportes de brechas de seguridad para identificar tendencias, entre otras labores que se mencionan más adelante. Este equipo está conformado para este caso por profesionales, administradores de las herramientas de seguridad, representantes de proveedores de las herramientas, el director del área, el gerente del área, equipo de mesa de ayuda y demás trabajadores que se vean implicados en apoyar las labores de brechas de seguridad.

Es importante mencionar que la mayor limitante dentro del presente escrito es el contrato de confidencialidad firmado en el momento de ingresar a la entidad bancaria, por lo que puede haber

información que se deba modificar con el fin de mantener la seguridad del banco y de su información.

METODOLOGÍA

5.1 TIPO DE INVESTIGACIÓN

Para este trabajo se va a realizar una investigación Aplicada, la cual se caracteriza por ser una investigación enfocada a la resolución de un problema. Para este caso, se quiere plantear una metodología que facilite la gestión de cierre de brechas de seguridad al Banco Popular. Por otra parte, se tendrá un enfoque Explicativo - Inductivo, es decir que el nivel de profundización se dará a partir de como los datos que ya se tienen en el banco (estadísticas, porcentajes y variables) se correlacionan de tal forma que se pueda estudiar el cambio de estos mismos teniendo en cuenta la metodología que se vaya a aplicar.

Por último, se recurrió a la investigación Cuasi-Experimental para efecto de realizar pruebas, ya que fueron ejecutadas de forma controlada sobre una muestra conocida (equipos con antivirus), al tiempo en que se observan cambios y se pudieron dar con observaciones que servirán para sacar conclusiones sobre la metodología que se esté aplicando en el momento.

5.4 FUENTES

5.4.1 FUENTES PRIMARIAS

- Informe del reporte de los equipos en las herramientas de seguridad del banco.
- Documentación disponible en internet del proveedor de Antivirus.
- Información suministrada por la ingeniera a cargo Paula Rubio y el equipo de brechas de seguridad.

- Documento de casuísticas encontradas en la brecha de seguridad anteriormente.
- Metodologías usadas antes de iniciar con la investigación.
- Recomendaciones por parte del Gerente del área Andrés Jácome acerca de la confidencialidad en los datos suministrados fuera del banco.

5.4.2 FUENTES SECUNDARIAS

- Documentación acerca de brechas de seguridad encontrada en internet.
- Documentación de Excel (Formulas, Tablas dinámicas, etc.).
- Conocimiento general sobre ciberseguridad.

5.5 INSTRUMENTOS DE CAPTURA, PROCESAMIENTO Y GENERACIÓN DE RESULTADOS

- Consolas de administración de cada una de las herramientas.
- Reporte de cruce de herramientas hecho en Excel.

5.6 PASOS METODOLÓGICOS

Los siguientes ítems trataran a detalle los pasos metodológicos para dar solución a cada uno de los objetivos específicos propuestos a partir del objetivo general y planteamiento del problema.

- **Objetivo Específico 1**
    - Consultar la metodología actual para encontrar las brechas de seguridad en el banco.

- Proponer un cambio al modelo de cruce de herramientas actual con el objetivo de que pueda ser más eficiente.
- Realizar pruebas con el modelo propuesto y analizar el comportamiento del porcentaje de la brecha de seguridad en antivirus.

- **Objetivo Específico 2**
  - Obtener un reporte detallado de la cantidad de equipos que reportan en el agente de Antivirus, así como el listado de equipos en brecha.
  - Establecer un método para encontrar casuísticas que permitan saber él porque los equipos entran a ser brecha de seguridad.
- **Objetivo Específico 3**
  - Establecer un plan de mejora continúa teniendo en cuenta el reporte de brechas de seguridad y aplicando el concepto del ciclo de Deming.
- **Objetivo Especifico 4**
  - Elaborar la encueta correspondiente al método Delphi.
  - Enviar la encuesta a los expertos.
  - Evaluar retroalimentaciones que ellos otorguen.

5.6 CRONOGRAMA DE ACTIVIDADES

Tabla 1. Cronograma de Actividades

Actividad	Fecha de Inicio	Fecha de Finalización
Actividad A Consultar la metodología actual para encontrar las brechas de seguridad y proponer un cambio de la misma a detalle.	02/08/2021	23/08/2021
Actividad B Realizar pruebas y toma de evidencias al modelo planteado.	24/08/2021	13/09/2021

Actividad C Establecer una metodología con el equipo de trabajo la cual ayude a encontrar casuísticas a los equipos que pasan a ser brecha de seguridad.	14/09/2021	27/09/2021
Actividad D Elaboración del registro completo de casuísticas encontradas con sus respectivas soluciones u observaciones.	28/09/2021	11/10/2021
Actividad E Establecer un plan de mejora continúa teniendo en cuenta el reporte de brechas de seguridad y aplicando el concepto del ciclo de Deming	04/10/2021	01/11/2021
Actividad F Elaboración del formato de anteproyecto para ser revisado por el tutor.	07/12/2021	21/01/2022
Actividad G Desarrollo completo del documento de Monografía teniendo en cuenta la validación el cumplimiento de los objetivos mediante el método Delphi.	24/01/2022	14/03/2022

Fuente: Autor

5.7 Diagrama de Gantt

Gráfico 1. Diagrama de Gantt

Fuente: Autor

PARTE II

Estado del Arte

Capítulo 2

Estado del Arte

En este apartado se tratan los conocimientos que se van a tener en cuenta para el desarrollo del trabajo, algo importante a mencionar es que a pesar de ser un proyecto donde la gran mayoría de fuentes de información provienen por parte del equipo de trabajo del Banco Popular, también se tendrá en cuenta Internet como un buscador de información de apoyo.

Inicialmente dentro de las investigaciones relacionadas, en el CRAI Universitario se encuentra una investigación referente a una estrategia metodológica para disminuir riesgos de fuga de información en el teletrabajo. [13] Este documento es de gran ayuda por el panorama actualizado que maneja ya que, si bien no es tema relacionado directamente con las brechas de Antivirus, se plantea una estrategia de mejoramiento en la seguridad de la información priorizando siempre la información más sensible, en nuestro caso la herramienta antivirus.

A su vez es importante conocer de la mano de compañías o entidades grandes como es el manejo de ellos ante un ataque de seguridad generado por una brecha. Para esto se tiene el caso del ataque de seguridad a T-Mobile donde el atacante logró robar información de más de 50 millones de personas [6]; El ataque a la NASA donde se robó información sobre los laboratorios jet de propulsión por medio de una brecha de seguridad, en este documento la NASA expone a detalle el ataque y a su vez la solución y recomendaciones para la problemática presentada. [15] Otro de los casos más grandes fue el de la Internet Society donde información personal de miles de personas quedo expuesta por culpa de una mala configuración de uno de los proveedores de sistemas de gestión. [7] Por otra parte, está el comunicado del Banco Pichincha [3] el cual es uno de los bancos más grandes de Ecuador y que en 2021 sufrió un ataque que genero el corte de todas sus operaciones tecnológicas con el fin de evitar la propagación del ataque y género que los usuarios deban usar únicamente las oficinas físicas para realizar sus gestiones hasta que se lograra solucionar el inconveniente de información. [3].

Por otro lado están las investigaciones que otorgan información de recomendaciones y planes de acción ante incidentes de brechas de seguridad, entre estos documentos

encontramos las guías que realiza la AEPD (Agencia Española Protección de Datos) las cuales retratan una serie de recomendaciones de cómo actuar ante brechas de seguridad de datos, si bien pasa lo mismo con el párrafo anterior, en estas recomendaciones se basan en la protección de datos personales, también hay información que puede ayudar a crear una estrategia de mejora de brechas de herramientas de seguridad. [1]; Según CSL [5] el hecho de informar sobre las brechas de seguridad puede ayudar a las compañías a contrarrestar en un 40% los daños que se pueden ocasionar, en este escrito se mencionan algunas recomendaciones para generar conciencia dentro de las compañías y en sus trabajadores y que estos aprendan a dar informes proactivos.

A su vez, se tiene en cuenta investigaciones que ayuden a entender de mejor manera el impacto que causan las herramientas antivirus en las organizaciones, tal como lo menciona [8] en esta era de la tecnología no se debe dejar de lado el uso de un buen software de antivirus capaz de no solo contrarrestar el malware sino también de los ataques por spyware, ransomware o adwares. A su vez [4] retrata un estudio donde se evidencia que el 25% de Pymes en Latinoamérica llegan a obviar el uso de un software o herramienta de antivirus, provocando así que el ataque a este tipo de empresas sea más fácil en ciertos casos.

Por último, se tendrá en cuenta la información suministrada por el fabricante de Antivirus dentro del banco, sin embargo, por motivos de contrato de confidencialidad con la empresa y luego de una deliberación con el equipo de brechas de seguridad del banco llevada a cabo al final de la pasantía, se omitirá el nombre de los fabricantes de las herramientas de seguridad.

Capítulo 3

Bases Conceptuales

En este capítulo se encuentra toda la información detallada referente a los conceptos que se van a trabajar a lo largo del documento

3. MARCO CONCEPTUAL

3.1 BRECHA DE SEGURIDAD

Se entiende como una brecha de seguridad a todo incidente que un atacante puede aprovechar para acceder o atacar la información protegida, se puede estar conscientes de la brecha de seguridad, así como también se puede desconocer la existencia de la misma.

Según el Reglamento General de Protección de Datos de España (RPGD) otorga una definición de brecha de seguridad, como un incidente que destruya, afecte la integridad, o pierda la información que se está administrando. (L.2021)

Lo anterior se puede ver directamente relacionado a la protección de la información teniendo en cuenta la triada de la ciberseguridad, la cual se basa en la confidencialidad, integridad y disponibilidad.

3.2 TRIADA DE LA CIBERSEGURIDAD CIA

La Confidencialidad, la Integridad y la Disponibilidad de la información son los tres pilares que conforman la triada de la ciberseguridad. OnTek [17] expone que esta triada básicamente es un modelo diseñado con el fin de servir de guía a la implementación de políticas de seguridad en las empresas.

Gráfico 2. Triada de la ciberseguridad CIA

Fuente: Autor

En la figura anterior se ve de mejor manera como es que estos tres pilares abrazan la seguridad de la información, esto ya que se deben tener siempre en cuenta para todo proceso, política o metodología que se requiera en una empresa y que se relacione con la seguridad.

3.2.1 Confidencialidad

La confidencialidad se basa en que los datos siempre se mantengan restringidos únicamente y que el acceso únicamente se de a las personas autorizadas. Siempre se verá que en las empresas existirá información más sensible que otra, y

gracias a esto se puede establecer estrategias de control de acceso para la protección para cada tipo de información.

Según OnTek [17] existen modelos que ayudan a garantizar la confidencialidad de la información, entre ellos están el cifrado de los datos, identificación de usuario y contraseña, autenticación de dos pasos, tokens y ya de forma más directa con el personal la verificación biométrica.

3.2.2 Integridad

La integridad se basa en garantizar que la información no sea modificada o alterada con en todo su ciclo de vida, esto va de la mano con la confidencialidad ya que parte del flujo de la información íntegra depende de que el acceso a la misma sea dado únicamente al personal autorizado en la organización.

Normalmente se usan herramientas de versionamiento que ayuden a que se tenga un control de las versiones de los datos, esto con el fin de comparar que la información transmitida en un inicio sea la misma información recibida.

3.2.3 Disponibilidad

Sin duda la disponibilidad de la información un algo que siempre se debe garantizar en una compañía no solo para los propios trabajadores sino también para los clientes. La disponibilidad se basa en que al momento de acceder a los datos estos se encuentren ahí cada vez que se requieran.

3.3 ANTIVIRUS

Según la gran compañía tecnológica Verizon [19] un antivirus es una herramienta de seguridad encargada de detectar, prevenir y eliminar cualquier tipo de software malicioso (Malware).

Estos softwares se caracterizan por ejecutarse en segundo plano y escanear constantemente la maquina en busca de malware ofreciendo con esto una protección contra software malicioso en tiempo real.

3.3.1 ¿Cómo Funciona?

Lo principal es comprender que es lo que escanea un antivirus en las maquinas. Según [19] Este tipo de softwares o herramientas de protección se encargan de validar datos de páginas web, descargas, archivos internos de la computadora y programas o softwares antes y después de ser instalados.

La forma en cómo se evalúan las amenazas es comparando los archivos o programas con una base de datos de diferentes tipos de malware o archivos potencialmente peligrosos, esta base de datos normalmente se está actualizando ya que todos los días se encuentran o se crean diferentes amenazas por parte de los hackers.

De acuerdo con el Instituto Nacional de Ciberseguridad de España INCIBE [11] existen varias formas en las que se detectan los malwares en la red para posteriormente actualizar la base de datos de antivirus. Dos principales y más usadas son Forma Reactiva y Forma Proactiva.

- **Reactiva**

Está encargado de identificar únicamente el Malware ya conocido.

Gráfico 3. Forma Reactiva

Fuente:https://www.incibe.es/sites/default/files/contenidos/blog/20190530_antivirus/firmas-heuristica.png

- **Proactiva o Heurístico**

  Está encargado de identificar malware desconocido mediante la búsqueda de archivos maliciosos ya conocidos.

Gráfico 4. Forma Proactiva

Fuente:https://www.incibe.es/sites/default/files/contenidos/blog/20190530_antivirus/firmas-heuristica_02.png

Cuando el antivirus encuentra una amenaza o se sospecha de un archivo que puede contener un posible archivo peligroso, este se enviará a cuarentena donde el

usuario después de ser notificado podrá decidir si el archivo debe ser eliminado por completo o si se debe a un falso positivo.

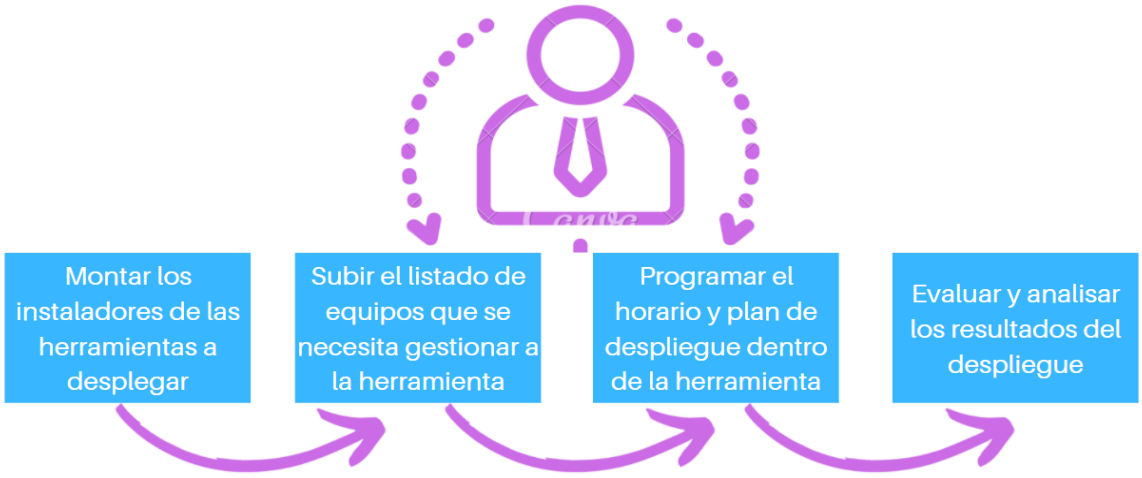
El proceso anterior es considerado el más básico y a su vez el más conocido, sin embargo, se puede ver que existen variaciones o automatizaciones cuando una organización implementa un antivirus en sus equipos. La creación de políticas e incluso los permisos de acceso del usuario de la maquina al software del antivirus es un ejemplo de restricciones o variaciones con respecto al uso de un antivirus en un hogar común a el uso que se le da en una compañía mediana o grande.

3.4 HERRAMIENTA CLIENT MANAGEMENT

Se trata de una de las herramientas de seguridad más importantes dentro de una organización en su gran mayoría medianas o grandes, esto ya que según DJCS (s. f.) el software se basa en una solución para automatizar y gestionar de mejor forma todos los procesos de TI mediante la conexión al dispositivo EndPoint.

Este tipo de software puede ofrecer una gran variedad de recursos para que el personal de IT tenga una mayor facilidad y control en la administración de los equipos de la compañía, sin embargo, el recurso de despliegue de agentes es sin duda el más importante de la herramienta siendo así el que posibilita enviar Sistemas operativos, versionamiento de programas, entre otro tipo de instaladores de manera fácil y rápida. (DJCS, s. f.)

Gráfico 5. Herramienta Client Management



Fuente: Autor

En el gráfico 5 se puede ver el modelo básico del sistema de despliegue de la herramienta Client Managment, empezando porque todo este proceso es realizado por un administrador de la herramienta el cual primero debe cerciorarse de contar con los instaladores de las herramientas que se van a usar y que estos sean compatibles dentro de la herramienta Client Managment, estos instaladores pueden ser sistemas operativos parchados con políticas de seguridad, versiones de los mismo, instaladores de herramientas de seguridad, software de aplicativos de la organización, versionamiento, entre otros, a su vez, no solo se puede enviar despliegues de instalación sino también de desinstalación desde que se cuente con el código script, así como también se pueden realizar reinicios de las máquinas en el caso de que sea requerido.

Después se tiene que exportar el listado de las máquinas que se van a gestionar, este listado normalmente es entregado al administrador de la herramienta por parte del

equipo de mesa de ayuda o de TI junto con las instrucciones exactas de que se debe hacer con dicho listo de máquinas.

Posteriormente, se debe programar la gestión a las máquinas, es decir, tomando el listado de máquinas se debe recurrir a las instrucciones entregadas por el cliente interno y luego se selecciona que tipo de gestión se va a realizar y en que horario, este último es muy importante ya que, dependiendo de la empresa, existen horarios de oficina donde las máquinas no se pueden intervenir sino hasta cuando el usuario que las use ya las tenga en stand by o que terminen su jornada laboral.

Finalmente se puede realizar una verificación del estado del gestionamiento de las máquinas al terminar, este reporte puede ser enviado a los clientes internos que solicitaron el despliegue y así puedan evaluar medidas según se requiera.

Capítulo 4
Marco Referencial

En el presente capítulo 4 se nombra a los diferentes aspectos normativos, estándares y entidades que rigen sobre la temática propuesta.

Es importante primero contextualizar que el banco popular es una de las entidades mas grandes a nivel nacional, establecida de acuerdo a la vigilancia de la Superintendencia financiera de Colombia y cuenta con gran cantidad de vigilancia interna por parte del mismo banco con el fin de cumplir a cabalidad los requerimientos para ofrecer a sus clientes la confiabilidad de sus activos inscritos.

Para este caso, el trabajo es desarrollado en una pasantía laboral mediante convenio con la Universidad Santo Tomas, se estableció al estudiante durante sus 6 meses de estadía en la Gerencia de Seguridad de la Información, la cual es la encargada de mantener la ciberseguridad del banco bajo los estándares y normativas vigentes, así como la que se encarga de realizar soporte, mantenimiento y capacitación a todo el personal sobre protección de sí mismos y de la red del banco a nivel nacional.

La pasantía fue bastante enriquecedora en cuanto a la posibilidad de aprendizaje sobre los temas de la seguridad de la información como de los equipos del banco, ya que al ser ubicado en el Área de Brechas de Seguridad, se pudo entender que hay más allá de los equipos que los clientes muchas veces solo llegan a ver al visitar una oficina física. El conocimiento sobre protección de los equipos por medio de distintos tipos de herramientas de seguridad se aprende mejor desde el punto de vista de un ingeniero el cual se encarga de velar por el buen funcionamiento de los equipos y a su ves proponer siempre planes de mejoras que puedan ayudar al Banco a mejorar en cada uno de sus procesos con un fin especifico. Esto es lo que la pasantía pudo entregar y se ve plasmado lo anterior en todo el desarrollo del trabajo.

4.1 NORMA ISO 27001

Esta norma internacional fue creada específicamente para implementar Sistemas de Gestión de Seguridad de la Información (SGSI). La cual otorga un reglamento explicito para proteger la información de cualquier empresa sin importar su tamaño.

Los beneficios que trae el hacer uso de esta norma al momento de implementar un SGSI dependen de la protección o prioridad que se le dé a la información más valiosa o confidencial. Según la guía de implementación de la norma suministrada por NQA [16] se mencionan tres principales beneficios:

- **Beneficio Comercial**

  Trata básicamente de que toda organización que cuente con un SGSI teniendo en cuenta los lineamientos de la norma 27001, provoca que la organización se vuelva mucho más competitiva en el mercado comercial y las diferencia contra otras empresas.

- **Beneficio Operacional**

  En materia del uso de la norma ISO 27001, se puede encontrar que esta misma se enfoca en que la empresa que la use pueda encontrar una tranquilidad de sus operaciones con respecto a la seguridad de su información. Si bien no siempre se podrá tener un 100% de seguridad, se busca que se disminuya en gran medida la aparición de incidentes.

- **Tranquilidad**

  Muy de la mano con los dos benéficos anteriores, la tranquilidad se convierte en un beneficio que la compaña puede aprovechar no solo para

aumentar si visibilidad en el mercado laboral sino también en la confianza de desarrollar mediante buenas prácticas un plan de seguridad de la información.

4.2 MÉTODO DELPHI

Este método se basa en la recolección de diferentes opiniones de expertos en el tema trabajado con el fin tener diferentes opiniones del tema en común y validar el cumplimiento del trabajo según la proyección que se tenía.

El grafico 6 proyecta el método Delphi de mejor forma:

Gráfico 6. Método Delphi

Fuente: https://www.cicerocomunicacion.es/metodo-delphi/ Año 2021.

PARTE III

Desarrollo de la Investigación

POLÍTICA DE CONFIDENCIALIDAD CON EL BANCO POPULAR

Dentro de las políticas firmadas con la compañía existen clausulas en las que el trabajador se compromete a no revelar información confidencial como por ejemplo, cifras o porcentajes exactos, datos financieros, datos personales de clientes y/o trabajadores y para el caso del área de ciberseguridad, nombres de los proveedores de las herramientas de seguridad, porcentajes o cifras exactas relacionadas a cobertura de las herramientas, proyectos confidenciales que supongan un riesgo para las negociaciones con nuevos socios, modelos de protección de los datos, infraestructura lógica y física que pueda poner el vulnerabilidad la compañía y finalmente compartir casos reales de brechas de seguridad las cuales estén o no remediadas.

De acuerdo a lo anterior, para el desarrollo del trabajo la información suministrada fue cambiada con respecto a la real, sin embargo, si se podrá presentar y realizar estimaciones y pruebas que den un resultado real y relevante a la solución de la problemática planteada al inicio del documento.

Capítulo 1

Estado Actual de la gestión de brechas de seguridad en Antivirus

En este primer capítulo se presenta el método actual usado por el Banco Popular para definir sus brechas de seguridad.

Al momento de ingresar a la gerencia de ciberseguridad lo primero fue resaltar la problemática que se estaba viviendo con respecto a las herramientas de seguridad, explícitamente con Antivirus y gracias a esto, junto al equipo de brechas liderado por la directora Carolina Castro se acordó que era necesario implementar una nueva metodología.

Como se mencionó en el planteamiento del problema, la entidad viene creando diariamente un reporte del cruce de herramientas con respecto al inventario total del banco, y es gracias a esto que se puede entender la situación actual de las herramientas de seguridad, en especial antivirus.

En la tabla 2 se puede ver el reporte de equipos en cada una de las herramientas de seguridad y al frente el inventario total de máquinas dentro del banco, se reserva la forma exacta de cómo se obtienen los valores por motivos de confidencialidad, pero básicamente se hace un conteo de todos los equipos dentro del banco, entiéndase “equipo” para este documento a todos los computadores (laptops o Desktops) dentro del banco. Para el caso mostrado en la tabla 2 se menciona un inventario de 5000 máquinas.

Posteriormente se exporta directamente de las consolas de cada una de las herramientas, la cantidad de equipos que están reportando actualmente, esta cantidad de equipos puede llegar a variar entre los días de la semana.

Finalmente se obtiene el porcentaje con respecto a la cantidad de equipos que están reportando en la herramienta entre el inventario total de máquinas dentro del banco.

Tabla 2. Reporte de herramientas

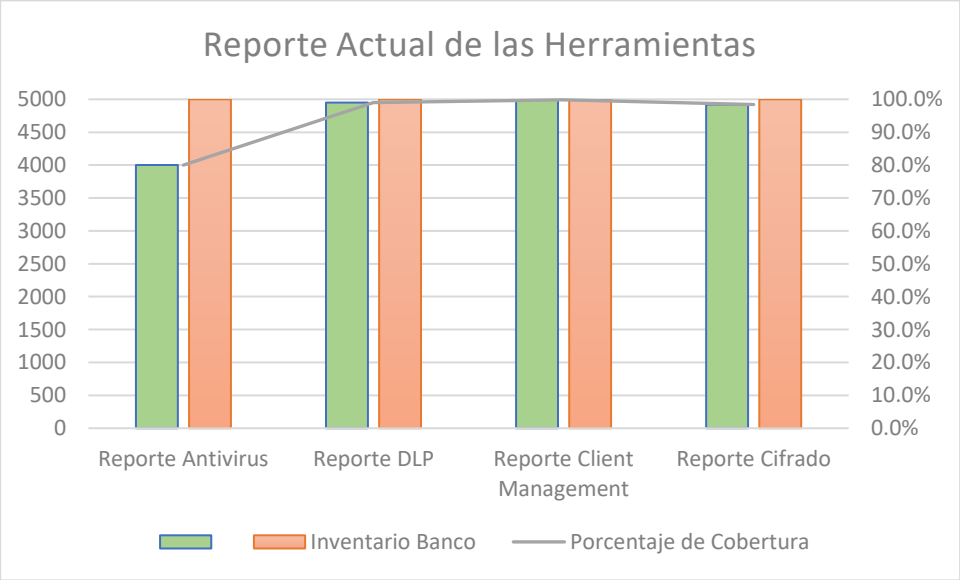
		Inventario Banco	Porcentaje de Cobertura
Reporte Antivirus	4250	5000	85,0%
Reporte DLP	4950	5000	99,0%
Reporte Client Management	4992	5000	99,8%
Reporte Cifrado	4920	5000	98,4%

Fuente: Autor

En el grafico 7 se puede evaluar de mejor manera la diferencia significativa que existe en el reporte de la herramienta Antivirus. En el se aprecian la cantidad de equipos en el banco (5000) vs cada uno de los reportes en cada una de las herramientas de seguridad.

Ej: Para el caso de Antivirus se tienen 4000 equipos reportando de los 5000 totales.

Gráfico 7. Reporte actual de las herramientas



Fuente: Autor

Luego de obtener estos resultados, junto al equipo de brechas de seguridad incluido el gerente del área Andrés Jácome, surgió la problemática sobre herramienta de Antivirus, es esta misma reunión se acordaron los siguientes puntos:

- Todo equipo dentro del banco debe contar con al menos la herramienta Antivirus.
- Todas las herramientas de seguridad deben contar con al menos 98% de cubrimiento con respecto al inventario total de máquinas.
- Los equipos con brecha de Antivirus pasarían a ser prioridad dentro del gestiona miento diario del equipo de brechas.
- Se entregarán avances semanales donde se pueda evidenciar la gestión realizada con la herramienta.
- Se debe establecer un modelo estratégico que permita identificar porque los equipos no reportan en la herramienta.
- Se deben buscar causas raíces repetitivas que, al ser solucionadas, puedan ofrecer una mejora significativa.

Algo importante a resaltar es que dentro del banco **Es una brecha de seguridad todo equipo que no reporte en los últimos 5 días**, esta norma fue puesta por equipo de brechas de seguridad anteriormente ya que se necesitaba tener una certeza de que equipos se deben priorizar para una intervención y cuáles no.

Capítulo 2

Acciones de Mejoramiento

En este capítulo correspondiente al desarrollo, se expondrán por medio de ejemplos, tablas y ecuaciones aquellos métodos empleados para desarrollar la propuesta. Teniendo en cuenta algunas recomendaciones propuestas en la norma ISO27001 y otras fuentes de información dentro del mismo Banco.

2.1 RECOMENDACIONES A TENER EN CUENTA DE ACUERDO A LA NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001.

Un modelo de gestión de mejora a un sistema de información referente a la ciberseguridad no puede ser establecido en una organización sin tener en cuenta la normativa ISO 27001. Por lo que fue bastante recomendable por parte del gerente y equipo de brechas aplicar ciertos puntos que faciliten al diseño de la propuesta, en este caso se tiene en cuenta el punto 6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES. (ICONTEC, 2013)

2.1.1 GENERALIDADES DE LA PROPUESTA

La compañía debe tener claro el conocimiento y las necesidades claramente establecidos con respecto a la solución que se quiere implementar, teniendo en cuenta las personas que van a trabajar en la propuesta y su rol en el aporte a la misma. (ICONTEC, 2013)

La compañía se debe asegurar que se cumplan los propósitos deseados, que el impacto se vea disminuido, que se elimine cualquier posibilidad de efectos secundarios o efectos indeseados que afecten directamente el funcionamiento del proceso ya establecido y que por su puesto exista un plan de mejora continua. (ICONTEC, 2013)

2.1.2 Valorar Los Riesgos De La Seguridad De La Información Dentro De La Propuesta.

La compañía al momento de evaluar la propuesta debe asegurarse de establecer bien qué criterios se usarán para dar por hecho una brecha de seguridad,

asegurarse que estas valoraciones generen resultados óptimos y válidos a la solución de la propuesta y finalmente identificar los riesgos de la información que se ven afectados al momento de dar solución y cuáles son los autores o coautores que dan pie al desarrollo de estos riesgos. (ICONTEC, 2013)

2.1.3 Tratamiento De Los Riesgos Encontrados

Según la norma (ICONTEC, 2013) al momento de crear un modelo de gestión de los riesgos que para este caso son la baja en los dispositivos con Antivirus, se debe tener en cuenta lo siguiente:

- Realizar una selección apropiada de opciones para tratar los riesgos.
- Determinar los controles necesarios para aplicar estas opciones.
- A toda opción se le debe justificar por qué se quiere implementar, así como justificar por qué se excluyen otras opciones.
- Se debe tener una aprobación de los dueños de los riesgos, para este caso el administrador de la herramienta. Así como también de los jefes encargados de remediar la brecha.

2.2 MÉTODO PARA IDENTIFICAR Y DISMINUIR LA BRECHA DE SEGURIDAD EN SU SOFTWARE ANTIVIRUS A NIVEL NACIONAL.

A continuación, se puede observar la construcción del método para identificar y disminuir la brecha de seguridad de Antivirus en el banco popular teniendo en cuenta el proceso actual que se realiza en el banco e implementando mejoras de acuerdo a las sesiones o reuniones con el equipo de brechas de seguridad.

2.2.1 Reporte de cruce de herramientas

Para entender a detalle cómo se obtienen las brechas de seguridad en el banco es importante primero explicar que es el Reporte de cruce de herramientas. Este reporte fabricado en Excel es una base de datos de todos los equipos del banco (laptops y desktops) a nivel Nacional, donde se detalla de cada uno los siguientes ítems o columnas:

- Hostname del equipo
- Estado del trabajador (Activo o Inactivo)
  - Activo = Está trabajando en el Banco
  - Inactivo = El trabajador ya no pertenece al Banco
- Nombre de usuario asignado al equipo
- Cédula del Usuario del equipo
- IPv4
- Ubicación del equipo (Edificio del Banco o Conectado por VPN)
- Tipo de equipo (Laptop o Desktop)
- Fecha del último reporte del equipo en cada una de las herramientas de seguridad
  - Antivirus
  - Data Lost Prevention
  - Client Managment
  - Proxy
  - VPN
  - Herramientas de Cifrado

A su vez se tiene un apartado en el documento donde por medio de tablas dinámicas se detalla cada una de las herramientas de seguridad. A continuación, se muestra un ejemplo de la tabla de seguridad de antivirus.

Antivirus	
Ultima fecha de reporte	Ultimos 5 día
Tipo	
Desktop	####
Laptop	####
TOTAL	####

Tabla 3. Antivirus *Fuente: Autor*

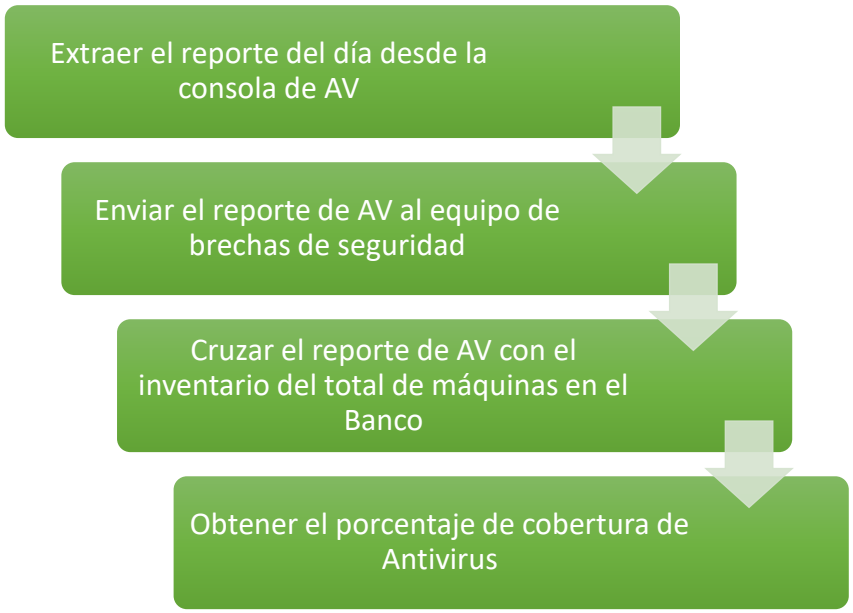
En la tabla 3 se puede ver el título o nombre de la herramienta de seguridad que se está detallando, en el recuadro de "Ultima fecha de reporte" se puede desplegar todas las fechas en las que se han reportado los equipos, allí únicamente se seleccionan los últimos 5 días ya que estos son los que se encuentran fuera de brecha de seguridad, posteriormente se encuentran el tipo de equipo y la cantidad de reportes para cada caso, esto teniendo en cuenta el listado de los últimos 5 días, finalmente se suman los equipos que hay dentro de los últimos 5 días y este sería el valor total de equipos cubiertos por antivirus en el banco.

2.2.2 Método Actual

Al momento de definir el proceso actual que se estaba usando por parte del Banco para definir las brechas de seguridad del software antivirus, se tuvieron en cuenta procesos que venían desde el administrador de la herramienta de seguridad, pasando por el equipo de brechas y posteriormente dando como resultado el reporte actual de la cobertura dentro del banco.

Inicialmente el proceso para identificar el porcentaje de cobertura de antivirus (AV) se desarrolla de la siguiente manera:

Gráfico 8. Método actual



Fuente: Autor

Como se puede evidenciar es un modelo bastante sencillo, sin embargo, es importante detallar el proceso de "Cruzar el reporte de AV con el del total de máquinas en el Banco" esto, ya que en este proceso es donde se realiza mayormente todo el cálculo de las variables que influyen al porcentaje que se tiene al final.

Teniendo en cuenta lo anterior, el proceso de detalla de la siguiente manera:

I. Se ingresa el reporte de Antivirus a la hoja de cálculo designada.

II. Se eliminan Hostnames duplicados

III. Se ingresan los Hostnames restantes al reporte de cruce de herramientas para que la demás información se autocomplete (Ver 3.3.1).

IV. Se obtiene la tabla dinámica con la información únicamente de la herramienta de antivirus.

V. Se extrae el total de equipos que reportan en antivirus los últimos 5 días.

VI. Se realiza la siguiente formula:

$$\frac{Total\ de\ equipos\ en\ AV}{Total\ Inventario\ (5000)} \times 100 = Porcentaje\ de\ cobertura\ AV\%$$

En el apartado de *Análisis del Estado Actual (Pag.29)* se puede ver el proceso con los datos que se tiene al momento en el Banco.

2.3 DEFINICIÓN Y MEJORAMIENTO DEL PROCESO CON EL CUAL SE IDENTIFICAN LAS BRECHAS DE SEGURIDAD EN EL SOFTWARE ANTIVIRUS.

Teniendo en cuenta el método anterior se realizó una reunión con el equipo de brechas de seguridad y allí se crearon las siguientes preguntas para tener en cuenta y poder desarrollar un plan de mejora con un lineamiento base:

- ¿Los trabajadores del Banco que se encuentran en vacaciones cuentan como brecha de seguridad?
- ¿Qué pasa con los equipos de los trabajadores que se van del Banco?

Teniendo en cuenta las preguntas anteriores se realizaron varios análisis junto a los trabajadores del equipo de brechas encargados de la fabricación del cruce de herramientas obteniendo los siguientes resultados.

- **¿Los trabajadores del Banco que se encuentran en vacaciones cuentan como brecha de seguridad?**

Se verificó que al momento de que un trabajador del banco se encuentra en vacaciones su computador ya sea portátil o desktop puede ser apagado o puede únicamente reportar en otras herramientas que no requieran una conexión o uso del equipo como antivirus, por lo que es normal que el reporte de dicho equipo desaparezca en el lapso de tiempo en el que el trabajador se encuentre fuera de labores.

Por lo anterior se decide que los trabajadores que se encuentren en vacaciones se excluyan del reporte del cruce de herramientas hasta que estos retornen a sus respectivas labores. Esto afecta no solo al total final de la herramienta antivirus sino también al inventario total de equipos en el banco.

De acuerdo a este orden de ideas, en el reporte del cruce de herramientas se agrega una columna más donde se especifique si el usuario se encuentra en vacaciones o no mediante un estado (True o False) siendo:

True = El usuario se encuentra en vacaciones.

False = El usuario se encuentra trabajando.

A su vez se toma como un filtro más en las tablas dinámicas de cada una de las herramientas teniendo lo siguiente:

Tabla 4. Tabla dinámica Antivirus

Antivirus	
Ultima fecha de reporte	Ultimos 5 días
Estado del Trabajador	False
Tipo	
Desktop	####
Laptop	####
TOTAL	####

Fuente: Autor

Al momento de realizar las pruebas de este cambio junto a la directora del área Carolina Castro, se evidencio un aumento bastante significativo del porcentaje de cobertura de antivirus en el banco. Esto se puede evidenciar a continuación:

Esta sería la situación sin efectuar ningún cambio:

Tabla 5. Reporte de AV antes de cambios

		Inventario Banco	Porcentaje de Cobertura
Reporte Antivirus	4250	5000	85,0%

Fuente: Autor

Por otra parte, se identifican 500 trabajadores en vacaciones por lo que se tiene lo siguiente:

Tabla 6. Reporte de AV sin trabajadores vacacionando

		Inventario Banco	Porcentaje de Cobertura
Reporte Antivirus	4250+50 = **4300**	5000-500 = **4500**	96%

Fuente: Autor

Según la tabla 6 se puede ver que efectivamente se eliminan los 500 trabajadores que están de vacaciones del inventario de equipos del banco. Sin embargo, como se menciona anteriormente, el hecho de que un trabajador este en vacaciones significa que no es una brecha de seguridad por lo que teniendo en cuenta la tabla 6 se ve que de los 500 trabajadores en vacaciones solo 50 se encontraban siendo brecha de seguridad en antivirus por lo que automáticamente dejarían de ser brecha y se sumarian al total de equipos de antivirus.

$$\frac{4300}{4500} \times 100 = 96\%$$

Teniendo así un aumento significativo de un 11% de cobertura de antivirus en el banco.

- **¿Qué pasa con los trabajadores que se van del banco?**

Dentro de este punto se debe tener en cuenta la importancia del Directorio Activo (DA) dentro del banco, recordando que es básicamente una base de datos donde se encuentran todos los trabajadores y allí es conectado cada uno de ellos con sus respectivos recursos de red para poder desempeñar sus labores.

Es por lo anterior que se puede deducir que si un trabajador pertenece al Directorio Activo es porque este se encuentra trabajando en el Banco, y en dado caso de que este abandone el banco ya sea por termino de contrato o por otro motivo. Este automáticamente debe ser retirado del directorio activo y con esto el ya no tendría acceso a la red interna de la compañía.

Es importante mencionar que, si un equipo reporta en el Directorio Activo, algunas herramientas podrán seguir viendo en sus bases de datos al equipo y este podría seguir reportando en las mismas en caso de que este equipo se encuentre en un almacén o en un puesto de trabajo sin ser utilizado. Ejemplo de esto, un trabajador X dejó la compañía, pero el equipo que tenía asignado en vez de ser automáticamente desconectado del directorio activo se deja en estado activo. Esto generará que habrá herramientas como por ejemplo DLP o Cifrado que seguirán conectadas al equipo generando reportes y es por esto que ese equipo se volvería una brecha de seguridad en las demás en herramientas, en este caso Antivirus. **Se**

debe recordar que, si un equipo reporta en al menos una herramienta, automáticamente debe reportar en las demás.

Teniendo en cuenta lo último, se realizaron investigaciones propias y junto al equipo de brechas de seguridad se pudo evidenciar que existían equipos aún en el Directorio Activo pertenecientes a trabajadores que ya había abandonado el banco. Las investigaciones se llevaron a cabo de la siguiente forma:

- Se toma el reporte de directorio activo y se exporta a Excel.
- Se añade el reporte al reporte de cruce de herramientas.
- Se agrega una columna en la que se pueda ver cuál es el estado de cada Hostname con respecto a Directorio Activo.
- Se compara la columna de *Estado del Trabador* con la nueva de *Directorio Activo*.

Finalmente se procedió a realizar las pruebas con el cambio realizado:

Tabla 7. Reporte de AV

		Inventario Banco	Porcentaje de Cobertura
Reporte Antivirus	4300	4500	96%

Fuente: Autor

Al momento de realizar la comparación de columnas se encontraron que 70 personas no se encontraban trabajando ya en el banco y que aun así seguían apareciendo en el Directorio Activo. Teniendo en cuenta esto, se observó que de estos 70 equipos que se eliminarían 5 reportaban aún en antivirus, teniendo lo siguiente:

Tabla 8. Reporte de AV sin equipos fuera de DA

		Inventario Banco	Porcentaje de Cobertura
Reporte Antivirus	4300-5 = **4295**	4500-70 = **4430**	97%

Fuente: Autor

De nuevo haciendo el cálculo con la fórmula anterior se tiene un aumento de un 1% al porcentaje de cobertura de Antivirus, teniendo casi que la brecha de antivirus en el porcentaje deseado como un mínimo por el banco (98%).

$$\frac{4295}{4430} \times 100 = 97\%$$

2.3 GESTIÓN DE BRECHAS DE SEGURIDAD EN ANTIVIRUS HASTA EL CIERRE TOTAL O PARCIAL.

Al momento de definir el proceso de gestiona miento de las brechas de seguridad, es importante primero relacionar el punto anterior (3.3.3).

Después de que se tiene el porcentaje de cobertura de cada una de las herramientas establecido, lo siguientes es validar que más se puede hacer para que este porcentaje suba usando una gestión u observación de las problemáticas que hacen que los equipos estén en brecha de seguridad.

La primera de estas se validó con el equipo de brechas donde se parte de la premisa de ¿Qué hacer para identificar los problemas que provocan que los equipos dejen de reportar en las consolas de las herramientas de seguridad? Y es gracias a esto que se trae a tema el uso de la herramienta de gestión como una de las herramientas primordiales al momento de querer gestionar las brechas de seguridad.

Como se había mencionado anteriormente en el documento, le herramienta de gestión o Client Management, es una herramienta en la que se puede desplegar

configuraciones de forma remota a gran cantidad de equipos al mismo tiempo y de forma organizada y programable.

Junto al equipo de brechas se decide entonces que es primordial hacer más uso de la herramienta ya que por el momento solo se usaba cuando se querían hacer reinicios o despliegues de scripts por parte del equipo de soporte técnico. La propuesta inicial fue tomar todos los equipos en brechas de seguridad sin importar la herramienta y desplegarla por medio del Client Management, sin embargo, se decidió que la priorización por el momento debe ser a la herramienta de Antivirus ya que es la que menos porcentaje de cobertura tiene.

2.3.1 Despliegues por medio del Client Management

De acuerdo con lo anterior, se creó una reunión con el administrador de la herramienta de antivirus con el fin de que este facilite los instaladores del agente y que puedan ser añadidos a la herramienta de Client Management para posteriormente iniciar con los despliegues a equipos afectados.

Luego de tener la herramienta de Client Management con los instaladores, se extrajo un listado de los Hostnames de los equipos que no estaban reportando en la herramienta antivirus, este listado es enviado a los encargados de la herramienta Client Management para que se les haga una reinstalación de los agentes por medio de un despliegue programado.

Al día siguiente estos fueron los resultados:

Tabla 9. Equipos enviados a despliegue

Equipos enviados a despliegue	
135	
Despliegue Correcto	**Despliegue Fallido**
97	38

Fuente: Autor

Como se evidencia, se enviaron los 135 equipos que no están aún dentro de la cobertura de AV, así mismo se tiene que de estos 135, tuvieron un despliegue correcto 97 equipos haciendo alusión a que el agente de antivirus quedó correctamente instalado. Por otra parte, fueron 38 equipos en los que el despliegue fue fallido, con esto, se entiende por despliegue fallido cuando la herramienta de Client Management no tuvo alcance al equipo ya sea porque el equipo se encontraba apagado o porque no estaba conectado a la red.

Por parte de los porcentajes, luego de que se hizo el despliegue de los agentes se solucionaron 60 equipos teniendo lo siguiente:

Tabla 10. Reporte de AV con agentes solucionados

		Inventario Banco	Porcentaje de Cobertura
Reporte Antivirus	4295+60 = **4355**	4430	98,3%

Fuente: Autor

Como se puede observar en la tabla 10, el porcentaje subió un 1,3% llegando así al porcentaje mínimo que se buscaba cubrir en el banco, sin embargo, es importante continuar con el proceso de gestión para seguir aumentando la cobertura de la herramienta Antivirus.

Un análisis que se puede sacar a partir de los resultados obtenidos es que varios agentes pueden desplegarse correctamente en los equipos, sin embargo, no significa que estos vuelvan a reportar en las consolas de administración, esto ya que pueden existir otras problemáticas con el equipo que provoquen que la reinstalación del agente no sea suficiente. Por otro lado, algunos agentes de antivirus pueden llegar a corromperse en los equipos del banco, normalmente pasa cuando no se actualizan seguido y estos llegan a dejar de responder en las consolas de administración, otro de los casos que pueden llegar a pasar es que por espacio en la máquina no se puedan descargar más actualizaciones del Antivirus y así este deje de funcionar.

Finalmente, con el equipo de brechas se decidió que **estos despliegues se hagan al menos tres veces a la semana** con el fin de que cada vez que un equipo se desconecte o desaparezca de la consola de administración, esta pueda subir de nuevo, con esto se tendrá una gestión constante y se evitarán brechas a futuro.

2.3.2 Gestión de equipos por medio de soporte técnico.

Como se mencionó anteriormente en el documento, el Banco cuenta con un equipo de soporte técnico tercerizado de la compañía IBM, este equipo es el encargado de recibir los tickets que escalan todas las áreas del banco que requieran una ayuda con respecto a sus equipos, servidores, etc.

Para este caso, junto al equipo de brechas de seguridad y el equipo de soporte técnico se estableció un acuerdo de integración a las brechas de seguridad, este acuerdo fue propuesto por el Gerente Andrés Jácome donde

básicamente lo que se busca es que se prioricen los casos de soporte donde se vean implicados equipos en brecha de seguridad.

La forma de escalar los casos se dan por medio de un software llamado Help Desk o Mesa de ayuda, allí se pueden crear tickets donde se exponga un problema o situación específica con un equipo u herramienta para que este sea gestionado o solucionado por el equipo de soporte técnico. Los casos normalmente tienen un numero único que los identifica tal como un ID propio.

Teniendo en cuenta todo lo anterior se decide continuar con la creación de los pasos para gestionar las brechas de seguridad. Así como en el punto anterior, se seguirá priorizando la herramienta de antivirus ya que lo que se busca es mejorar en la medida de lo posible su porcentaje de cobertura y ya luego se podrá impactar las demás herramientas.

Para iniciar la gestión con el equipo de soporte técnico, primero se estableció el cuándo se van a escalar caso a soporte técnico, esto con el fin de optimizar el proceso y no sobrecargar a los trabajadores de IBM con casos que se pueden solucionar de otras formas. Por lo que teniendo en cuenta esto, posteriormente a los tres días a la semana en los que se hacen despliegues por medio de la herramienta de Client Management y de acuerdo a los resultados de despliegue entregados. Se toman esos equipos los cuales fallaron en el despliegue de seguridad o que a pesar de que el despliegue salió satisfactorio no reportan aún en las consolas de administración y se escalan a soporte técnico mediante un ticket único para cada uno de los equipos.

Tabla 11. Resultados del despliegue de agentes

No reportan despues de despliegue	Despliegue Fallido
37	38
Equipos enviados a soporte = 75	

Fuente: Autor

Otro punto que se aclaró en la reunión de soporte con el equipo de brechas de seguridad, es sobre los resultados de los tickets, hay que recordar que el equipo de soporte está en la obligación de dar solución a los casos escalados, ya sea dando una solución parcial o no, todo debidamente documentado de tal forma que se demuestre que problema había y que solución se dio.

Después de este proceso de gestión con soporte técnico se tiene que de los 75 casos escalados se solucionaron 70 equipos por completo confirmando reporte de los equipos en las consolas de administración.

Tabla 12. Reporte de AV luego de gestión de soporte

		Inventario Banco	Porcentaje de Cobertura
Reporte Antivirus	4355+70 = **4425**	4430	99,9%

Fuente: Autor

Como se puede evidenciar en la tabla 12, se pudo lograr un porcentaje bastante óptimo de cobertura de antivirus teniendo en cuenta la gestión realizada por soporte técnico. A su vez de los 75 equipos que se pudieron solucionar por completo, solamente 5 no se pudieron gestionar correctamente, esto debido a

problemas de ubicación (Zonas donde por el momento por temas de pandemia no pueden acceder los técnicos o también que están retiradas de ciudades principales donde el acceso es complicado).

A pesar de que más adelante se hablarán sobre las recomendaciones, si es importante decir desde ahora que la priorización de una herramienta de seguridad es muy importante al momento de querer cerrar brechas de seguridad, así como también lo ideal es tener una muy buena comunicación con el equipo de soporte técnico para lograr un trabajo en equipo con los administradores de la herramienta afectada y se dé una solución adecuada.

2.3.3 Gestionamiento final de la brecha de seguridad en Antivirus.

Teniendo en cuenta los procesos anteriores ya se puede crear una serie de pasos para gestionar la brecha de seguridad de antivirus:

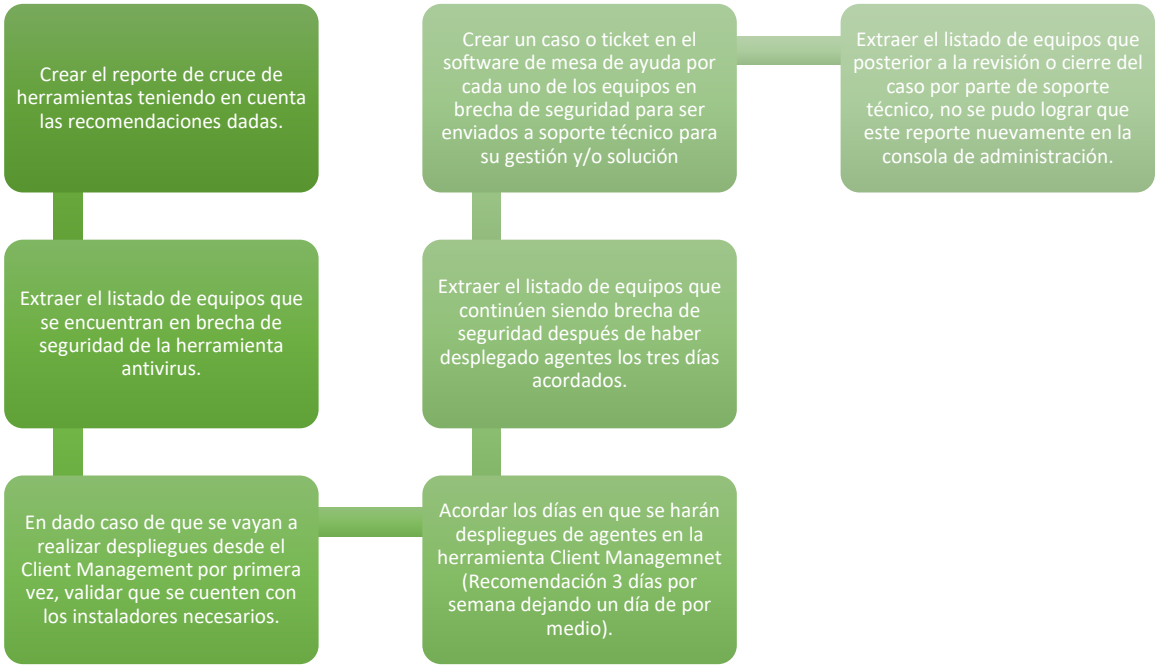
I. Crear el reporte de cruce de herramientas teniendo en cuenta las recomendaciones dadas.
II. Extraer el listado de equipos que se encuentran en brecha de seguridad de la herramienta antivirus.
III. En dado caso de que se vayan a realizar despliegues desde el Client Management por primera vez, validar que se cuenten con los instaladores necesarios.
IV. Acordar los días en que se harán despliegues de agentes en la herramienta Client Managemnet (Recomendación 3 días por semana dejando un día de por medio).

V. Extraer el listado de equipos que continúen siendo brecha de seguridad después de haber desplegado agentes los tres días acordados.

VI. Crear un caso o ticket en el software de mesa de ayuda por cada uno de los equipos en brecha de seguridad para ser enviados a soporte técnico para su gestión y/o solución.

VII. Extraer el listado de equipos que posterior a la revisión o cierre del caso por parte de soporte técnico, no se pudo lograr que este reporte nuevamente en la consola de administración.

Gráfico 9. Proceso para gestionar la brecha de seguridad



Fuente: Autor

2.4 PROCESO DE MEJORA CONTINUA PROPUESTO PARA QUE LA BRECHA DE SEGURIDAD EN EL SOFTWARE DE ANTIVIRUS NO SE VUELVA A REABRIR

Para el proceso de mejora se plantea inicialmente que la base de todo sea el reporte entregado por parte de soporte técnico con respecto a la gestión realizada a los equipos que se les escalaron. Todo esto ya que como se ha evidenciado a lo largo del documento todo es un proceso en conjunto para llegar a un método final. Teniendo en cuenta esto es importante mencionar primero que se compone este reporte entregado por soporte.

Dentro del análisis realizado con el equipo de brechas de seguridad del banco, se concretó que, para trabajar en un plan de mejora, el equipo de soporte técnico debía entregar lo siguiente:

- Número del caso asignado a cada equipo
- Hostname del equipo
- Tipo de equipo (Laptop o Desktop)
- Problema encontrado
- Diagnóstico o gestionamiento realizado
- Solución o respuesta al caso especificada

2.4.1 Documentación de casos encontrados.

Posterior a esto se revisan estos resultados y se evalúan mediante el uso de histogramas o graficas de tendencias con el fin de observar patrones que

ayuden a identificar la causa raíz a los problemas que hacen que los equipos dejen de reportar en las herramientas de seguridad, en este caso antivirus.

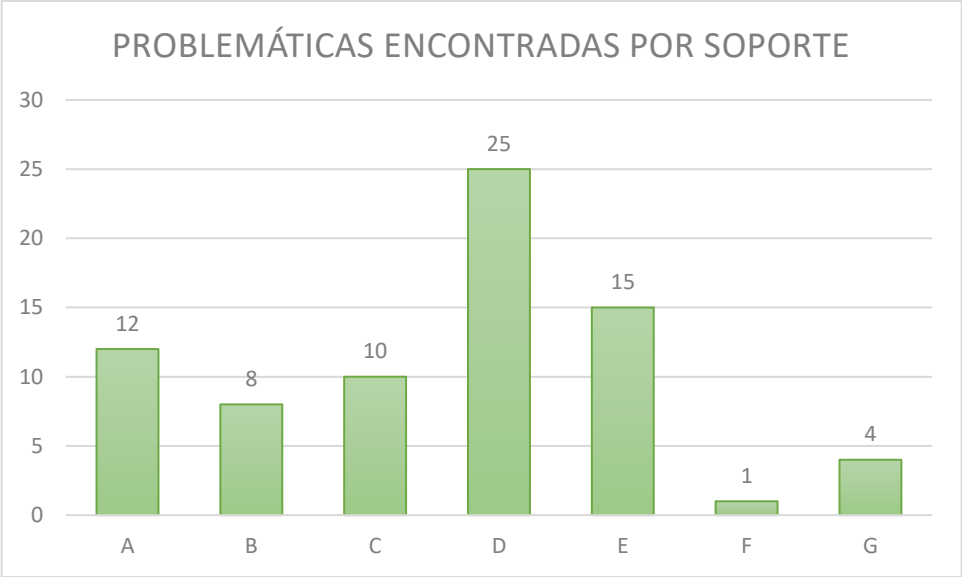
Un ejemplo de lo anterior es identificando dentro de los problemas encontrados por soporte técnico, cual de estos es el que más se repite o es más recurrente, con esto se busca una estrategia especifica que ayude a mitigar este problema desde la raíz y así se solucionarían la gran mayoría de los equipos. Por cuestiones de confidenciales no se puede tratar un caso real del Banco, sin embargo, se puede ejemplificar más a la práctica de la siguiente forma:

Suponiendo que se tenga el listado de los 75 equipos que se escalaron a soporte técnico, lo ideal es primero identificar y separar en grupos los problemas encontrados:

- Problemática A = 12
- Problemática B = 8
- Problemática C = 10
- Problemática D = 25
- Problemática E = 15
- Problemática F =1
- Problemática G = 4

Teniendo en cuenta esto se puede expresar las distintas problemáticas encontradas de la siguiente forma en un gráfico:

Gráfico 10. Problemáticas encontradas por soporte.



Fuente: Autor

De acuerdo con el grafico 10 se puede deducir que la problemática D es la que más se repite en los equipos que dejan de reportar en las consolas de administración de las herramientas y se convierten en brecha de seguridad. Con esto en mente se puede entrar a crear un plan de priorización de acuerdo a la cantidad de equipos encontrados por problemática, a su vez, ir documentando dichos problemas y soluciones para establecer un documento de ayuda que se pueda ir actualizando todo el tiempo y que sirva de glosario para problemas futuros.

2.4.2 Plan de mejora continua

La ISO 27001 se basa en modelo PHVA o ciclo de Deming no solo para llevar a cabo los sistemas de gestión de la información sino también como una herramienta para la

mejora continua de los mismos. Por lo que para este se puede partir teniendo en cuenta estos 6 pasos:

1) Identificar la mejora

   Esto hace alusión a que el equipo de brechas de seguridad debe buscar que es lo que el banco necesita para mejorar, que estrategias se pueden usar para optimizar aún más el método usado para gestionar las brechas de seguridad.

2) Definir qué es lo que se va a mejorar

   El equipo de brechas debe encontrar que variables son las que están implicadas en todo el proceso de brechas y cuales llegan a ser las más detonantes para medirlas y mejorarlas.

3) Obtener la mayor información posible del estado actual

   Todo el equipo debe de estar consciente de que es lo que se tiene y que a donde es donde se quiere llegar, esto implica conocer muy bien el proceso que se están realizando.

4) Analizar esta información

   Muy de la mano con el punto anterior, luego de conocer el estado actual es cuando ahora si se puede entrar a analizar que falencias existen y que variables no se están teniendo en cuenta para listarlas y así añadirlas al plan de mejora.

5) Profundizar la mejora con todos los equipos implicados en el proceso de brechas de seguridad.

   No solamente el equipo de brechas de seguridad debe ser el que se encargue de las mejoras al proceso de gestión, si bien son los encargados de velar por la disponibilidad de las herramientas de seguridad, también es importante que los

demás equipos implicados se integren a los planes de mejoras para así tener un panorama de opiniones más amplio y obtener un mayor número de soluciones.

6) Implementar esta mejora.

   Finalmente se implementa estas mejoras teniendo en cuenta siempre las prioridades y no solo ejecutándolas sino también evaluando el comportamiento del antes y el después a la implementación, para así tener un feedback del proceso y validar de mejor forma procesos futuros.

Gráfico 11. Plan de mejora continua.

Fuente: Autor

3. MÉTODO DELPHI

Para llevar a cabo todo lo que corresponde al método Delphi, de acuerdo a esto la propuesta es compartida con personas que conozcan del tema y puedan responder preguntas orientadas con base al desarrollo de la propuesta, y así poder obtener diferentes puntos de vista.

3.1 FORMULARIO SUMINISTRADO A LOS EXPERTOS.

Nombre: _____

Empresa: _____

Cargo: _____

Después de leer el documento responda las siguientes preguntas:

1era Pregunta:

¿Considera que el método propuesto aborda una oportunidad de mejoramiento apropiado y pertinente para el manejo de brechas de seguridad en el Banco?

R/_____

_____

_____

_____

_____

2da Pregunta:

¿Considera que los objetivos fueron cumplidos satisfactoriamente y a cabalidad?

R/_____

_____

_____

_____

_____

3ra Pregunta:

¿Considera que el desarrollo del método fue acorde a lo planteado inicialmente?

R_____

_____

_____

_____

_____

4ta Pregunta:

¿Considera que en un futuro esta propuesta podría servir de referencia a la hora de implementar un método de gestión de brechas de seguridad?

R_____

_____

_____

_____

Observaciones y/o comentarios adicionales:

R/_____

_____

_____

3.2 RESPUESTAS.

EXPERTO #1

Nombre: Paula Brillyt Rubio Rincón

Empresa: Banco Popular

Cargo: Profesional de Prevención de Ciberataques

EXPERTO #2

Nombre: Erika Pimentel

Empresa: InterLAN – Banco Popular

Cargo: Especialista de TI Nivel 1

Tabla 13. Respuesta de los expertos

Pregunta	Respuesta Experto #1	Respuesta Experto #2
¿Considera que el método propuesto aborda una oportunidad de mejoramiento apropiado y pertinente para el manejo de brechas de seguridad en el Banco?	Si, La propuesta cumple con la necesidad del Banco en cuanto a la búsqueda de un punto de partida para iniciar con un plan de mejora continua que nos ayude a que la brecha de seguridad sea cada día menor.	Claro que sí, el compañero desarrollo de manera cuidadosa un plan de mejora de la gestión que estábamos realizando en el banco, el aporte que entrego con este escrito a la entidad fue bastante valioso y vamos a seguir trabajando sobre este mismo para mejorar.
¿Considera que los objetivos fueron cumplidos	Si, La propuesta cumple con la necesidad del Banco en cuanto a la búsqueda de un punto de partida para iniciar con un plan de mejora	Si ya que, desde un punto de vista de resultados, fue gracias a este método planteado en el trabajo que la brecha de seguridad en los

satisfactoriamente y a cabalidad?	continua que nos ayude a que la brecha de seguridad sea cada día menor.	equipos con problemas de antivirus pudo solucionarse en su gran mayoría. Si bien hay aspectos que aún es bueno que en la entidad se sigan mejorando como por ejemplo el llevar a cabo el cruce de herramientas de una forma un poco más dinámica y rápida, creo que gran parte de la propuesta está acorde a lo planteado desde el inicio y a su vez va acorde a los recursos disponibles en el banco.
¿Considera que el desarrollo del método fue acorde a lo planteado inicialmente?	Si, si bien considero que hay procesos que se pueden mejorar aún más, el método que se plantea se desarrolla acorde a los tiempos de trabajo y al alcance que tiene el Banco Popular.	Claro que sí, desde el análisis que se realizó con el equipo de brechas de seguridad se pudieron desarrollar alternativas y soluciones que permitieron al Banco optimizar esa gestión a las brechas de seguridad, la documentación es bastante clara a pesar de que se tuvieron bastantes restricciones por el tema de la confidencialidad y aun así el escrito es bastante congruente con el trabajo que se desarrolla en el área.
¿Considera que en un futuro esta propuesta podría servir de referencia a la hora de implementar un método de gestión de brechas de seguridad?	Por supuesto, este método fue creado desde un inicio para suplir una necesidad del Banco por mejorar sus procesos en el tema de brechas de seguridad, sin embrago considero que el escrito está bastante abierto a la posibilidad de que otras entidades sean bancarias o no lo usen como una guía para aplicar conceptos de ciberseguridad, así como para obtener una seria de recomendaciones en caso de que estén usando un modelo de gestión y quieran recurrir a ideas de mejora continua.	Por supuesto, este método fue creado desde un inicio para suplir una necesidad del Banco por mejorar sus procesos en el tema de brechas de seguridad, sin embrago considero que el escrito está bastante abierto a la posibilidad de que otras entidades sean bancarias o no lo usen como una guía para aplicar conceptos de ciberseguridad, así como para obtener una seria de recomendaciones en caso de que estén usando un modelo de gestión y quieran recurrir a ideas de mejora continua.

Observaciones y/o comentarios adicionales:	Me gustó mucho como el pasante pudo expresar en el trabajo todo el proceso desarrollado en el banco teniendo en cuenta la política de confidencial firmada al momento de su contratación, esto da muestra de que esta propuesta puede ser aplicada a otras empresas.	El pasante en verdad entendió el propósito de la pasantía ya que lo importante no era únicamente cumplir con sus labores en el Banco sino también aprender mucho más sobre el mundo de la ciberseguridad y empezar a aplicar estos conceptos.

3.3 ANÁLISIS DE LAS RESPUESTAS.

Después de analizar cada una de las retroalimentaciones de las dos expertas, se puede deducir que el escrito es calificado de manera satisfactoria ya que el desarrollo del método se expresó de manera clara teniendo en cuenta las limitaciones del Banco. Sin embargo, como menciona la Ingeniera Paula Rubio, la propuesta puede contener ciertos conceptos que son usados únicamente por el Banco Popular, por lo que la pregunta de que si este escrito puede llegar a ayudar a otras empresas puede llegar a depender en gran medida de que tanto se asemejen los recursos de soporte técnico entre la empresa que quiere aplicar el método al Banco Popular.

PARTE IV

Conclusiones y Recomendaciones

CONCLUSIONES

Luego del desarrollo del documento se pudo evidenciar que efectivamente el porcentaje de cobertura del software o herramienta de antivirus aumentó desde su 85% inicial hasta un 99,9% superando así la meta del 98% que se había propuesto desde un inicio. Con lo anterior se puede evidenciar que, si bien la gestión que se estaba realizando en el banco no era mala, si se pudo mejorar llevando a cabo distintas soluciones propuestas tanto por el equipo de brechas de seguridad como otras áreas que se involucran día a día en esta gestión.

Con lo anterior se puede concluir que un proceso de identificación de brechas de seguridad correcto, puede ayudar a mejorar en gran medida el gestionamiento de las mismas, esto se ve demostrado en el aumento de un 85% de cobertura de antivirus a un 97% tan solo por indagar un poco más en la información que se tenía en cuenta al momento de realizar el cruce de la misma. A su vez con esto se puede tener certeza de la necesidad de que el equipo encargado de brechas de seguridad se reúna más seguido para proponer y analizar nuevas iniciativas o ideas que ayuden a mejorar los procesos que se realizan en el momento.

Por su parte la gestión de las brechas de antivirus no se podía llevar al cabo del todo sin la colaboración de las áreas como despliegue de agentes por medio de Client Management y el área de soporte técnico o Help Desk, esto da a resaltar la unión que tiene el banco con las distintas áreas implicadas y demuestra la importancia para otras compañías de adoptar planes de mejoras en las que incluyan distintas áreas en las reuniones de planeación. Fue gracias a este trabajo en conjunto que el porcentaje de cobertura de antivirus logró subir de un 97% a un 99,9% sobrepasando la propuesta inicial de un 85%. A su vez, se puede concluir que el método lineal de pasar del área de despliegues al área de soporte genera que los equipos con problemas tengan una mayor revisión.

Gracias a la buena gestión de los equipos tanto por el equipo de brechas de seguridad, pasando por el área de despliegues de agentes y finalizando en el equipo de soporte técnico, se pudo crear un documento en el cual se especifiquen los problemas más comunes, así como los problemas específicos de cada equipo y con esto se mejoran los tiempos en los que un equipo es reportado como brecha de seguridad, hasta su respectiva solución.

RECOMENDACIONES

Si bien el tener un glosario donde se puedan solucionar los problemas más recurrentes es una estrategia bastante buena para disminuir tiempos a la gestión de solución de equipos en brecha, así como para alivianar la carga del equipo de soporte técnico. Lo más importante es siempre identificar las causas raíces de los problemas, dentro del análisis hecho a las problémicas encontradas en el banco existe algo denominado factor humano, el cual hace referencia a la influencia del ser humano en los errores que aparecen en los equipos.

Para este caso en concreto, se evidencia que muchos problemas pueden llegar a provocarse por el desconocimiento de los trabajadores hacia el uso de sus equipos, un ejemplo de esto es que desconozcan que estos necesitan de un cierto espacio en disco para que las herramientas de seguridad se puedan actualizar, que deben tener sus equipos encendidos al momento de que se realicen despliegues de agentes por medio de Client Managment o que error más común en el que no reinician sus equipos periódicamente sino que solo se dejan en estado de suspensión provocando que estos nunca actualicen sus políticas de seguridad en caso de que estas necesiten de un reinicio de la máquina.

Todos estos factores anteriores generan que ciertas problemáticas empiecen a surgir y provoquen que el funcionamiento tanto del equipo como de sus herramientas de seguridad no sea el óptimo por lo que la propuesta del equipo de brechas de seguridad parte de la base de una necesidad de

capacitar más allá a los trabajadores sobre los procesos que existen más allá de la labor que ellos realizan día a día y que así estos sean conscientes de las labores que se realizan desde el área de Ciberseguridad para proteger la información del banco y la de sus trabajadores.

Referencias Electrónicas

[1] AEPD. (2021, junio). *Guía para la notificación de brechas de datos personales*. https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

[2] Agencia Española Proteccion de Datos. (2019, 18 septiembre). *Brechas de seguridad de datos personales: qué son y cómo actuar*. AEPD. https://www.aepd.es/es/prensa-y-comunicacion/blog/brechas-de-seguridad-de-datos-personales-que-son-y-como-actuar

[3] Banco Pichincha. (2021, 11 octubre). *Banco Pichincha on* [Tweet]. Twitter. https://twitter.com/BancoPichincha/status/1447628963858296834?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1447628963858296834%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.elcomercio.com%2Factualidad%2Fnegocios%2Fbanco-pichincha-ciberseguridad-ciberataque-hackeo.html

[4] CSL. (2018, 26 agosto). *El 25% de las PyMEs de Latinoamérica no cuentan con solución antivirus*. Ciberseguridad LATAM. https://www.ciberseguridadlatam.com/2018/08/27/el-25-de-las-pymes-de-latinoamerica-no-cuentan-con-solucion-antivirus/

[5] CSL. (2021a, marzo 1). *Informar de manera proactiva sobre brechas de seguridad reduce los daños para empresas en un 40%*. Ciberseguridad LATAM. https://www.ciberseguridadlatam.com/2021/03/02/informar-de-manera-proactiva-sobre-brechas-de-seguridad-reduce-los-danos-para-empresas-en-un-40/

[6] CSL. (2021b, agosto 21). *La brecha de T-Mobile se eleva a más de 50 millones de personas*. Ciberseguridad LATAM. https://www.ciberseguridadlatam.com/2021/08/23/la-brecha-de-t-mobile-se-eleva-a-mas-de-50-millones-de-personas/

[7] CSL. (2022, 18 febrero). *Una configuración errónea de un tercero, expuso los datos de Internet Society a la red*. Ciberseguridad LATAM. https://www.ciberseguridadlatam.com/2022/02/21/una-configuracion-erronea-de-un-tercero-expuso-los-datos-de-internet-society-a-la-red/

[8] CSL - The Hackers News. (2021, 26 noviembre). *Si no estás usando un software antivirus, no estás prestando atención*. Ciberseguridad LATAM. https://www.ciberseguridadlatam.com/2021/11/29/si-no-estas-usando-un-software-antivirus-no-estas-prestando-atencion/

[9] DJCS. (s. f.). *BMC Client Management*. https://www.djcs.com.ve/gestion-de-servicios-y-soporte/bmc-client-management

[10] ICONTEC. (2013). *NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001*. https://www.academia.edu/40913480/NORMA_T%C3%89CNICA_NTC_ISO_IEC_COLOMBIANA_27001_TECNOLOG%C3%8DA_DE_LA_INFORMACI%C3%93N_T%C3%89CNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTI%C3%93N_DE_LA_SEGURIDAD_DE_LA_INFORMACI%C3%93N_REQUISITOS

[11] INCIBE. (2022, 18 enero). *¿Qué hace un antivirus para detectar el malware?* https://www.incibe.es/protege-tu-empresa/blog/hace-antivirus-detectar-el-malware

[12] L. (2021a, diciembre 23). *Brechas de seguridad: Qué son y cómo gestionarlas*. Grupo Atico34. https://protecciondatos-lopd.com/empresas/notificar-brechas-seguridad/

[13] L.I.V.A.N.F.S.G. (2021b, septiembre). *Estrategia metodológica para minimizar riesgos de fuga de información empresarial en teletrabajo*. CRAI USTA. http://hdl.handle.net/11634/37639

[14] MinCiencias. (2021, febrero). *PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*. Ministerio de Ciencias Colombia.

https://minciencias.gov.co/sites/default/files/ckeditor_files/D103PR03%20Gesti%C3%B3n%20de%20Incidente%20de%20seguridad%20de%20la%20Informaci%C3%B3n%20V01.pdf

[15] NASA. (2019, junio). *CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY* (IG-19-022). Office of Inspector General. https://oig.nasa.gov/docs/IG-19-022.pdf

[16] NQA. (2020). *ISO 27001:2013 GUÍA DE IMPLANTACIÓN*. nqa. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

[17] OnTek. (2021, 29 agosto). *Tríada CID (Confidencialidad, Integridad y Disponibilidad)*. https://www.ontek.net/que-es-triada-cid/

[18] *Qué es un antivirus - Definición, significado y explicación*. (s. f.). Verizon Fios. https://espanol.verizon.com/info/definitions/antivirus/

[19] Verizon. (s. f.). *Qué es un antivirus - Definición, significado y explicación*. Verizon Fios. https://espanol.verizon.com/info/definitions/antivirus/