DISEÑO MANUAL AUTODIAGNÓSTICO SEGURIDAD DE LA INFORMACIÓN: NOTARÍAS DE BOGOTÁ.

Juan Carlos Villamil Rojas

Director del trabajo de grado:

Olmer Garcia
co-asesor Giovanny Ortegon

Universidad de Bogota Jorge Tadeo Lozano
Facultad de Ciencias Naturales e Ingeniería
Ingeniería de sistemas

Bogota, D.C.
2021

UTADEO
UNIVERSIDAD DE BOGOTÁ JORGE TADEO LOZANO

Tabla de Contenidos

Índice de tablas

Índice de Gráficos

1 TÍTULO

DISEÑO MANUAL AUTODIAGNÓSTICO SEGURIDAD DE LA INFORMACIÓN: NOTARÍAS DE BOGOTÁ.

SELF-DIAGNOSTIC MANUAL DESIGN INFORMATION SECURITY: NOTARIES OF BOGOTÁ.

2 AUTORES

Nombres	**Juan Carlos Villamil Rojas**
Formación académica	**Estudiante Ingeniería de sistemas**
Institución	**Universidad de Bogota Jorge tadeo Lozano**
Correo Electrónico	**juanc.villamilr@utadeo.edu.co**

Tabla 1. Autor del proyecto.

3 RESUMEN

Desde que nace el individuo hasta que fallece necesita de las notarías, comenzado con el registro civil de nacimiento pronto da a luz, cuando llega a la pubertad autenticación de títulos, en la adultez generación de sus escrituras, en el estertor de su vida y posterior partida de este mundo, su registro de defunción; los notarios del círculo de bogotá son funcionarios públicos, pero sus empleados, infraestructura, tecnologías responden a las lógicas del mercado privado, generando una asimetría en el servicio a partir de tecnologías implementadas, sin embargo los sistemas Notariales deben ser seguros, garantizando la legalidad y legitimidad.

Teniendo en cuenta que se incrementaron los delitos informáticos en las notarías atacando directamente su sistema interno, hurto en portales de pago, robo de información, daño de servidores, intentos de hacking a la red de las notarías y modificación de documentos públicos, esto auspiciado por el desconocimiento del procedimiento para auto-diagnosticar las notarías en cuanto a tecnologías de la información para poder corregir la brecha digital de seguridad, por esto el trabajo actual se considera necesario para el sector notarial bogotano.

Utilizando la metodología inductiva de autodiagnóstico propuesta por el mintic, partiendo de la exploración previa a partir del levantamiento de información y estado del arte del sector notarial, para entender sus particularidades, siguiendo con el análisis con base en escenarios reales dentro de tres notarías del círculo de bogotá y matriz de riesgo, por

último desarrollamos un manual de seguridad informática, para generar ambientes más seguro, mitigando la opción de ataques por parte de ciberdelincuentes o fallos inherentes a la gestión del área de sistemas, la lógica del presente trabajo se basa en escenarios reales que afronte en auditorías de la superintendencia de notariado y registro sumados a fallos de los sistemas notariales que hice frente durante los último meses.

palabras clave: Seguridad, mintic, notarías, tecnologías, riesgo.

4 ABSTRACT

From the moment the individual is born until he dies he needs the notaries, begun with the civil registry of birth soon gives birth, when he reaches puberty authentication of titles, in the adulthood generation of his writings, in the rattle of his life and subsequent departure from this world, his death record; the notaries of the circle of Bogotá are public officials, but their employees, infrastructure, technologies respond to the logics of the private market, generating an asymmetry in the service from implemented technologies, however the Notarial systems must be secure, guaranteeing legality and legitimacy.

Taking into account that computer crimes increased in notaries directly attacking their internal system, theft in payment portals, theft of information, damage to servers, attempts to hack the network of notaries and modification of public documents, this sponsored by the ignorance of the procedure to self-diagnose notaries in terms of information technologies in order to correct the digital security divide, for this reason, the current work is considered necessary for the Bogota notarial sector.

Using the inductive methodology of self-diagnosis proposed by the mintic, starting from the previous exploration from the collection of information and state of the art of the notarial sector, to understand its particularities, continuing with the analysis based on real scenarios within three notaries of the circle of bogotá and risk matrix, finally we developed a computer security manual, to generate safer environments, mitigating the option of attacks by cybercriminals or failures inherent in the management of the systems area, the logic of this work is based on real scenarios that I face in audits of the superintendence of notaries and registration added to failures of the notarial systems that I faced during the last months.

keywords: Security, mintic, notaries, technologies, risk.

5 INTRODUCCIÓN

La seguridad informática es parte fundamental de la sociedad, igualmente las nuevas lógicas de digitalización estatal que enmarcan los servicios notariales como servicios que se deben empezar a hacer desde internet (Super Notariado, 2021), esta digitalización de los procesos, acelerada por el covid-19, las notarías cerraron de un momento a otro sin previo aviso, sin tener la posibilidad de prepararse al nuevo escenario tecnológico, además la contracción económica en el país generó una falta de recursos para las correctas implementaciones de tecnología de borde para asegurar los servicios notariales.

Ya en el país hay una ruta de digitalización nacional a través del estado desde hace casi 10 años (Mintic, 2010,) y por medio de operadores tecnológicos (Super Notariado, 2021), que son empresa que se encargan de prestar servicios a las notarías, en el mundo el avance en estado unidos y europa es abismal, donde completamente los servicios notariales llevan años prestando de forma virtual ahondando desde la seguridad (Amann, 2012).

Sin embargo el escenario es nuevo para las notarías de bogotá, dada su naturaleza independiente ellos mismos deben procurar las mejores prácticas informáticas, pero estas recaen en un abismo, dado que hay lógicas de gestión en seguridad informática como la iso 27001 que atañe a las entidades privadas (Icontec, 2006), o la NTC GP 1000 que implica directamente a las instituciones públicas, en este orden la jurisprudencia desobliga a las notarías de un marco tecnológico de implementación, ocasionando que las guías y anexos técnicos implementan u orientan a los operadores tecnológicos (empresas que implementan un servicio a los procesos notariales), pero en si las notarias no conocen cómo realizar un diagnóstico de su seguridad, este auto-diagnóstico es la base de una posterior reparación de fallos o posibles brechas de seguridad (super notariado, 2021).

Entrevistando a varios notarios exponen la misma lógica; no se tiene una visión clara de cuál sería el proceso para comenzar a diagnosticar la seguridad de la información dentro de la notaría, además sin tener esta información clara directamente por el señor notario o notaría, sería imposible robustecer los procesos notariales.

Por tal razón el presente trabajo presente dilucidar,cómo realizar un diseño de manual de autodiagnóstico de seguridad de la información para las notarías de Bogotá, a partir del levantamiento de información revisión del estado del arte del sector notarial donde entendamos las particularidades de este sector, además realizar matriz de riesgos y análisis de casos reales en tres notarías en el círculo de Bogotá, para con la información obtenida diseñar un manual basado en hechos reales de ciberseguridad y los datos obtenidos de los puntos anteriores que se ajuste a la realidad notarial del país, más específicamente de las notarías del círculo de bogotá, todo esto apoyado de la metodología del mintic y su guía para desarrollo tecnológico para el país (Mintic, 2010).

6 METODOLOGÍA

la metodología inductiva de autodiagnóstico propuesta por el mintic, partiendo hechos particulares de tres notaría, hasta llegar a la generalidad del manual de autodiagnóstico seguridad de la información,

6.0.1 Exploración previa a partir del levantamiento de información y estado del arte del sector notarial para entender las particularidades del sector notarial.

Durante esta etapa, se recopila y clasifica la información tecnológica, unido a la data obtenida por medio de la experiencia ganada por la praxis, concerniente a las notarías del círculo de Bogotá.

6.0.3 Análisis con base en escenarios reales dentro de tres notarías del círculo de Bogotá y matriz de riesgo.

Con los datos recopilados, la matriz de riesgos cuantificando y evaluando el riesgo, se analizaron los posibles escenarios de fortaleza y debilidad, que enfrentan las notarías del círculo de Bogotá en el ámbito tecnológico, además se analizaron 6 escenarios reales dados en tres notarías de Bogotá.

6.0.4 Diseño propuesta del manual de seguridad informática :

Se hallaran un conjunto de estamentos comunes entre el sector notarial, dichos estamentos se utilizaran para la realización del manual de autodiagnóstico de seguridad de la información, para las notarías del círculo de bogotá.

6.1 Planteamiento del Problema.

las notarías fueron creadas con el decreto 2148 de 1983, cada notario es nombrado en propiedad hasta su edad de jubilación, donde debe ceder la notaría al nuevo notario escogido, generalmente venden los equipos, muebles, enseres, software a los nuevos notarios, esto genera que la notaría conserva el total de la infraestructura tecnológica de notario a notario, su personal interno no tiene la formación para brindar la ciberseguridad necesaria dentro de las instalaciones,utilizan software sin licencia y toda su seguridad informática se centra en plataformas de terceros, recordando que las notarías tienen un sistema interno del cual acceden a las plataformas de los terceros y este sistema interno es el que está más desprotegido y de dónde se cometen la mayor cantidad de ataques informáticos, al igual el desconocimiento del quehacer de la seguridad informática donde se tenga una guia de como auto diagnosticar la notaría en su estructura interna genera los escenarios desprovistos de blindaje informático (Super Notariado, 2021,).

6.1.1 Problema central

En base en estos puntos el problema central es el siguiente:

¿Cómo se puede blindar a las notarías y robustecer los sistemas a tal nivel que mitigue los ciberataques y los fallos de las tecnologías?

6.1.2 Problemas secundarios.

Presenta los siguientes problemas secundarios:

La notaría no tiene un plan de contingencia ante cualquier eventualidad tecnológica.

Las notarías han recibido varios ataques informáticos, no cuenta con un plan de ejecución y solo ha tomado medidas reactivas de último minuto.

Los servidores de la notaría están desprovistos de seguridad perimetral.

La notaría ha sufrido varias averías tecnológicas que han dejado sin servicio tecnológico por varias horas.

El personal interno no cuenta con la formación necesaria para evaluar internamente la notaría en el ámbito de la ciberseguridad.

No se cuenta con una guía para realizar un autodiagnóstico ni con documentación inicial.

6.2 Objetivos

6..2.1 objetivo general

Diseñar un manual de autodiagnóstico para las notarías del círculo de Bogotá, con aras de mejorar la gestión-seguridad, dentro y fuera de las instalaciones.

6.2.2 objetivos específicos

- ➔ Generar matriz de riesgos con base en una muestra de 3 notarías del círculo de Bogotá, de la localidad de Chapinero, a partir del estudio de casos reales de fallas de sistemas dentro de las notarías.

- ➔ Diseñar un manual de seguridad informática, teniendo en cuenta las particularidades del servicio notarial.

- ➔ Aplicar los conocimientos adquiridos en la universidad, para diseñar un manual de seguridad informática , con las mejores prácticas, y los conocimientos adquiridos en la etapa laboral junto con los lineamientos legales y procedimentales de la superintendencia de notariado y el Mintic.

6.3 justificación

La norma ISO 27001 nos provee un marco para para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI), está adopción nos provee una posición estratégica en ciberseguridad dentro de la organización, está diseñado para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información, las Notarías como instituciones encargadas de la fe pública de la Nación gozan de una necesidad intrínseca en la planeación y ejecución de un (sgsi) a la medida, al igual nos basamos en las normas que regulan las notarias y los lineamientos dados por el ministerio de telecomunicaciones (Icontec, 2006).

La planeación y posterior adopción del manual de autodiagnóstico de seguridad de la información para las las notarías del círculo de bogotá, generará un escenario más sano, fiable y confiable para las transacciones digitales que se realicen dentro de su organización y servirá de garante para los procesos de cara al cliente.

6.3.1 justificación económica

Generalmente el proceso manual, genera reprocesos, la falta de una política clara de ciberseguridad plantea un escenario de pérdida económica, dado que cada activo de información es valioso para la organización, la inactividad producida por un fallo en la infraestructura tecnológica ocasiona pérdidas millonarias para la notaría, el tener el control de sus sistemas informáticos minimiza las pérdidas económicas y maximiza el roi, sin embargo todo esto se origina a partir del autodiagnóstico de la organización (Mintic, 2016).

6.3.2 justificación social

La impermeabilización de un manual de autodiagnóstico de seguridad de la información para las las notarías del círculo de bogotá, contrae varios beneficios para la organización, minimizando posible fraude procesal en la fe pública que dan los notarios, asegurando la exactitud de sus procesos que pueden afectar directamente a la nación (mintic, 2016, #).

6.3.3 Justificación Tecnológica

El presente trabajo pretende brindar las herramientas para tener un control del riesgo y generar un autodiagnóstico dentro de cada notaría, contribuyendo de manera acertada a mejorar los procesos dentro de las notarías en Bogotá (mintic, 2016)á.

6.4 Alcance y límites

6.4.1 Alcance

Realizar la documentación y proceso de los siguientes ítems:

1. Entender la lógica notarial a partir de la contextualización con el estado del arte.

2. Realización de matriz de riesgo, y un análisis real por cada riesgo a partir de ventanas de mantenimiento en tres notarías del círculo de Bogotá.

3. Realización de manual con base en la matriz de riesgo y los hallazgos encontrados en los problemas tecnológicos de las notarías afrontados en el siguiente trabajo.

6.5 ** Exploración previa a partir del levantamiento de información y estado del arte del sector notarial para entender las particularidades del sector notarial**

La función que tiene el notario de dar la fe pública de un proceso legal, por lo tanto necesitan en su labor diaria la utilización de herramientas tecnológicas para gestión, la supervisión y el control de los instrumentos públicos, con el fin de obtener información rápida, veraz y confiable. Dado que las notarías de primer nivel son entes autónomos en sus procesos internos (supernotariado, 2021) sustenta expresamente“No tienen personería jurídica, es el Notario quien responde como persona natural de esa oficina. No tienen la calidad de contribuyentes. Es una forma de organización administrativa para diferenciar dentro de cada Círculo Notarial en orden numérico, los Notarios que tienen competencia dentro del mismo,la Notaría no es más que la sede física donde despacha sus funciones el Notario designado para desempeñar ese cargo.

No son entes públicos ni son dependencias de la Superintendencia de Notariado y Registro, es una oficina donde el Notario, como particular que es, presta el servicio público de Notariado, y responde como persona natural de las obligaciones que le señala la Ley.”,recae la responsabilidad en esta autonomía en la notaría, responsabilidad de la seguridad, la correcta ejecución de las labores, para su posterior legalidad por medio de la fe pública.

Dado que las notarías están divididas en círculos notariales y hay una distinción económica, técnica y tecnológica según la categoría del municipio donde se encuentre el accionar de la notaría (constitución política de colombia, 1991,) expresa “El artículo 320 de la Constitución Política, dispone que la “ley podrá establecer categorías de municipios de acuerdo con su población, recursos fiscales, importancia económica y situación geográfica, y señalar distinto régimen para su organización, gobierno y administración”. Esta norma de la Constitución Política fue reglamentada por la Ley 136 de 1994, que a su vez fue modificada por la Ley 1551 de 2012, en la cual se establecen siete categorías de municipios (Especial, Primera, Segunda, Tercera, Cuarta, Quinta y Sexta)., las notarías que yacen en municipios de primera categoría sufren de una autonomía del presupuesto nacional y administrativa, que genera un escenario de libertad en cierta toma de decisiones y un riesgo informático si se toman medidas incorrectas, en la presente investigación nos centraremos en las notarías que se encuentran en municipios del primer nivel y como sus medidas o falta de ellas generan un peligro digital para el proceso.

Las notarías se generan a partir del decreto 2148 de 1983, donde se disponen toda la reglamentación general para el servicio notarial en colombia, se denota que los notarios del círculo de bogotá por ser un municipio de primer nivel, recae la responsabilidad de financiar con recursos propios, además los recursos generados por las notarías de este círculos se deberán financiar a las notarías que yacen en los demás municipios más pequeños.

Con esta lógica sabemos que el éxito de las notarías del resto de país dependen del éxito intrínseco de las notarías de bogotá, sabiendo esto y que la lógica de la financiación depende exclusivamente para las notarías del círculo de bogotá, del dinero invertido por su respectivo notario, esto genera un escenario de inversión y retorno de la inversión (ROI), generando un escenario de servicios públicos que esté suscrito a la normas del libre mercado y competencia (Mintic, 2010).

Cada notaría necesita software que puede ayudarlo a completar las tareas que realiza para brindarle un mejor servicio, mayor beneficio y competitividad en el mercado, pero muchas actividades aún no tienen este tipo de herramienta o las implementan de forma incorrecta, generando una brecha importante de seguridad, retraso en los procesos, pérdida de inversión y cuando se realiza un servicio público se afecta la fe pública y la administración pública.

Además de lo anterior en las Notarías reposa el protocolo (compendio de documentos físicos que el notario debe ser garante), documentos que son material procesal, haciendo parte del proceso misional de las notarías, en estos reposa la fe pública Dada por cada notario en su delegación, siendo el reducto de los procesos de apoyo que en suma generan tal documento, entendiendo que los procesos de apoyo son la base para generar el actuar jurídico de la notaría que en últimas se materializa en el protocolo.

A su vez las notarías son afectadas por ciberdelincuentes, que atacan directamente los sistemas internos, las notarías no saben cómo diagnosticar sus sistemas informáticos, esto se comprueba de entrevistar a tres notarios del círculo de bogotá, además la misma superintendencia se centra en generar una reglamentación general (para los operadores tecnológicos, empresas prestadoras del servicio como autenticaciones, escrituración o facturación.) que no ataca la base sino el final del proceso notarial, olvidando la implementación interna de sus servicios, servidores, computadores y software interno de la notaría (Super Notariado, 2014,).

6.6 Antecedentes de Proyectos Anteriores.

En la actualidad las notarías cuentan con un marco normativo y técnico que hegemoniza el uso del servicio notarial digital, enmarcando un macroproceso de cara al cliente (procesos misionales)unido con las instituciones de control por medio de x-road, medidas que buscar la actualización del estado,la racionalización de trámites y gestionar una seguridad digital a partir de la firma digital, un proyecto bastante ambicioso beneficioso para la nación, sin embargo se enmarca en los macro procesos, procesos misionales y hasta ahora está en implementación, falta la corrección que la praxis da a este tipo de proyecto y los ajustes que se dan unidos a la cultura inherente colombiana, estas reglamentación recae en los operadores tecnológicos (super notariado, 2021,).

Donde se retrata las nuevas tecnologías para la transformación notarial en países del primer mundo, enfocando toda su lógica en suplir y automatizar procesos misionales, entendiendo que estos países ya tienen soluciones para la base social, los procesos de apoyo, como lo son conexiones de internet, pirateria, carreteras, alimentación, educación etc,dónde vemos casos de éxito en países desarrollados color atados unidos, la unión europea, para nuestro país sabiendo que ese debe crear un escenario inspirado en el exterior pero ajustado a nuestra realidad (Popkova & Sergi, 2019, #).

Además los estudios anteriores se centraron en plataformas para autenticar procesos por medio de certificados digitales, plataformas construidas con blockchain y lógicas de certificados ssl en sistemas notariales de autenticación. (Amann, 2012, #)

En Colombia más específicamente tenemos unos adelantos tecnológicos en proyectos de ingeniería de sistemas, cómo lo son signo 365 de la empresa corporación avance, firma digital por gear electric, sistema notario, la firma digital regulada por el gobierno nacional, la factura electrónica todos estos proyectos se centran en los procesos misionales enfocados en los operadores tecnológicos(empresa que prestan servicios digitales a las notarías), olvidando los procesos de auto diagnóstico en cuanto a sistemas y seguridad de la información que originan por procesos misionales.

Las notarías sufren desde el momento de su creación ataques por parte de delincuentes que modifican documentos como escrituras, registros civiles dejando sin sistema o página web a la notaría, en pasado años a una notaría le cambiaron su página web por una pagina de adultos, en otra notaría modificaron escrituras públicas para beneficiar a un privado,ademas de casos como robos a las plataformas bancarias de las cuentas de la notaría dentro de las instalaciones, modificaciones de los documentos en digital, la suplantación de identidad por medio de la firma registrada, hechos al margen de la ley que en el mayor de sus casos se realiza desde el interior de las Notarías, casos de ciberataques que desactivan el sistema de las notarías por varias horas o días en algunos casos (Super Notariado, 2014,).

7 RESULTADOS Y DISCUSIONES

Se analizan 3 notarías del círculo de bogotá de la localidad de chapinero, donde se encuentra una simetría en los datos encontrados, partiendo de la documentación técnica que se le solicita a los notarios que es inexistente, solo poseen documentación de los procesos administrativos como son los procesos misionales de registro, escrituración y protocolo, no hay documentación de los procesos tecnológicos internos de la notaria, o los planes de acción que llevan a cabo ante cualquier eventualidad los cuales son inexistentes, se evalúan los riesgos encontrados en común por las tres notarías que se sitúan en la localidad de chapinero,

Las tres notarías exponen el mismo escenario: desconocimiento del proceso interno para el diagnóstico de la seguridad de la información, además de informar que la contracción económica género un detrimento de los ingresos para las notarías, ocasionando despidos y recorte en los presupuestos de todas las áreas, incluyendo el área de sistemas, por lo cual no se plantean reestructurar el área tecnológica en le próximo año.

los problemas comunes encontrados en las tres notarías son, fallos en la red que desconecta algún área de la empresa que se encarga de algún servicio notarial, falla en lo servidores en el último año, que generó la desconeccion del servicio notarial por varias horas, software obsoleto o desarrollado dentro de la notaría con fallos de seguridad, desconocimiento de la lógica de los backups de la información importante, virus en equipos coyunturales para pagos o transacciones del servicio notarial, posibles puertas traseras o software piratas en equipos de la notaría: dado que se encuentran en común estos riesgos informáticos, se plantea una matriz de riesgo a continuación para evaluar su incidencia dentro de la notaría.

Además al partir de la inexistencia de documentación tecnológica que relacione los procesos en seguridad de la información dentro de la notaría y el desconocimiento del proceso para evaluar el estado inicial de una notaría, yace una necesidad de estandarizar o proteger y guiar el proceso notarial a través de una guía que simplifique o ejemplifica estos procesos.

Sin embargo los notarios están dispuestos a una solución para el diagnóstico, con lo cual basar soluciones efectivas, se realizan los análisis y se compromete la información recolectada como información privada, dado que tiene ips públicas, códigos fuentes parte derechos de autor, e información sensible que puede ser utilizada por ciber atacantes para afectar el; servicio notarial.

7.1 **Análisis con base en escenarios reales dentro de tres notarías del círculo de Bogotá y matriz de riesgo**

7.1.1 Matriz de riesgo.

Matriz de riesgos, riesgo 1 al 3

EJE	PROCESO	OBJETIVO	CAUSA	RIESGO	DESCRIPCION DEL RIESGO	TIPO DE RIESGO	VERIFICACION RIESGO DE CORRUPCION	ES RIESGO CORRUPCION	CODIGO	CONSECUENCIA
Eje de Calidad	Gestión de la tecnología e información	Orientar la gestión de las Tecnologías de la Información y las Comunicaciones – TIC - articulada con la estrategia de negocio, generando valor en el marco de las políticas y lineamientos establecidos por la autoridad competente.	Indisponibilidad de los: Canales (WAN, LAN), Servidores y correo electrónico.	falla servidores y correos Afectación de la plataforma tecnológica de canales, servidores y correo electrónico.	Interrupciones que afectan la funcionalidad de canales, servidores , y correo electrónico de forma parcial.	Tecnología	Se puede presentar acción u omisión del funcionario o colaborador. No hay uso del poder. No hay desviación de la gestión de lo público. No hay beneficio particular. NO ES UN RIESGO DE CORRUPCIÓN	NO	GT1	falla correos, canales y servidores, Afectación de la operación de los procesos de la entidad que se soportan en infraestructura tecnologica, por indisponibilidad de canales, servidores y correo electrónico.
Eje de Calidad	Gestión de la tecnología e información	Orientar la gestión de las Tecnologías de la Información y las Comunicaciones – TIC - articulada con la estrategia de negocio, generando valor en el marco de las políticas y lineamientos establecidos por la autoridad competente.	Rotación de personal que conoce el modelo operativo que soporta el sistema de información. Cambio de priorización de actividades propias del área solicitante del desarrollo software. Brechas entre la operación real y el modelo operativo previsto para el sistema de información o desarrollo software. El área solicitante no participa en la etapa de especificación y pruebas de acuerdo a lo planificado. Desfase en la estimación de esfuerzo en las etapas del ciclo de desarrollo. Desfase en la estimación del alcance de los requerimientos.	software obsoleto, Afectación en el cumplimiento de la entrega de los requerimientos solicitados por las áreas usuarias	Retraso en las etapas del ciclo de desarrollo de las funcionalidades nuevas o ajustes a los desarrollos de software, por no ejecutarse en los tiempos estimados (o programados) por dificultades asociadas con la disponibilidad del usuario funcional y/o desfase en la estimación del esfuerzo	Operativo	No hay acción u omisión. No hay uso del poder. No hay desviación de la gestión de lo público. Se puede generar un beneficio particular. NO ES UN RIESGO DE CORRUPCIÓN	NO	GT2	letargo creacion de software, Afectación en la entrega oportuna de los desarrollos de software solicitados por las áreas usuarias
Eje de Calidad	Gestión de la tecnología e información	Orientar la gestión de las Tecnologías de la Información y las Comunicaciones – TIC - articulada con la estrategia de negocio, generando valor en el marco de las políticas y lineamientos establecidos por la autoridad competente.	falla del cableado estructurado	cableado estructurado ,afectacion en la comunicacion general de la notaria	interrupcion del servicio notarial y posible multa o perdida de investidura	Tecnología	Se puede presentar acción u omisión del funcionario o colaborador. No hay uso del poder. No hay desviación de la gestión de lo público. No hay beneficio particular. NO ES UN RIESGO DE CORRUPCIÓN	NO	GT3	cableado estructurado nulo afectacion en la optencion de copias de registro civil, creacion de escrituras y gestion de servicios de hojas notariales

Tabla 2 , matriz de riesgos notarías,fuente propia

Se analizan los riesgos;
GT1: falla servidores y correos Afectación de la plataforma tecnológica de canales, servidores y correo electrónico.
GT2:software obsoleto, Afectación en el cumplimiento de la entrega de los requerimientos solicitados por las áreas usuarias.
GT3:cableado estructurado ,afectación en la comunicación general de la notaría.

Matriz de riesgos, riesgo 4 al 6

EJE	PROCESO	OBJETIVO	CAUSA	RIESGO	DESCRIPCION DEL RIESGO	TIPO DE RIESGO	VERIFICACION RIESGO DE CORRUPCION	ES RIESGO CORRUPCION	CODIGO	CONSECUENCIA
Eje de Calidad	Gestión de la tecnología e información	Orientar la gestión de las Tecnologías de la Información y las Comunicaciones – TIC - articulada con la estrategia de negocio, generando valor en el marco de las políticas y lineamientos establecidos por la autoridad competente.	nula generacion de backups de la informaicon que reposa en las notarias.	falta de backups, afectacion del servicio e interrupcion total del servicio, con nula opcion de rescate de la informacion	en algun imprevisto se puede perder toda la informacion, donde sin tener replicas de la informacion se perderian todos los registros civiles y escrituras	Tecnología	Se puede presentar acción u omisión del funcionario o colaborador. Se puede presentar uso del poder. Se puede presentar desviación de la gestión de lo público. Se puede generar un beneficio particular. ES UN RIESGO DE CORRUPCIÓN	SI	GT4	falta de backups afectacion del quehacer notarial
Eje de Calidad	Gestión de la tecnología e información	Orientar la gestión de las Tecnologías de la Información y las Comunicaciones – TIC - articulada con la estrategia de negocio, generando valor en el marco de las políticas y lineamientos establecidos por la autoridad competente.	software pirata	software, pirata falla de los equipos, multas, virus en los equipos de computo, posibilidad de acceso por medio de un tercero por medio de una back door a la informacion de la notaria	se puede tener multas por utilizar software pirata, ademas de generar fallos de seguridad	Tecnología	Se puede presentar acción u omisión del funcionario o colaborador. Se puede presentar uso del poder. Se puede presentar desviación de la gestión de lo público. Se puede generar un beneficio particular. ES UN RIESGO DE CORRUPCIÓN	SI	GT5	software pirata, modificacion de la fe publica y posible perdida de informacion
Eje de Calidad	Gestión de la tecnología e información	Orientar la gestión de las Tecnologías de la Información y las Comunicaciones – TIC - articulada con la estrategia de negocio, generando valor en el marco de las políticas y lineamientos establecidos por la autoridad competente.	virusa implanmtados o descargados por error	posibilidad de descargar un virus, malware, o la posibilidad de implantar un virus en los equipos de la notaria	se puede implantar un software malicioso en los equipos de la notaria, afectando los pilares de la informacion	Tecnología	VC No hay acción u omisión. No hay uso del poder. No hay desviación de la gestión de lo público. Se puede generar un beneficio particular. NO ES UN RIESGO DE CORRUPCIÓN	NO	GT6	robo de informacion, robo de dinero

Tabla 3, matriz de riesgos 2 notarías ,fuente propia

Se analizan los riesgos;

GT4:falta de backups, afectación del servicio e interrupción total del servicio, con nula opción de rescate de la información.
GT5:software, pirata falla de los equipos, multas, virus en los equipos de cómputo, posibilidad de acceso por medio de un tercero por medio de una backdoor a la información de la notaría.
GT6: posibilidad de descargar un virus, malware, o la posibilidad de implantar un virus en los equipos de la notaría

2. ANALISIS DE RIESGO INHERENTE							
EJE	PROCESO	RIESGO	CODIGO	RIESGO INHERENTE			
				PROBABILIDAD	DETERMINACIÓN DE IMPACTO	IMPACTO	NIVEL RIESGO
Eje de Calidad	Gestión de la tecnología e información	falla servidores y correos Afectación de la plataforma tecnológica de canales, servidores y correo electrónico.	GT1	CASI SEGURO	Las categorias afectadas son: -Proceso -Imagen -Recursos -Intervención -Información Total Categorias: 5	CATASTROFICO	EXTREMA-INACEPTABLE 25
Eje de Calidad	Gestión de la tecnología e información	software obsoleto, Afectación en el cumplimiento de la entrega de los requerimientos solicitados por las áreas usuarias	GT2	CASI SEGURO	Las categorias afectadas son: -Información Total Categorias: 1	INSIGNIFICANTE	ALTA-IMPORTANTE 5
Eje de Calidad	Gestión de la tecnología e información	cableado estructurado ,afectacion en la comunicacion general de la notaria	GT3	CASI SEGURO	Las categorias afectadas son: -Información Total Categorias: 1	INSIGNIFICANTE	ALTA-IMPORTANTE 5

Tabla 4 , matriz de riesgos notarías 3,fuente propia

Al evaluar el riesgo, de fallo de servidor GT1, que es casi seguro que ocurra dado que, ya ha pasado con anterioridad según información suministrada por la notaría, con un nivel de riesgo inaceptable y un impacto catastrófico (una notaría perdió 1 mes de información por falla en los servidores), seguido en compromiso de la infraestructura por el gt2 y gt3.

2. ANALISIS DE RIESGO INHERENTE							
EJE	PROCESO	RIESGO	CODIGO	RIESGO INHERENTE			
				PROBABILIDAD	DETERMINACIÓN DE IMPACTO	IMPACTO	NIVEL RIESGO
Eje de Calidad	Gestión de la tecnología e información	falta de backups, afectacion del servicio e interrupcion total del servicio, con nula opcion de rescate de la informacion	GT4	POSIBLE	Las categorias afectadas son: -Imagen Total Categorias: 1	MODERADO	ALTA-IMPORTANTE 9
Eje de Calidad	Gestión de la tecnología e información	software, pirata rsins de los equipos, multas, virus en los equipos de computo, posibilidad de acceso por medio de un tercero por medio de una back door a la informacion de la notaria	GT5	POSIBLE	Las categorias afectadas son: -Recursos Total Categorias: 1	MENOR	MODERADO 6
Eje de Calidad	Gestión de la tecnología e información	posibilidad de descargar un virus, malware, o la posibilidad de implantar un virus en los equipos de la notaria	GT6	CASI SEGURO	DI Las categorias afectadas son: -Recursos Total Categorias: 1	MENOR	ALTA-IMPORTANTE 10

Tabla 5, matriz de riesgos notarías 4,fuente propia

Los siguientes riesgos más importantes según el nivel de impacto son gt4 (backups), gt6 (virus) y por último gt5 (software sin licencia), dado que el menor riesgo es gt5 por su impacto menor en la organización, los otros dos riesgos generan un impacto moderado

7.2 mapa de riesgos

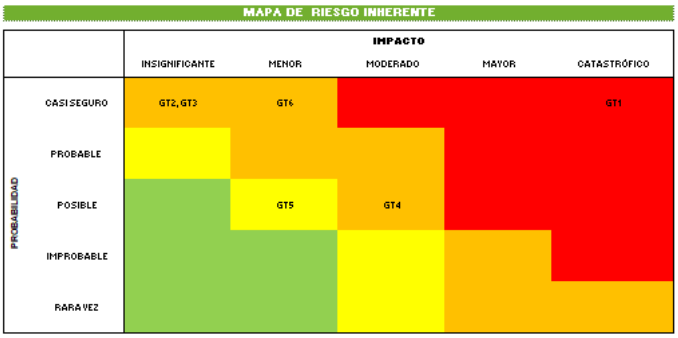


Gráfico 1 , mapa residual,fuente propia

Vemos cómo se posicionan en la gráfica anterior el mapa de riesgo inherente con base en el impacto, por lo cual hay que prestar total atención al gt1 que corresponde con los fallos de servidores, por su impacto catastrófico, según la experiencia varias notarías poseen este fallo, además tienen servidores desde hace más de 11 años sin ninguna actualización, con sistemas obsoletos opensuse 9.0, que en la última década no se les ha realizado mantenimiento , actualización y optimización, donde reposa el sistema notarial con toda la información notarial, sistemas como lo son notario o sinfony que corren sobre cmd en un servidor de archivos.

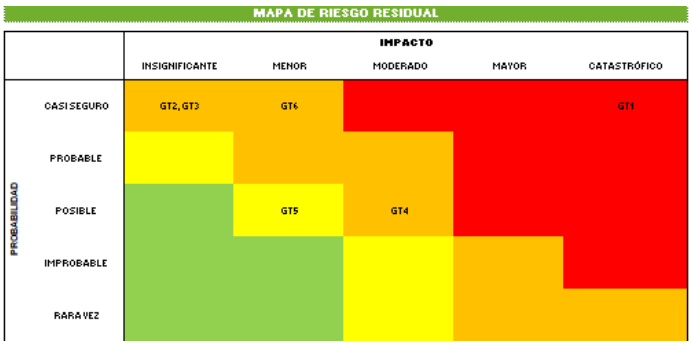


Gráfico 2, mapa residual,fuente propia

Actualmente por desconocimiento no se obtiene una reducción del riesgo residual dado que hay desconocimiento por parte de las notarías por medio de un auto diagnóstico, que ayude a determinar el estado actual de ellas

7.3: Análisis real de los riesgos por medio de casos reales de fallas dentro de las notarías.

Se analizan 6 escenarios reales encontrados en común en las tres notarías:

7.3.1 GT1: falla servidores y correos Afectación de la plataforma tecnológica de canales, servidores y correo electrónico.

Se analiza por medio de la herramienta nmap,el servidor principal dentro de la notaría, en el cual encontramos la siguiente información, para si encontrar informacion que nos de luz a posibles vulnerabilidades,

Escaneo nmap

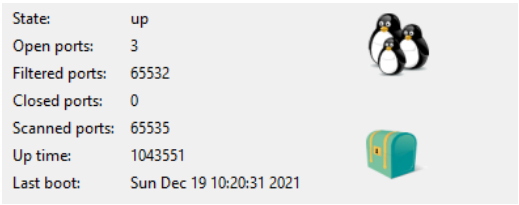


Gráfico 3, escaneo sistema operativo ,fuente propia

Encontramos que el servidor está en estado activo, con último reinicio del 19 de diciembre del 2021, con 65532 puertos filtrados por medio del firewall del sistema operativo, el sistema operativo es sles 15. sp2, el cual fue instalado el día 20, de noviembre del 2021, luego de una falla en la localidad de Chapinero del alumbrado público, que genera el apagado repentino de los equipos, y la falla del sistema operativo.

Escaneo de puertos nmap servidor

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 8.1 (protocol 2.0)
139	tcp	open	netbios-ssn	Samba smbd 4.6.2
445	tcp	open	netbios-ssn	Samba smbd 4.6.2

Gráfico 4, escaneo de puertos ,fuente propia

Se escanea el servidor encontrado tres puertos activados, puerto de samba tanto de entrada como salida, los puertos 139 y 445, se utilizan para el servidor lógico samba, con el cual se comparte información con los computadores de sistema operativo windows, y el puerto 22 con el cual se conecta por medio de ssh, este puerto lo utilizo constantemente para darle soporte al servidor cuando es necesario.

Escaneo puertos nmap router

Port	Protocol	State	Service	Version
53	tcp	open	domain	dnsmasq 2.40
80	tcp	open	http	
443	tcp	open	https	
2601	tcp	open	zebra	GNU Zebra routing software 0.93b
2602	tcp	open	zebra	GNU Zebra routing software 0.93b
5443	tcp	open	spss	
60443	tcp	open	unknown	

Gráfico 5, escaneo de puertos router,fuente propia

Se escanea el router para encontrar brechas a partir de los puertos abiertos, nos encontramos con un escenario desalentador dado que, se encuentran puertos no conocidos abiertos, se indaga al personal interno de la notaría y no saben por qué o quién abrió estos puertos, además no hay documentación al respecto, además varias personas y empresas intervienen estos dispositivos sin generar trazabilidad o articulación procedimental entre ellas.

Se encuentran abiertos los puertos 5443, 60443, 53, 2601, 2602, los cuales no se tiene información dentro de la empresa para que son utilizados, los puertos 80 y 443 son para navegación.

7.3.2 GT2:software obsoleto, Afectación en el cumplimiento de la entrega de los requerimientos solicitados por las áreas usuarias

Analizamos el servidor de una notaría que posee un software desarrollado por un tercero, El servidor posee una versión antigua de php , la versión 5.3, el servidor se encuentra en sles 12 sp 1, sin contrato de licencia lo cual es un fallo de seguridad importante dentro de la organización, dado que sin la licencia el servidor no se puede actualizar, al igual no hay soporte para php 7 u 8, los cuales son los estandarizados hoy dia para el desarrollo de software en php.

Carpeta de software notarial

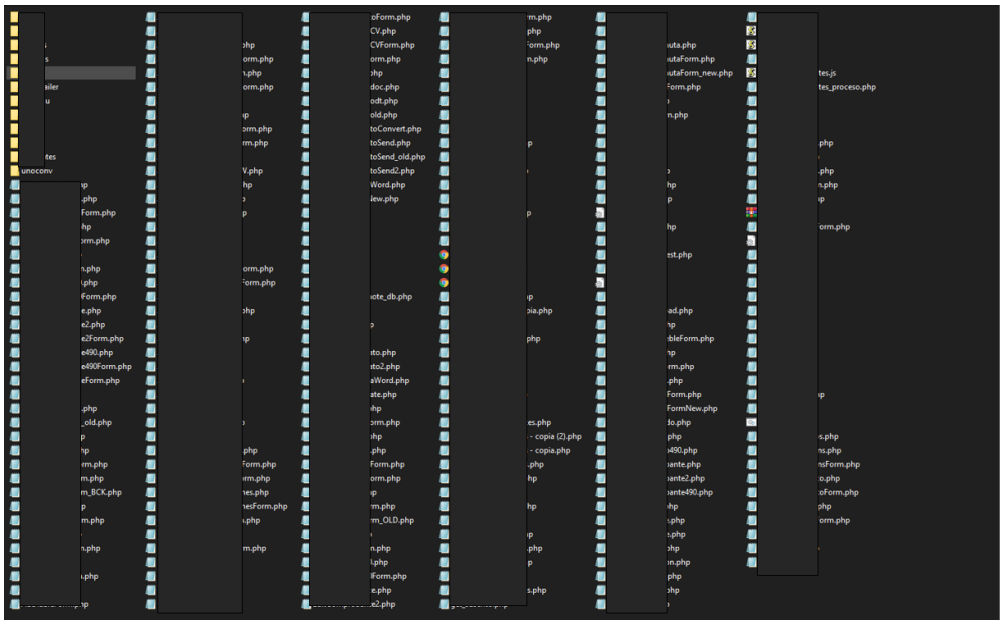


Gráfico 6, software notarial para la creación de escrituras,fuente propia

Accedo al código fuente del software, para revisar su construcción, solicitó la documentación a la notaría la cual según información directa de la notaría es inexistente, la persona que desarrolló el proyecto no entregó documentación alguna, el software está construido en php, con bases de datos en mysql, sin embargo se encuentra que no esta organizado el codigo y no corresponde a tipo de desarrollo de software, solo se encuentra un compendio de clases en la carpeta raíz, clases repetidas y codigo sin utilizar, se oculta la información de los nombres de las clases por solicitud del notario directamente y posterior firma de contrato de confidencialidad firmado entre la notaría y mi parte.

script base de datos software notarial

Gráfico 7, base de datos del software para la creación de escrituras,fuente propia

Se encuentran los backups de las bases de datos realizados diariamente, des del dia 18 de noviembre del 2019, sin embargo al analizar las bases de datos nos encontramos sin contenido cifrado, es fácilmente posible copiar las claves y usuarios del sistema dado que se encuentran en texto plano, se oculta la información de los datos confidenciales por solicitud del notario directamente, posterior firma de contrato de confidencialidad firmado entre la notaría y mi parte.

7.3.3 GT3:cableado estructurado ,afectación en la comunicación general de la notaría:

por medio de solicitud de la notaría se analiza la coneccion de internet, dado que varios funcionarios reportan fallas en la conexión, al revisar dicha conexión se evidencia que tienen una conexión banda ancha con el proveedor claro, de 100 megas, sin embargo al hacer las pruebas de conexión funciona correctamente, al entrevistar a los funcionarios que reportan el problema indican que la desconeccion llega cuando estiran los pies, re revisa la coneccion en la parte inferior de los puestos de trabajo y se encuentra que no hay cableado estructurado, solo hay un cable que viene desde el centro de datos por el piso hasta llegar al computador del funcionario, por lo cual cada vez que el funcionario estira las piernas se desconecta el cable.

Medición conexión internet herramienta de google fibre

Gráfico 8 , medición de canal 1 l,fuente propia

Medición conexión internet herramienta de speed test

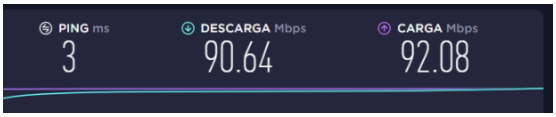


Gráfico 9, medición de canal 2l,fuente propia

Se realiza un tracert hacia la herramienta de gestión notarial signo 365, funciona correctamente, hay unos tiempos de respuesta agotados, se indaga con el proveedor tecnológico, donde nos indica que estos tiempos agotados son gracias a un firewall que ellos poseen para el filtrado de las conecciones.

Tracert notaria - signo360.co

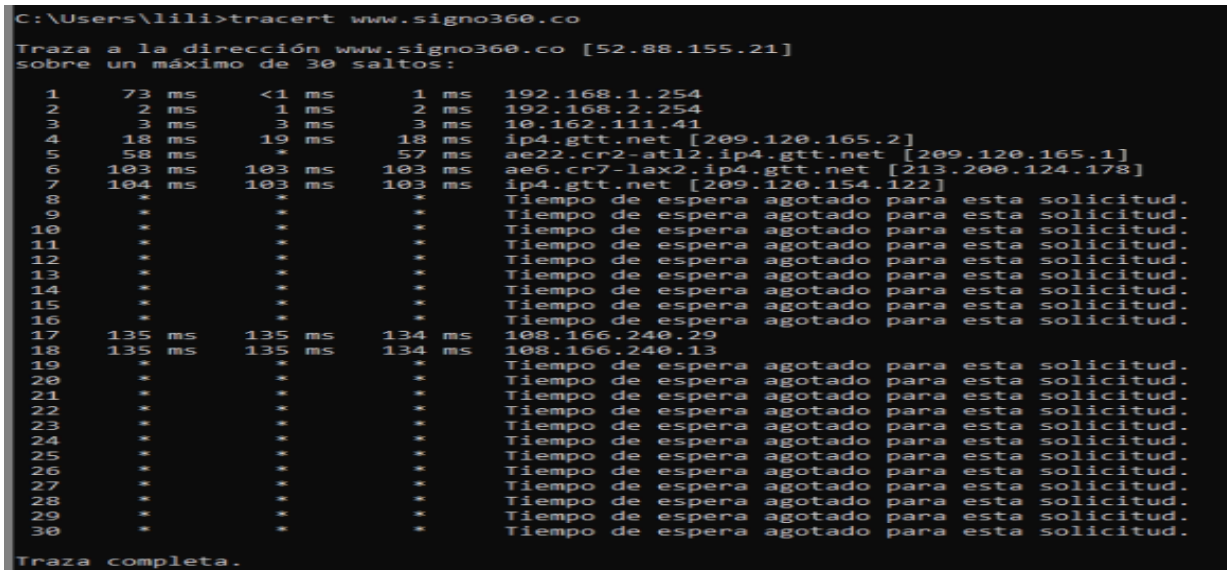


Gráfico 10, tracer signo 360l,fuente propia

7.3.4 GT4:falta de backups, afectación del servicio e interrupción total del servicio, con nula opción de rescate de la información.

Se analizan los backups de dos notarías, en la primera notaría se accede al archivo log que deja el trabajo de backups, se evidencian backups completos de bases de datos desde el 18 de noviembre del 2019 hasta la fecha, se abren los backups para verificar que la información se encuentre efectivamente, correctamente se encuentra la información dentro de los scrips de las bases de datos, sin embargo esta información no tiene ningún tipo de encriptación

Registro backups por medio de cron job 1

```
Respaldo realizado exitosamente el Mon Nov 18 15:57:27 -05 2019
Respaldo realizado exitosamente el Mon Nov 18 16:00:33 -05 2019
Respaldo realizado exitosamente el Tue Nov 19 23:00:02 -05 2019
Respaldo realizado exitosamente el Wed Nov 20 23:00:02 -05 2019
Respaldo realizado exitosamente el Thu Nov 21 23:00:01 -05 2019
Respaldo realizado exitosamente el Fri Nov 22 23:00:01 -05 2019
Respaldo realizado exitosamente el Sat Nov 23 23:00:02 -05 2019
Respaldo realizado exitosamente el Sun Nov 24 23:00:02 -05 2019
Respaldo realizado exitosamente el Mon Nov 25 23:00:01 -05 2019
Respaldo realizado exitosamente el Tue Nov 26 23:00:02 -05 2019
Respaldo realizado exitosamente el Wed Nov 27 23:00:02 -05 2019
Respaldo realizado exitosamente el Thu Nov 28 23:00:02 -05 2019
Respaldo realizado exitosamente el Fri Nov 29 23:00:02 -05 2019
Respaldo realizado exitosamente el Sat Nov 30 23:00:02 -05 2019
Respaldo realizado exitosamente el Sun Dec  1 23:00:02 -05 2019
Respaldo realizado exitosamente el Mon Dec  2 23:00:01 -05 2019
Respaldo realizado exitosamente el Tue Dec  3 23:00:02 -05 2019
```

Gráfico 11 ,registro backups 1 ,fuente propia

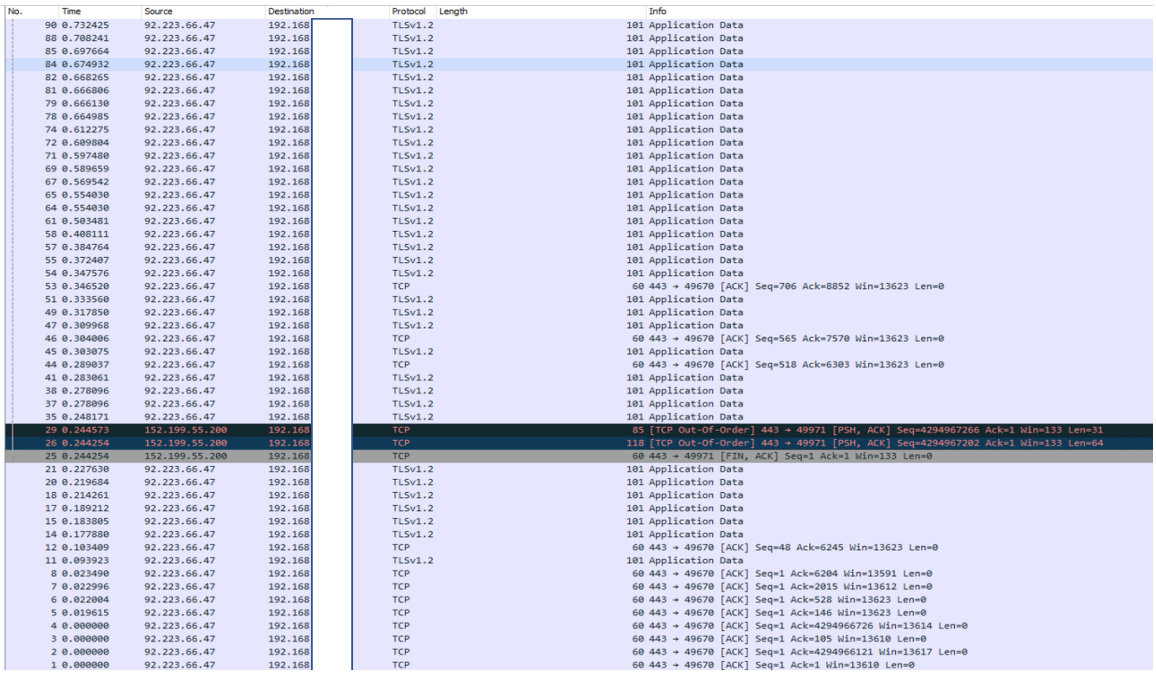
Registro backups por medio de cron job 2

```
Respaldo realizado exitosamente el Thu Dec  9 23:00:04 -05 2021
Respaldo realizado exitosamente el Fri Dec 10 23:00:03 -05 2021
Respaldo realizado exitosamente el Sat Dec 11 23:00:04 -05 2021
Respaldo realizado exitosamente el Sun Dec 12 23:00:04 -05 2021
Respaldo realizado exitosamente el Tue Dec 14 23:00:04 -05 2021
Respaldo realizado exitosamente el Wed Dec 15 23:00:04 -05 2021
Respaldo realizado exitosamente el Thu Dec 16 23:00:04 -05 2021
Respaldo realizado exitosamente el Fri Dec 17 23:00:04 -05 2021
Respaldo realizado exitosamente el Sat Dec 18 23:00:04 -05 2021
Respaldo realizado exitosamente el Sun Dec 19 23:00:04 -05 2021
Respaldo realizado exitosamente el Mon Dec 20 23:00:04 -05 2021
Respaldo realizado exitosamente el Tue Dec 21 23:00:04 -05 2021
Respaldo realizado exitosamente el Wed Dec 22 23:00:04 -05 2021
Respaldo realizado exitosamente el Thu Dec 23 23:00:04 -05 2021
Respaldo realizado exitosamente el Fri Dec 24 23:00:04 -05 2021
Respaldo realizado exitosamente el Sat Dec 25 23:00:04 -05 2021
Respaldo realizado exitosamente el Sun Dec 26 23:00:04 -05 2021
Respaldo realizado exitosamente el Mon Dec 27 23:00:04 -05 2021
Respaldo realizado exitosamente el Tue Dec 28 23:00:04 -05 2021
```

Gráfico 12,registro backups 2 ,fuente propia

7.3.5 GT5:software, pirata falla de los equipos, multas, virus en los equipos de cómputo, posibilidad de acceso por medio de un tercero por medio de una backdoor a la información de la notaría.

Escanero notaría por medio de wireshark



No.	Time	Source	Destination	Protocol	Length	Info
90	0.732425	92.223.66.47	192.168	TLSv1.2	101	Application Data
88	0.708241	92.223.66.47	192.168	TLSv1.2	101	Application Data
85	0.697664	92.223.66.47	192.168	TLSv1.2	101	Application Data
84	0.674932	92.223.66.47	192.168	TLSv1.2	101	Application Data
82	0.668265	92.223.66.47	192.168	TLSv1.2	101	Application Data
81	0.666806	92.223.66.47	192.168	TLSv1.2	101	Application Data
79	0.666130	92.223.66.47	192.168	TLSv1.2	101	Application Data
78	0.664985	92.223.66.47	192.168	TLSv1.2	101	Application Data
74	0.612275	92.223.66.47	192.168	TLSv1.2	101	Application Data
72	0.609804	92.223.66.47	192.168	TLSv1.2	101	Application Data
71	0.597480	92.223.66.47	192.168	TLSv1.2	101	Application Data
69	0.589659	92.223.66.47	192.168	TLSv1.2	101	Application Data
67	0.569542	92.223.66.47	192.168	TLSv1.2	101	Application Data
65	0.554030	92.223.66.47	192.168	TLSv1.2	101	Application Data
64	0.554030	92.223.66.47	192.168	TLSv1.2	101	Application Data
61	0.503481	92.223.66.47	192.168	TLSv1.2	101	Application Data
58	0.408111	92.223.66.47	192.168	TLSv1.2	101	Application Data
57	0.384764	92.223.66.47	192.168	TLSv1.2	101	Application Data
55	0.372407	92.223.66.47	192.168	TLSv1.2	101	Application Data
54	0.347576	92.223.66.47	192.168	TLSv1.2	101	Application Data
53	0.346520	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=706 Ack=8852 Win=13623 Len=0
51	0.333560	92.223.66.47	192.168	TLSv1.2	101	Application Data
49	0.317850	92.223.66.47	192.168	TLSv1.2	101	Application Data
47	0.309968	92.223.66.47	192.168	TLSv1.2	101	Application Data
46	0.304006	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=565 Ack=7570 Win=13623 Len=0
45	0.303075	92.223.66.47	192.168	TLSv1.2	101	Application Data
44	0.289037	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=518 Ack=6303 Win=13623 Len=0
41	0.283061	92.223.66.47	192.168	TLSv1.2	101	Application Data
38	0.278096	92.223.66.47	192.168	TLSv1.2	101	Application Data
37	0.278096	92.223.66.47	192.168	TLSv1.2	101	Application Data
35	0.248171	92.223.66.47	192.168	TLSv1.2	101	Application Data
29	0.244573	152.199.55.200	192.168	TCP	85	[TCP Out-Of-Order] 443 → 49971 [PSH, ACK] Seq=4294967266 Ack=1 Win=133 Len=31
26	0.244254	152.199.55.200	192.168	TCP	118	[TCP Out-Of-Order] 443 → 49971 [PSH, ACK] Seq=4294967202 Ack=1 Win=133 Len=64
25	0.244254	152.199.55.200	192.168	TCP	60	443 → 49971 [FIN, ACK] Seq=1 Ack=1 Win=133 Len=0
21	0.227630	92.223.66.47	192.168	TLSv1.2	101	Application Data
20	0.219684	92.223.66.47	192.168	TLSv1.2	101	Application Data
18	0.214261	92.223.66.47	192.168	TLSv1.2	101	Application Data
17	0.189212	92.223.66.47	192.168	TLSv1.2	101	Application Data
15	0.183805	92.223.66.47	192.168	TLSv1.2	101	Application Data
14	0.177880	92.223.66.47	192.168	TLSv1.2	101	Application Data
12	0.103409	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=48 Ack=6245 Win=13623 Len=0
11	0.093923	92.223.66.47	192.168	TLSv1.2	101	Application Data
8	0.023490	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=1 Ack=6204 Win=13591 Len=0
7	0.022996	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=1 Ack=2015 Win=13612 Len=0
6	0.022004	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=1 Ack=528 Win=13623 Len=0
5	0.019615	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=1 Ack=146 Win=13623 Len=0
4	0.000000	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=1 Ack=4294966726 Win=13614 Len=0
3	0.000000	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=1 Ack=105 Win=13610 Len=0
2	0.000000	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=1 Ack=4294966121 Win=13617 Len=0
1	0.000000	92.223.66.47	192.168	TCP	60	443 → 49670 [ACK] Seq=1 Ack=1 Win=13610 Len=0

Gráfico 13, escanero wireshark ,fuente propia

Se analiza un equipo de la notaría en modo promiscuo, para revisar el tráfico, el funcionario informa que desde ese equipo realiza los pagos de toda la notaría, que en pasados días el mouse se movía solo, además se encuentra que el equipo tenía un office no licenciado.

Al hacer el escaneo con wireshark, se encuentran una conecciones remotas desconocidas hacia unas ips remotas,

resultado escaneado, conexión remota por 443.

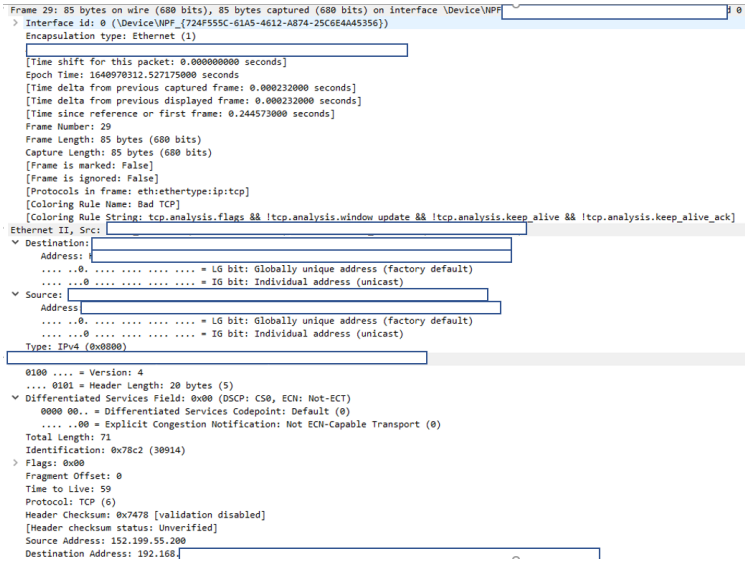


Gráfico 14, escanero wireshark 2 ,fuente propia

7.3.6 GT6: posibilidad de descargar un virus, malware, o la posibilidad de implantar un virus en los equipos de la notaría

Al analizar un equipo dentro de la notaría, revisamos y el equipo tenía antivirus activo, licenciado, es un equipo que utilizan varias personas dentro de la notaría y además se utiliza para acceder a las plataformas bancarias, sin embargo hay unos software en visual script que se encuentran sospechosos dado que tienen nombres poco comunes y están agregados al inicio del sistema operativo.

Carpeta de startup de windows, computador notarial.

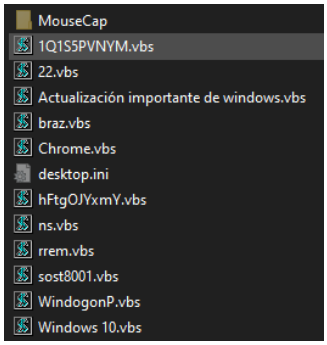


Gráfico 15 archivos vbs encontrados en notaria ,fuente propia

Los archivos en la imagen de arriba son tomados directamente de uno de los computadores principales de la notaría, por lo cual se analizan por medio de la herramienta antivirus del cai virtual de la policía nacional, dado que el antivirus instalado en el equipo no encontró ninguna anomalía.

Informe cai virtual policia nacional

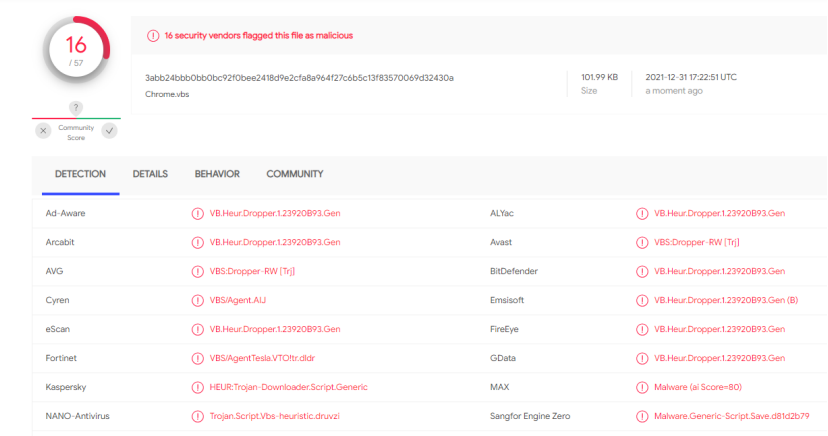


Gráfico 16, análisis archivos cai virtual con resultados ,fuente propia

Al analizar con la herramienta de la policía nacional, nos indica que posee 16 tipos de virus en los archivos analizados.

Informe fortinet

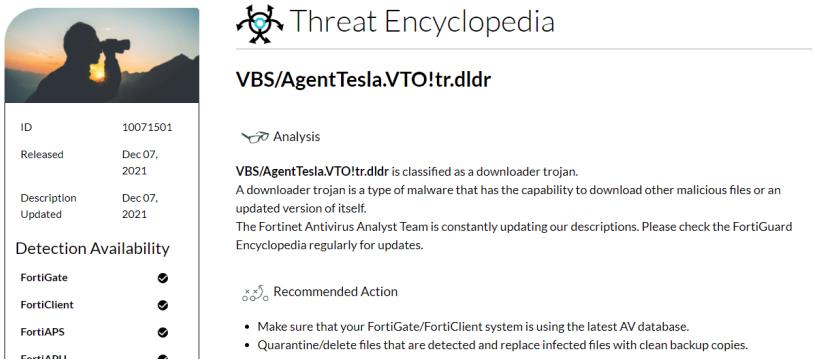
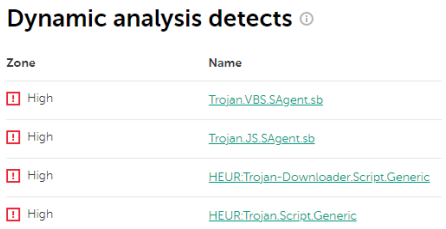


Gráfico 17, análisis archivos por medio de fortiguard,fuente propia

Unos de los malware identificados luego de analizar los archivos con la herramienta de escaneo de fortigate-fortinet, es un software troyano que se auto actualiza, puede realizar cargas y descargas directamente a la computadora infectada.



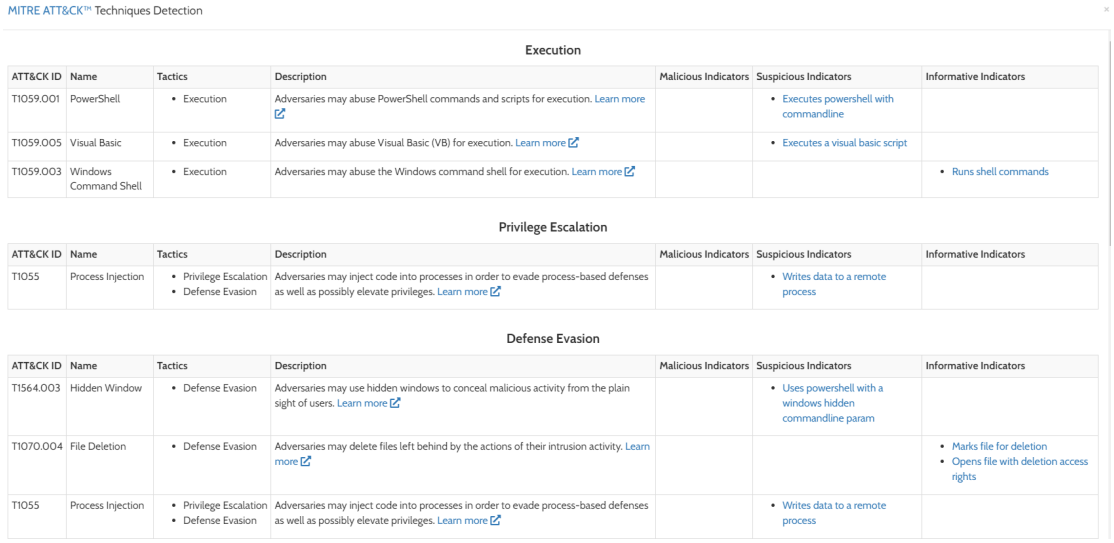
Dynamic analysis detects

Zone	Name
High	Trojan.VBS.SAgent.sb
High	Trojan.JS.SAgent.sb
High	HEUR:Trojan-Downloader.Script.Generic
High	HEUR:Trojan.Script.Generic

Gráfico 18, análisis archivos por medio de kaspersky web 2 ,fuente propia

Al analizar con la herramienta de Kaspersky para obtener más información, se evidencia que el software malicioso posee 4 agentes de conexión que trabajan como procesos del sistema.

Informe Mitre parte 1



MITRE ATT&CK™ Techniques Detection

Execution

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1059.001	PowerShell	• Execution	Adversaries may abuse PowerShell commands and scripts for execution. Learn more		• Executes powershell with commandline	
T1059.005	Visual Basic	• Execution	Adversaries may abuse Visual Basic (VB) for execution. Learn more		• Executes a visual basic script	
T1059.003	Windows Command Shell	• Execution	Adversaries may abuse the Windows command shell for execution. Learn more			• Runs shell commands

Privilege Escalation

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1055	Process Injection	• Privilege Escalation • Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more		• Writes data to a remote process	

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1564.003	Hidden Window	• Defense Evasion	Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. Learn more		• Uses powershell with a windows hidden commandline param	
T1070.004	File Deletion	• Defense Evasion	Adversaries may delete files left behind by the actions of their intrusion activity. Learn more			• Marks file for deletion • Opens file with deletion access rights
T1055	Process Injection	• Privilege Escalation • Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more		• Writes data to a remote process	

Gráfico 19, análisis archivos por medio de mitre ,fuente propia

Dada la gravedad de los hallazgos, procedemos a revisar más a fondo dichos archivos en el inicio del sistema operativo, para determinar que pueden operar dentro de la computadora, encontramos que los archivos pueden, correr visual basic script, abrir terminales shell para correr comandos del sistema, ejecutar comandos de powershell,

escribir datos en procesos remotos, elevar privilegios de sistema, correr comando ocultos del usuario, borrar datos del sistema, evadir firewall y antivirus.

Informe Mitre parte 2

MITRE ATT&CK™ Techniques Detection

T1070.004	File Deletion	• Defense Evasion	Adversaries may delete files left behind by the actions of their intrusion activity. Learn more			• Marks file for deletion • Opens file with deletion access rights
T1055	Process Injection	• Privilege Escalation • Defense Evasion	Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Learn more		• Writes data to a remote process	
T1112	Modify Registry	• Defense Evasion	Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Learn more			• Modifies proxy settings

Credential Access

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	• Credential Access • Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more			• Installs hooks/patches the running process

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1012	Query Registry	• Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more			• Queries sensitive IE security settings • Monitors specific registry key for changes • Queries the display settings of system associated file extensions • Reads the windows installation date • Reads information about supported languages

Gráfico 20, análisis archivos por medio de mitre 2 ,fuente propia

Además de lo anterior vemos como la herramienta hitre att&ck, nos define los archivos con la posibilidad de acceder a las credenciales del sistema, autenticar por medio de apis, monitorear cambios del sistema, modificar extensiones y programas asociados a ellas, leer información de lenguajes.

Informe Mitre parte 3

T1082	System Information Discovery	• Discovery	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more			• Reads the cryptographic machine GUID • Contains ability to read software policies
T1018	Remote System Discovery	• Discovery	Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Learn more		• Checks network status using ping	

Collection

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	• Credential Access • Collection	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more			• Installs hooks/patches the running process

Gráfico 21, análisis archivos por medio de mitre 3 ,fuente propia

Por último encontramos que los archivos maliciosos son capaces de correr la interfaz visual del sistema operativo al igual que el CLI, leer información del software dentro de la computadora e instalar o desinstalar software o parches de seguridad.

Diagrama ejecución de acciones por medio del script

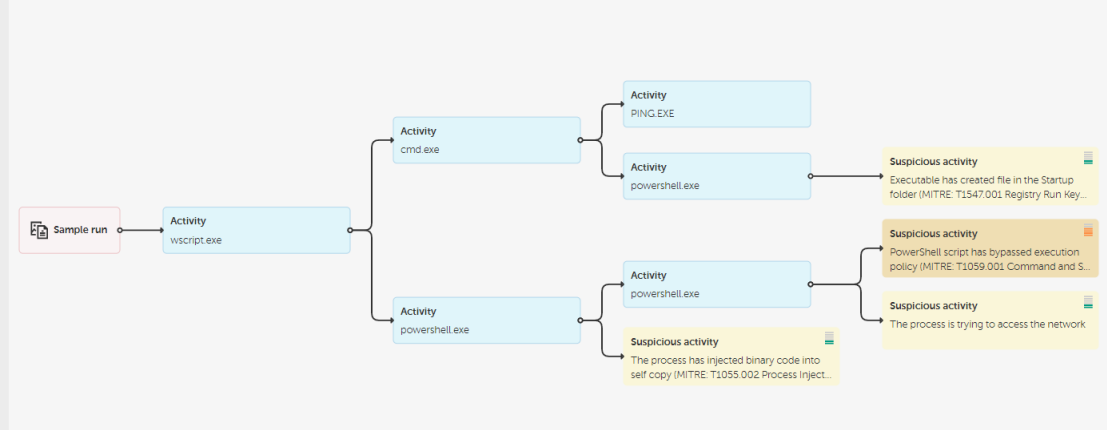


Gráfico 22, acción del virus sobre el sistema notarial ,fuente kaspersky

Los scripts dentro del equipo de la notaría que se corren al inicio de la computadora, actúan de la manera que describe el gráfico, se corre al iniciar el sistema operativo, evaden el software antivirus, ejecuta una shell de powershell y cmd: inyectan código binario en el sistema, toman control del equipo, verifica que los demás archivos del código malicioso estén en la carpeta de startup del sistema operativo, si no se encuentran, el mismo los crea.

Luego de esto eleva privilegios dentro del sistema y se conecta por medio de un broadcast a la red para infectar más equipos.

8 CONCLUSIONES

Luego de analizar diferentes escenarios reales dados por notarias de primer nivel del círculo de Bogotá, encontramos que la brecha digital entre notarías es grande y estas están melladas por el vertiginoso cambio tecnológico. comprobamos que soluciones de antivirus por si solas no son suficientes para una correcta seguridad tecnológica, además que la falta de capacitación tanto de los funcionarios internos de la notaría como del mismo notario genera una brecha de seguridad abismal, tanto así que la toma de decisiones por parte de los stakeholders sin conocimiento intrínseco en tecnología ocasiona la disrupción tecnológica y expone al estado colombiano por medio de las notarías a una obsolescencia tecnológica.

Con base en el análisis de 6 riesgos identificados en común en las tres notarías objeto de estudio se procede a hacer una matriz de riesgo, la cual nos arroja una visión global de los problemas más comunes que pueden afectar una notaría

Vemos en los mapas de riesgo que la falta de una estrategia clara puede ocasionar fallos en la gestión notarial, ocasionando pérdida de activos intangibles, credibilidad y efectos socioeconómicos altamente contraproducentes para el país.
Es imperante extender el manual que se expone a continuación a todas las notarías, para que ellas mismas puedan hacer un análisis inicial de su situación tecnológica con aras de la seguridad informática de los procesos notariales y que sirva de guía para la correcta implementación de un sistema tecnológico robusto y fiable.

Partiendo de los casos reales analizados en el presente documento, encontramos temas en común que suceden en varias notarías a nivel nacional en el ámbito tecnológico, pero se encuentra que el quehacer del ingeniero de sistemas, está permeada por el presupuesto minimizado gracias a la contracción económica del país.

9 RECOMENDACIONES

9.1 **Diseño propuesta del manual de seguridad informática**

Desde el ministerio de tic, se desarrolló hace casi una década manuales ingenieriles en pro de la seguridad y confiabilidad ante desastres informáticos, los cuales hacen parte de los repositorios nacionales de información, es imperante tener estos documentos como ejes rectores para las notarías, las cuales necesitan una implementación idónea de sus recursos tecnológicos, por lo cual se desarrolla estas recomendaciones generales.

Es objetivo desarrollar una metodología de autodiagnóstico enfatizada en lo preventivo, donde prime robustecer la estructura tecnológica, cambiando el paradigma de una asistencia enfatizada en la reactividad antes los fallos, dado que al prevenir estos, se puede optimizar los recursos, minimizar los riesgos y ser más asertivos en la implementación de nuevas tecnologías ante las notarías.

El diseño de un manual de auto diagnóstico que sirva como base y guía para las notarías del círculo de Bogotá, es una herramienta fundamental para el mejoramiento continuo de los procesos notariales, además que sirve de tipo ideal para prevenir y evaluar la seguridad de la información dentro de las notarías.

Para el anterior enunciado se plantea la siguiente estructura en le manual de autodiagnóstico de la seguridad de la información en las notarías de bogotá:

10 MANUAL

10.1.1 Levantamiento de información:

Con base en la información inicial podemos tomar medidas preventivas y evaluar la institución, validando sus procesos, tecnologías aplicadas y parametrizar sus prácticas.

1:Reunirse con los gerentes de las notarías, directivos, funcionarios jefes de personal y el staff de tecnología.

Reunión de inicio con los stakeholders en la notaría, el notario, el notario suplente, jefes de personal, gerentes de las notarías, jefe de jurídica.

2: Reunir toda la información necesaria para la toma de decisiones con base en las tecnologías de la información.

Se debe recopilar información necesaria, permitiendo identificar los activos de la información dentro de la notaría, permitir conocer el contexto operacional, organigramas, mapas de procesos tecnológicos, políticas de seguridad , metodologías, manuales de identificación de riesgos, stakeholders dentro de la entidad, para poder evaluar los manuales y hacer una centralización de la identificación de las amenazas.

3:Consolidar un repositorio de información sobre el estado actual, que corresponda a las tecnologías de la información.

Agrupar toda la información para así poder procesarla, debe generarse un repositorio común para toda la información que sirva para la toma de decisiones tecnológicas y la evaluación del autodiagnóstico, puede ser por ejemplo un drive con acceso exclusivo de los stakeholders, aws s3, un servidor de samba, file server, entre otros.

10.1.2 prueba y análisis :

La documentación es el eje inicial, sin embargo muchas de las prácticas dentro de la institución están enmarcadas en documentos inertes, por lo cual es imperante realizar pruebas de ingeniería y un análisis tecnológico a su infraestructura.

4:Pruebas administrativas donde se evidencia la lógica en cuanto a toma de decisiones con respecto a las tecnologías de la información.

Generar un entorno de testeo con los dirigentes de la notaría, para emular la toma de decisiones en cuanto a tecnologías de la información.

5:Pruebas técnicas de toda infraestructura tecnológica, para verificar la seguridad tecnológica dentro de la institución.

Técnicas empleadas para probar la seguridad informática dentro de la entidad, donde se evidencien vulnerabilidades, es necesario realizar manuales o basarse en los existente para realizar las pruebas, dado que hay diferentes tipos de escenarios y test; como lo son el conocimiento nulo. donde se realizan pruebas de testing sin tener conocimiento de la infraestructura, pruebas de conocimiento medio, donde se conoce parte del entorno tecnológico para ser testeado como lo puede ser el conocimiento medio de un funcionario

dentro de la notaria y las pruebas de conocimiento completo, donde se conoce a profundidad el esquema de la notaría y su infraestructura tecnológica.

6:Análisis PHVA(planear, hacer, verificar, actuar).

Analizar el ciclo de vida de la seguridad, Análisis PHVA(planear, hacer, verificar, actuar), el nivel de madurez tecnológico de la notaría con base en el modelo de seguridad.

7:Análisis de la institución con base en las mejores prácticas de la industria del sector, tanto notarial como el sector tecnológico.

Realizar una evaluación interna con base en la información obtenida en los pasos anteriores, donde se contraponga con las mejores prácticas actuales en ciberseguridad del sector notarial como del sector privado.

10.1.3 Informe y recomendaciones:

Dada la importancia de las nuevas tecnologías en el sector notarial, una de las mejores prácticas es informar sobre cada procedimiento, fallo bache de seguridad, por lo cual se plantea el siguiente esquema:

8:Evaluar la madurez sobre el modelo de seguridad y privacidad para la notaría.

Con base en la información obtenida, se puede evaluar la madurez de la notaría ante seguridad de la información y privacidad.

9:Identificar la brecha digital, para así poder solventar los letargos tecnológicos dentro de las notarías con base en la evaluación de donde estamos.

En esta parte del quehacer notarial con base en las tecnologías de la información, se puede plantear un comparativo de la brecha digital que posee la notaría con base en la data obtenida desde el punto uno al nueve, para así poder evaluar su seguridad informática en los procesos notariales.

10: Generar unas recomendaciones para remediar los hallazgos de este proceso, robusteciendo los sistemas de información.

La generación de informes con base en la información obtenida es imperante, dando a lugar a recomendaciones ingenieriles del ámbito de sistemas para la notaría, con base en las vulnerabilidades y hallazgos en los procesos anteriores.

11: Elaborar un plan de seguridad, con fechas claras, responsables de cada proceso, donde se tenga compromiso efectivo de cada una de las partes involucradas.

En esta última parte se pueden implementar informes detallados sobre cómo solventar las brechas de seguridad, responsables de cada proceso dentro de la notaría, generando compromisos en con el notario, jefes de personal y fechas para la solución.

11 AGRADECIMIENTOS

Agradecimiento a mi familia por el apoyo durante los años de carrera, a la universidad Jorge tadeo lozano por su gran formación que me sustentó en el campo laboral y especial; agradecimiento a mis profesores Olmer garcía y Giovanny Ortegon por su orientación oportuna en tan magno proyecto.

12 REFERENCIAS

[1] Amann, Bernhard. 2012. *Extracting Certificates from Live Traffic: A Near Real Time SSL Notary Service*. berkeley, California: International Computer Science Institute,. 10.1.1.475.9665.

[2] Icontec. 2006. *NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001*. 3rd ed. Bogota, Bogota: Icontec. https://www.icontec.org/normas/.

[3] Langston, Mark C. 2003. *Documentation Writing for System Administrators*. N.p.: USENIX Association.

[4] Mintic. 2010. *17 18 19 Guía para la preparación de las TIC para la continuidad del negocio*. 1.0.0 ed. Vol. 1. 1 vols. Bogota, Bogota: Mintic. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

[5] Mintic. 2016. *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.* 1.2 ed. Vol. 1. 1 vols. Bogota, Bogota: Mintic. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

[6] mintic. 2016. *Modelo de Seguridad y Privacidad de la Información Modelo*. 3.0.2 ed. Vol. 1. 1 vols. Bogota, Bogota: mintic. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

[7] mintic. 2016. *Procedimientos De Seguridad De La Información*. 1.0.0 ed. Vol. 1. 1 vols. Bogota, Bogota: MIntic. https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.
[8] Popkova, Elena G., and Bruno S. Sergi, eds. 2019. *Digital Economy: Complexity and Variety Vs. Rationality*. N.p.: Springer International Publishing.
[9] Procolombia. 2017. *Termnos de referencia hosting externo*. Bogota, Bogota: Fiducoldex. https://procolombia.co/.
[10] Super Notariado. 2014. *SISTEMA INTEGRADO DE CONSERVACION – SIC*. Bogota, Bogota: Super Notariado. https://www.supernotariado.gov.co/.
[11] Super Notariado. 2021. *PROYECTO DIGITALIZACIÓN NOTARIAL ANEXO TÉCNICO*. 1.0 ed. Bogota, Bogota: Super NOtariado. https://www.supernotariado.gov.co/prensa/noticias/proyecto-de-resolucion-por-medio-del-cual-se-establecen-los-lineamientos-para-la-prestacion-del-servicio-publico-registral-con-el-uso-de-las-tecnologias-de-la-informacion/.
[12] Super NOtariado. 2021. *PROYECTO DIGITALIZACIÓN NOTARIAL ANEXO TECNICO REPOSITORIO DE PROTOCOLO NOTARIAL*. 1.0 ed. Bogota, Bogota: Super Notariado. https://www.supernotariado.gov.co/.
[13] Super Notariado. 2021. *Resolucion 00013*. Bogota, Bogota: Super Notariado. https://www.supernotariado.gov.co.
[14] Super Notariado. 2021. *Resoluicion 00011*. Bogota, Bogota: Super Notariado. https://www.supernotariado.gov.co.
[15] Super Notariado. 2021. “Resolucion 00012 de 04-01-2021,” Resolucion Notarial. https://www.supernotariado.gov.co/. Digital.

[Anexo 1] Matriz de riesgos informáticos notarías del círculo de bogotá
[Anexo 2] Manual gráfico de auto diagnóstico de seguridad de la información en las notarías del círculo de bogotá