UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERIA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

Estudio de la seguridad informática de la red de datos del Gobierno Autónomo Descentralizado Municipal del cantón Alfredo Baquerizo Moreno "Jujan"

EGRESADO:

Carlos Apolonio Cañar Vera

TUTOR:

Ing. Joffre Vicente León Acurio MIE.

AÑO 2017

1. Introducción

En el Cantón Alfredo Baquerizo Moreno “Jujan”, un gran porcentaje de organizaciones hacen uso de las Redes Inalámbricas, ya sea para su red interna o para el acceso a internet. A pesar de que en la zona algunos Administradores de Redes conocen sobre los tipos de ataques existentes no se toman medidas de seguridad para proteger a las WLAN. Se debe poner mayor énfasis en los mecanismos de cifrado de la información, porque en la mayoría de casos se usan la configuración que esta por defecto. Se deben implementar técnicas de seguridad para proteger la información de las organizaciones.

El nivel de seguridad en la red inalámbrica del Gobierno Autónomo Descentralizado del Cantón Alfredo Baquerizo Moreno “Jujan” y los mecanismos de autenticación utilizados no siempre certifican la completa eficiencia en cuanto a la seguridad de una red inalámbrica. Además, en la Municipalidad se han implementado recientemente puntos de acceso a internet, sin poder en ninguna ocasión analizarlos completamente para comprobar el nivel de seguridad y vulnerabilidad. La información es considerada como un elemento importante en toda organización y la Municipalidad no es la excepción, por esta razón es de suma importancia que llegue a su destino totalmente íntegros.

2. DESARROLLO

EL Gobierno Autónomo Descentralizado del cantón Alfredo Baquerizo Moreno “Jujan”, ubicado en la provincia del Guayas, cantón del mismo nombre, dentro de la cabecera cantonal en las calles Jaime Roldós y José Domingo Delgado, se encuentran las instalaciones del G.A.D.M. Jujan. (SISTEMAS, 2017)

Figura 1 Ubicación G.A.D.M. Jujan / **Fuente**: Google Maps Ubicación del GADM Jujan

El G.A.D.M. Jujan ofrece servicios públicos de ayuda y estrategias para el bienestar del cantón, dentro de las cuales en uno de sus programas se encuentran las redes Wireless gratuitas, que es uno de los principales atractivos en el parque central y en las afueras de las entidades públicas que se encuentran ubicadas dentro del cantón.

El análisis a realizar utiliza una investigación documental ya que permite el estudio de problemas con el propósito de ampliar y profundizar el conocimiento de su naturaleza,

con apoyo, principalmente, en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos.

Dentro de la organización existen 26 departamentos, cada cual cumple una función y tiene como recursos informáticos:

- Computador(es)
- Internet
- Impresora(s)

Los departamentos todos realizan informes diarios, semanales, mensuales, se necesita del internet y de la red para poder compartir las carpetas, archivos, etc.

EL G.A.D.M. Jujan cuenta con una red LAN, consta de 2 routers básicos, 2 switch tp-link básicos de 24 puertos cada uno, cable utp par trenzado categoría 6, con sus respectivos conectores rj-45 de categoría 6.

Según (Raya, 2006) "Una red de computadoras es un sistema de datos interconectados entre equipos que permite compartir varios recursos e información. Por lo cual es necesario contar, con los computadores adecuados, tarjetas de red, cables de conexión, dispositivos periféricos y el software conveniente"

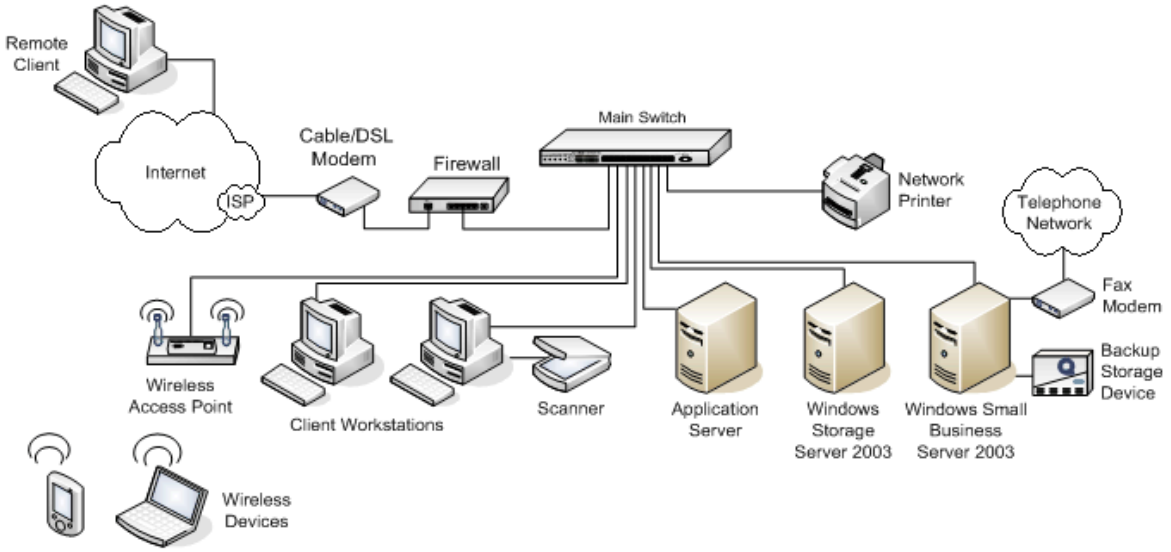
Por qué utilizan una red en el GADM JUJAN

(TANENBAUM, 2003) Menciona que en las organizaciones se cuenta con un gran número de computadoras. Ya que dentro de estas se tienen que llevar diferentes tareas como son: supervisar la producción, controlar inventarios, nomina, etc. Para realizar esto al principio las computadoras trabajaron por separado, pero en algún momento la administración decidió que trabajaran conectadas para correlacionar la información acerca de la compañía y llevar a cabo un mejor trabajo. Es en este momento que surgía la compartición de recursos y el objetivo es que los programas, impresoras, y los datos estén

disponibles para todos los miembros de trabajo. Al compartir recursos dentro de una organización, se logran alta fiabilidad, ahorro de dinero, seguridad y configuración de datos.

Después de lo mencionado, el GADM JUJAN cuenta con una red LAN, su conexión a las maquinas van del router a los dos switch de 24 puertos, del puerto del switch al pc, y al router tp-link de 3 antenas.

Figura 2 (LPS, 2008) ejemplo aproximado de como esta diseñada la red en el GADM JUJAN;/



Fuente: http://www.lps.com.es/index.php?carga=software_cc_2010_pro_caract;

Después de observar en la figura 2, vemos que la red LAN del GADM JUJAN, se puede entender mucho ahora hablemos de la red LAN:

De acuerdo con (wordpress, s.f.) Las redes de área local (generalmente conocidas como LANs) son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información.

Según (Pineda Mejillones, 2015)Políticas de Seguridad de la Red: Una política de seguridad es un conjunto de normas que rigen el comportamiento de una red de computadoras en relación a la seguridad. Es por eso que lo primordial es establecer los recursos disponibles en la red para establecer reglas de qué es lo que se puede y debe hacer por parte de los usuarios (internos y externos) con estos recursos. La seguridad en las redes debe empezar desde el acceso físico a los equipos o componentes de la red. Por lo general existe un centro de cómputo en el que se encuentran los equipos de conectividad como lo son los ruteadores (routers), conmutadores (switches) y concentradores (hubs), los servidores (Web, FTP, Proxy, Mail, base de datos, etc.) y los equipos de protección (firewalls, IDS, etc.). Esta área siempre es considerada crítica para cualquier empresa, por lo tanto, una de las primeras medidas es restringir el acceso físico al área solo a personal debidamente autorizado.

Según (Pineda Mejillones, 2015)Una red segura es aquella capaz de ofrecer típicamente las siguientes características:

- Confidencialidad: Este concepto está orientado a los datos, es decir, la información debe mantenerse reservada dentro de los límites de la empresa. Para mantener el nivel de confidencialidad se recomienda como solución la encriptación de la data.
- Integridad: El nivel de integridad de los datos se rige en los parámetros de información completa y exacta. Ambos factores son críticos después de haber manipulado los datos. Una medida de seguridad típica es el uso de firmas digitales, permisos de acceso a los archivos o carpetas a nivel de sistemas operativos.
- Autenticación: Es decir, buscar asegurar que sólo los usuarios autorizados tengan acceso a los datos y/o servicios. Como soluciones típicas se suele implementar las claves de acceso, sistemas de acceso biométrico, por citar algunos ejemplos.

Según (Pineda Mejillones, 2015)Tipos de vulnerabilidades en redes de computadoras: La causa típica de las redes con seguridad inadecuada es la falla en la implementación de políticas de seguridad y en el mal o nulo uso de herramientas que estén disponibles. Es vital que las empresas desarrollen planes operativos de seguridad y respuesta a eventos relativos.

Existen tres principales problemas que tienen que ver con la seguridad en una red de computadoras:

- Debilidad en la tecnología: Cada tecnología de redes y de computadoras tiene inherentes problemas de seguridad.
- Debilidad en la configuración—Hasta la tecnología más segura, cualquier deficiencia en la configuración o en el uso puede representar problemas de seguridad.
- Debilidad en las políticas—Una pobre definición o inapropiada implementación en la administración de políticas de seguridad puede convertirse en una fuente para el ingreso de usuarios no autorizados a los recursos de la red.

Ahora ya que estamos empapados en el tema me enfocare a unos de los mayores problemas de esta organización, compartir información: dentro de la red, se hace uso de compartir información para que dentro de cada departamento pueda ser utilizada de la forma más rápida, pero con el riesgo de que su fiabilidad y sus datos puedan ser modificados ya que no cuentan con normas o reglas apropiadas para su debida seguridad.

El ejemplo más crítico que se pudo observar dentro de la organización (contada por el Ing. Marcos Molina Sánchez, jefe encargado del departamento de Sistemas) que el alcalde había compartido la información de los sueldos para tesorería y alguien tomó ese documento y lo modificó, ¿descubrieron quién lo hizo?, ¿descubrieron si fue un empleado?, ¿Quién fue?, puesto a que el caso era critico el alcalde mandó a revisar toda la red y se descubrió que se duplicaban los router: hacen un “espejo”, los dos routers tplink

son de la misma marca y el mismo modelo, las configuraciones se duplicaban y con en la red existe otro routers que esta de modo libre (sin contraseña), para que puedan acceder empleados del GADM JUJAN, usuarios, ciudadanos en general.

Según (Pineda Mejillones, 2015)Desde esta perspectiva el realizar pruebas de vulnerabilidades y de detección de intrusos son partes necesarias de la infraestructura de seguridades, pero no representan por ellas mismas una infraestructura completa de seguridad.

Figura 3 (TPLINK, 2017), conexiones de router / Fuente: de tplink.es

De allí el problema la red inalámbrica libre se duplica las mismas configuraciones y se tienen acceso a las carpetas compartidas que como antes mencionamos no cuentan con normas o reglas de seguridad de la información como la norma ISO27001, puesto a el problema que sucedió con lo de los sueldos, fue por medio del acceso al router, que con conocimientos básico de informática sustrajeron la información que se compartida por medio de la red, se conecta con una laptop al router libre, te conectas a una unidad de red y aparece toda la información de las carpetas compartidas, genial verdad ¿suena difícil?, incluso jugaban con los cambios de clave en los dos routers y dejaban sin comunicación a maquinas que se conectaban por medio de Wireless, dentro del router libre se manejaban las siguientes configuraciones que la dejaban por default:

Puerta de enlace predeterminada: 192.0168.0.1

Usuario: admin

Contraseña: admin

De Acuerdo (Corletti Estrada , delitosinformaticos.com, 2007)Control de acceso a redes: Todos los servicios de red deben ser susceptibles de medidas de control de acceso; para ello a través de siete controles, en este grupo se busca prevenir cualquier acceso no autorizado a los mismos. Como primera medida establece que debe existir una política de uso de los servicios de red para que los usuarios, solo puedan acceder a los servicios específicamente autorizados. Luego se centra en el control de los accesos remotos a la organización, sobre los cuales deben existir medidas apropiadas de autenticación.

Según (Corletti Estrada , delitosinformaticos.com, 2007)Un punto sobre el que merece la pena detenerse es sobre la identificación de equipamiento y de puertos de acceso. Este aspecto es una de las principales medidas de control de seguridad. En la actualidad se poseen todas las herramientas necesarias para identificar con enorme certeza las direcciones, puertos y equipos que pueden o no ser considerados como seguros para acceder a las diferentes zonas de la empresa. Tanto desde una red externa como desde segmentos de la propia organización. En los controles de este grupo menciona medidas automáticas, segmentación, diagnóstico y control equipamiento, direcciones y de puertos, control de conexiones y rutas de red. Para toda esta actividad se deben implementar: IDSs, IPSs, FWs con control de estados, honey pots, listas de control de acceso, certificados digitales, protocolos seguros, túneles, etc.… Es decir, existen hoy en día muchas herramientas para implementar estos controles de la mejor forma y eficientemente, por ello, tal vez este sea uno de los grupos que más exigencia técnica tiene dentro de este estándar.

Acceso al router, acceso a todo los documento que se comparten en la red del GADM JUJAN, este problema viene surgiendo desde ya hace 2 años cuando la red se implantó y ha ocasionado graves problemas para el alcalde, empleados, trabajadores y usuarios de la red que se benefician con la utilización de los recursos compartidos.

La seguridad de las redes inalámbricas siempre ha sido un tema muy complicado, ya que el error de las personas que trabajamos en los procesos de normas de seguridades en las redes inalámbricas no tomamos en cuenta de cierta forma normas o reglas que ya rigen según la norma ISO 27001, dentro de los problemas en la red del Gobierno Autónomo Descentralizado del Cantón Alfredo Baquerizo Moreno "JUJAN", uno de los principales descuidos es no implementar normas o reglas para los trabajadores, cuando comparten información sin ninguna contraseña de seguridad, nos centraremos en la red de datos, la red de datos del GADM JUJAN.

Existen problemas de conectividad punto a punto, ya que ningún punto tiene una señalización o un nombre de los departamentos, cada enlace tiene una conexión con un cable de categoría 6, la red es muy difícil de manejar, los dispositivos están todos conectados entre sí, 3 router muchos cables, conexiones de punto a punto fallidas, utilización de páginas web no pertenecientes al campo laboral (redes sociales, videos) lo cual hacen que la banda ancha asignada se acorte.

Según (Pineda Mejillones, 2015)En la actualidad se puede probar la confiabilidad de un sistema realizando pruebas de detección de vulnerabilidades en una red y pruebas de detección de intrusos. Existen diferentes tipos de herramientas (las mismas que utiliza un hacker) para realizar esta evaluación, es lo que se conoce como ethical hacking. Este es un concepto que se puede definir como "Probar los diferentes métodos que un pirata informático puede seguir para dañar a la red, antes de que realmente lo haga". La infraestructura de seguridad es el complemento de las medidas, políticas, procedimientos

y prácticas a las tecnologías y productos que representan una iniciativa de seguridad de la organización. El éxito de estas medidas es principalmente detectar los problemas para retardar el daño y para mitigar los efectos de los errores y ataques.

El nivel de seguridad de la red inalámbrica del GADM JUJAN, y los mecanismos de autenticación utilizados no siempre certifican la completa eficiencia en cuanto a la seguridad de una red inalámbrica, además en la Municipalidad se han implementado recientemente puntos de acceso a internet sin poder en ninguna ocasión analizarlos completamente para comprobar el nivel de seguridad y de vulnerabilidad. La información es considerada como un elemento importante en toda organización y la municipalidad no es la excepción, por esta razón es de suma importancia que llegue a su destino totalmente integra.

Según (Pineda Mejillones, 2015)Existe gente técnicamente calificada que ansiosa espera tomar ventaja de las debilidades en la seguridad de redes y continuamente descubrir nuevas brechas de seguridad. A continuación, se explica con mayor detalle cada una de los problemas descritos anteriormente.

El mal manejo en seguridades de las redes inalámbricas existentes, políticas de seguridades antiquísimas, información filtrada por medio de terceras personas que obtienen acceso a los router.

(BERTOLIN, 2008)Dentro de este documento hablemos de la seguridad Informática siempre no debe solucionar los posibles problemas encontrados, debe informar procesos que de alguna forma afecte la seguridad de la información que se localice dentro de los sistemas de información empresariales

De acuerdo a este caso de estudio nombraré algunos puntos y temas que nos ayudaran a identificar algunas terminologías:

Dentro del ámbito guardaremos este concepto de información para recordarles que es un activo de los más importantes dentro de la organización.

De acuerdo con (RODRÍGUEZ RODRÍGUEZ & DAUREO CAMPILLO, 2003) La información, en su acepción más corriente, es el resultado de conocer hechos y, o, acontecimientos, sus causas y sus consecuencias. (NOY GOMEZ, 2017)"Desde el punto de vista de la ciencia de la computación, la información es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del ente que posee dicha información con su entorno".

Según la revista (welivesecurity, 2015)La información debe ser el bien más importante en toda las empresas en especial a la de esta organización, para esto presentaremos el debido informe de este estudio para poder ayudarles en lo que más se pueda a la organización para que puedan corregir a tiempo todas las falencias posibles detectadas en especial el error de duplicidad de router y al compartir archivos, cuando se busca proteger el hardware, redes, software, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la seguridad informática o ciberseguridad. Cuando se incluyen actividades de seguridad relacionadas con la información que manejan las personas, seguridad física, cumplimiento o concientización nos referimos a seguridad de la información.

Según (Dejan, 2017)El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

De acuerdo (ISO/IEC 27001, 2013) Control de acceso a información y aplicaciones: En este grupo, los dos controles que posee están dirigidos a prevenir el acceso no autorizado a la información mantenida en las aplicaciones. Propone redactar, dentro de la política de seguridad, las definiciones adecuadas para el control de acceso a las aplicaciones y a su vez el aislamiento de los sistemas sensibles del resto de la infraestructura. Este último proceder es muy común en sistemas críticos (Salas de terapia intensiva, centrales nucleares, servidores primarios de claves, sistemas de aeropuertos, militares, etc.), los cuales no pueden ser accedidos de ninguna forma vía red, sino únicamente estando físicamente en ese lugar. Por lo tanto, si se posee alguna aplicación que entre dentro de estas consideraciones, debe ser evaluada la necesidad de mantenerla o no en red con el resto de la infraestructura.

Según (Dejan, 2017)Las medidas de seguridad (o controles) que se puedan implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Según (Dejan, 2017)Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad

de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

De acuerdo (ISO/IEC 27001, 2013) Seguridad en los sistemas de archivos: La Seguridad en los sistemas de archivos, independientemente que existan sistemas operativos más robustos que otros en sus técnicas de archivos y directorios, es una de las actividades sobre las que se debe hacer un esfuerzo técnico adicional, pues en general existen muchas herramientas para robustecerlos, pero no suelen usarse. Es cierto que los sistemas de archivos no son un tema muy estático, pues una vez que un sistema entra en producción suelen hacerse muchas modificaciones sobre los mismos, por esto último principalmente es que una actividad que denota seriedad profesional, es la identificación de ¿Cuáles son los directorios o archivos que no deben cambiar y cuáles sí? Esta tarea la he visto en muy, pero muy pocas organizaciones, y puedo asegurar que es una de las que mayores satisfacciones proporciona en el momento de "despertar sospechas" y restaurar sistemas. Suele ser el mejor indicador de una actividad anómala, si se ha planteado bien el interrogante anteriormente propuesto. Si se logra identificar estos niveles de "esteticidad y cambio" y se colocan los controles y auditorías periódicas y adecuadas sobre los mismos, este será una de las alarmas de la que más haremos uso a futuro en cualquier etapa de un incidente de seguridad, y por supuesto será la mejor herramienta para restaurar un sistema a su situación inicial.

Dentro de este caso, se trata que la información sea segura dentro de los niveles de seguridad que se pueda proveer por medio de claves y accesos no libres, debemos saber que implementando normas técnicas como la ISO27001 y las seguridades en los routers para que no tengan terceras personas un libre acceso de la información que circula dentro de la red.

En la red del GADM JUJAN, las falencias encontradas en sus puntos más importantes:

robo de información, datos y falta de distribución de la banda ancha, por falta de normas, estándares o políticas de seguridad que afiancen la seguridad de la información.

CONCLUSIONES

Entre las principales conclusiones que se pueden obtener de esta investigación, se encuentran:

Se necesita establecer normas o reglas que ayuden a mejorar la situación y los conflictos dentro de la organización.

Los encargados del departamento de sistemas deben adaptarse y establecer estándares y protocolos para una mejor situación de la red informática.

Las carpetas o archivos compartidos deben realizarse de una forma que cada archivo que contenga, llegue a su destinatario.

La utilización de correos institucionales, aplacaría un poco con los documentos compartidos vía red informática.

La implementación de nuevas normas y más atención que se debe implementar en esta organización, para que los recursos compartidos sean más seguros.

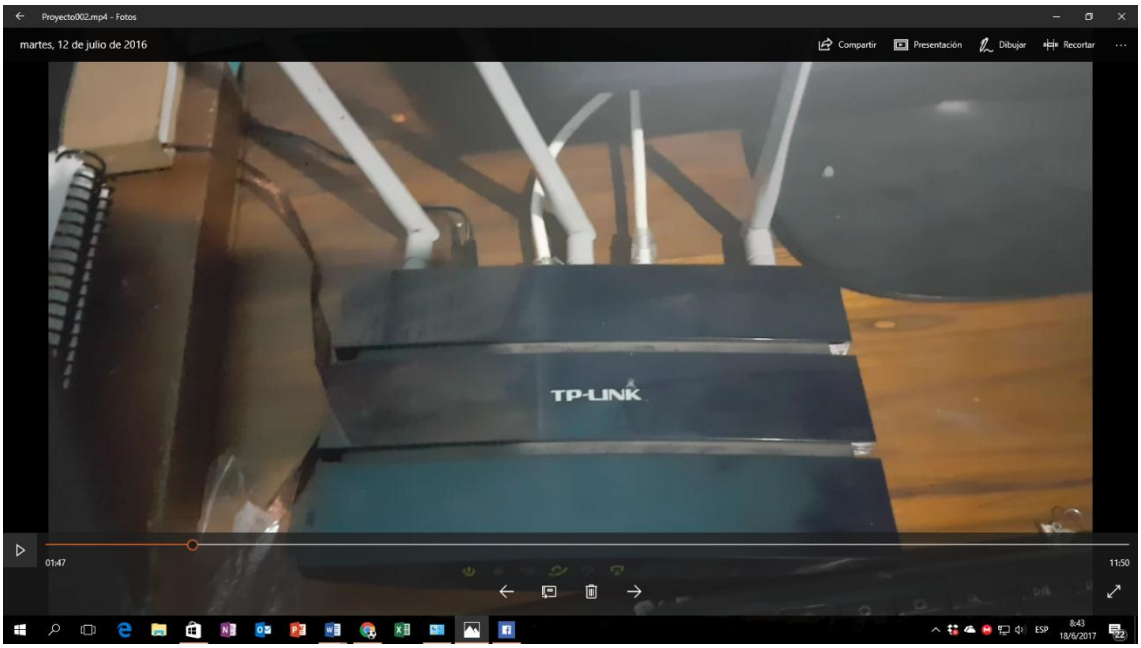
Se debe utilizar equipos más robustos para las conexiones, equipos corporativos ya que se está utilizando equipos domésticos, y esto facilita las cosas a los intrusos.

Este estudio también permitirá experimentar a los del departamento de sistemas que cada día se aprende más de las normas, que se deben tener en cuenta siempre antes de implementar una red, equipos indicados, personal capacitado, tener a la seguridad como un factor muy importante en el ambiente familiar, corporativo y doméstico.

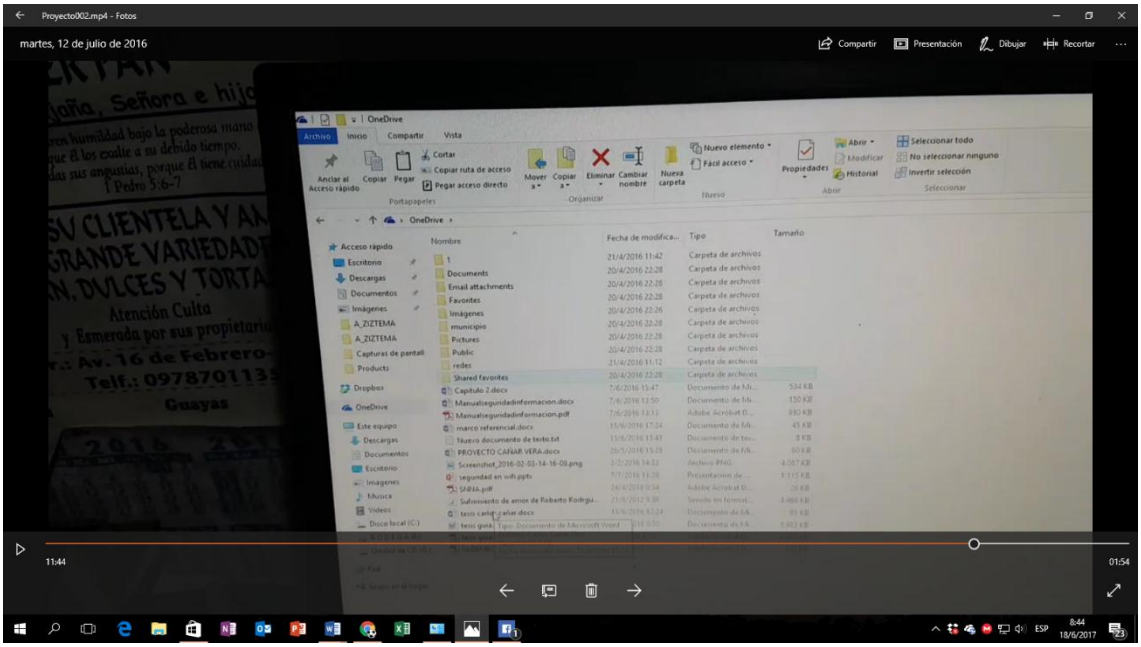
4. Anexos

Switch y conexiones

Ataque por medio de una laptop a la red

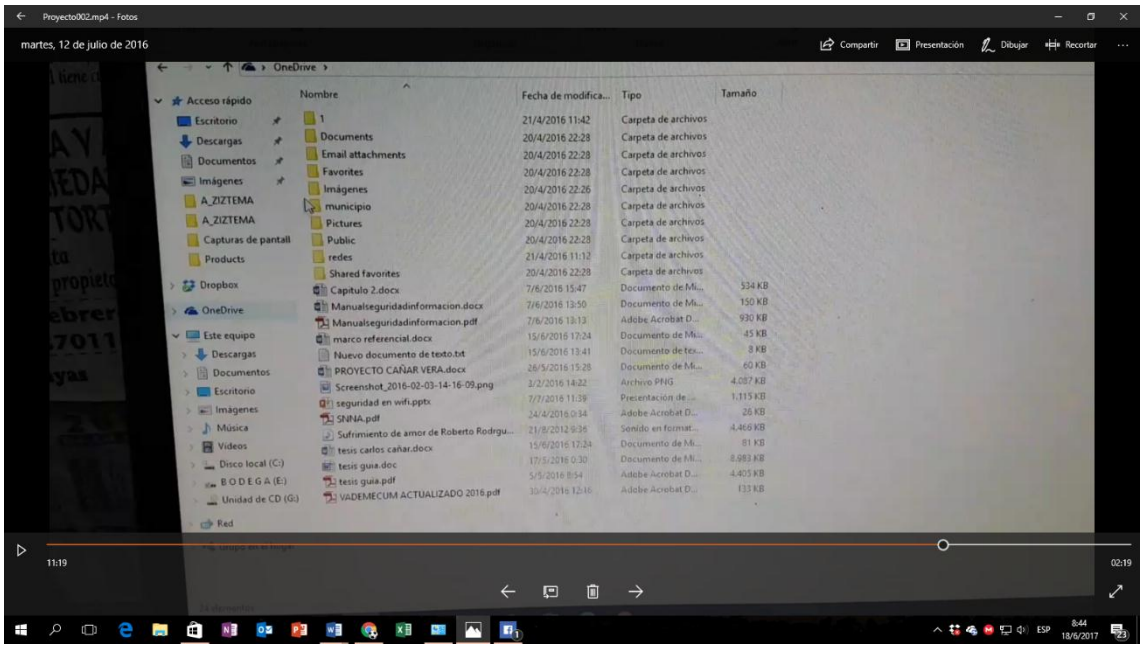


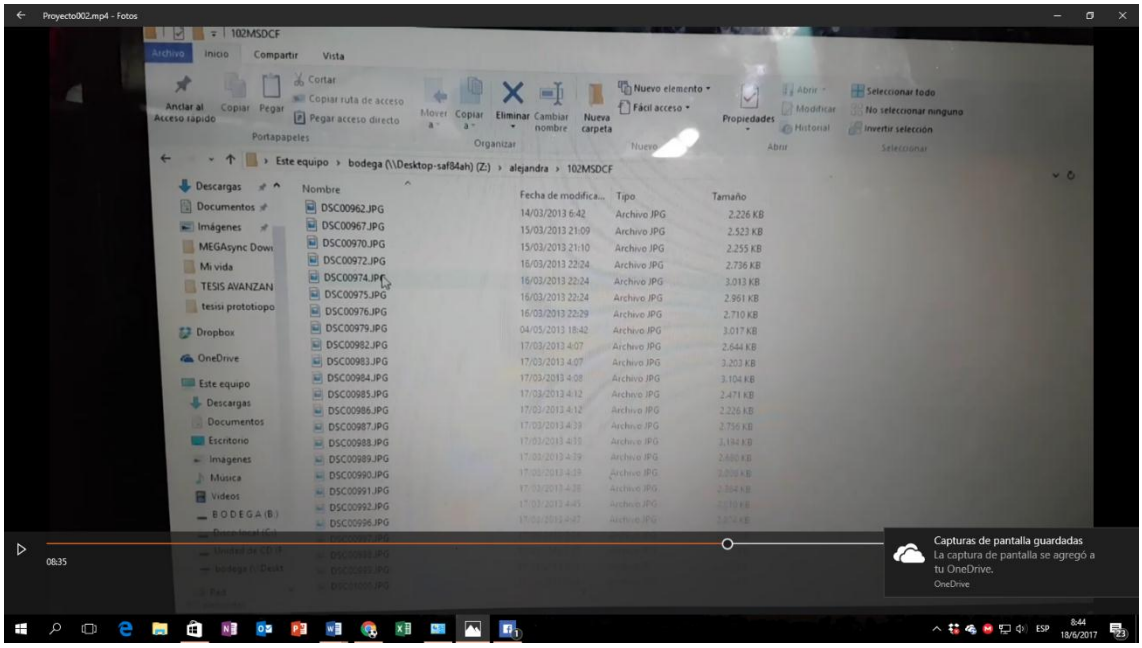
Router tp-link, utilizado en la organización.



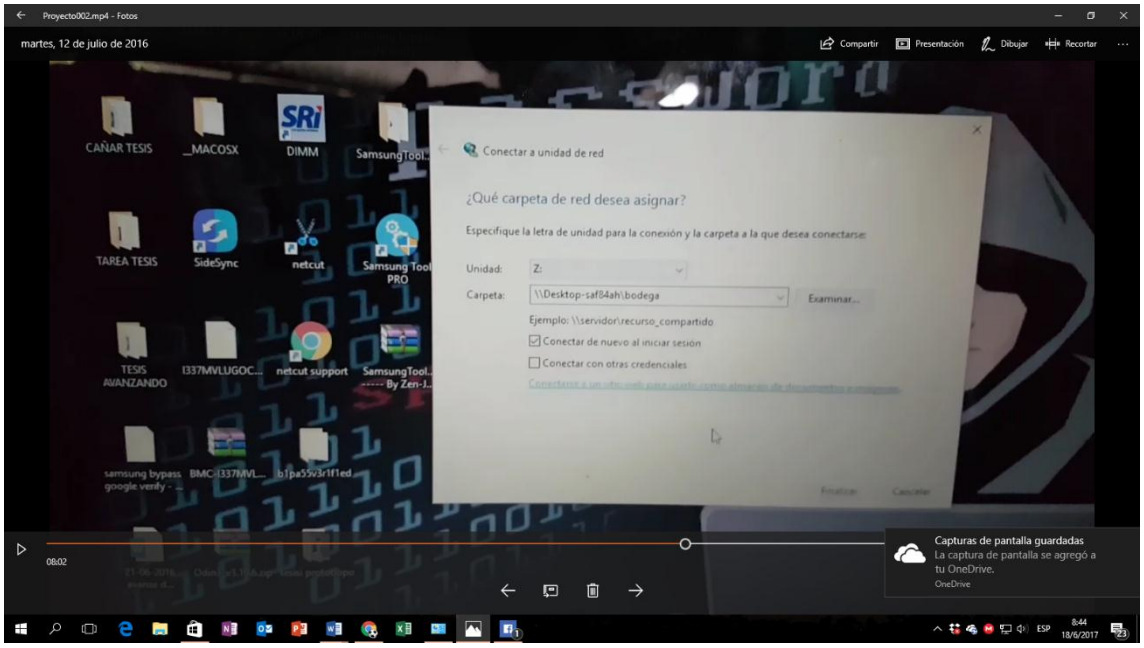
Carpetas compartidas en la red.

Carpetas compartidas en la red



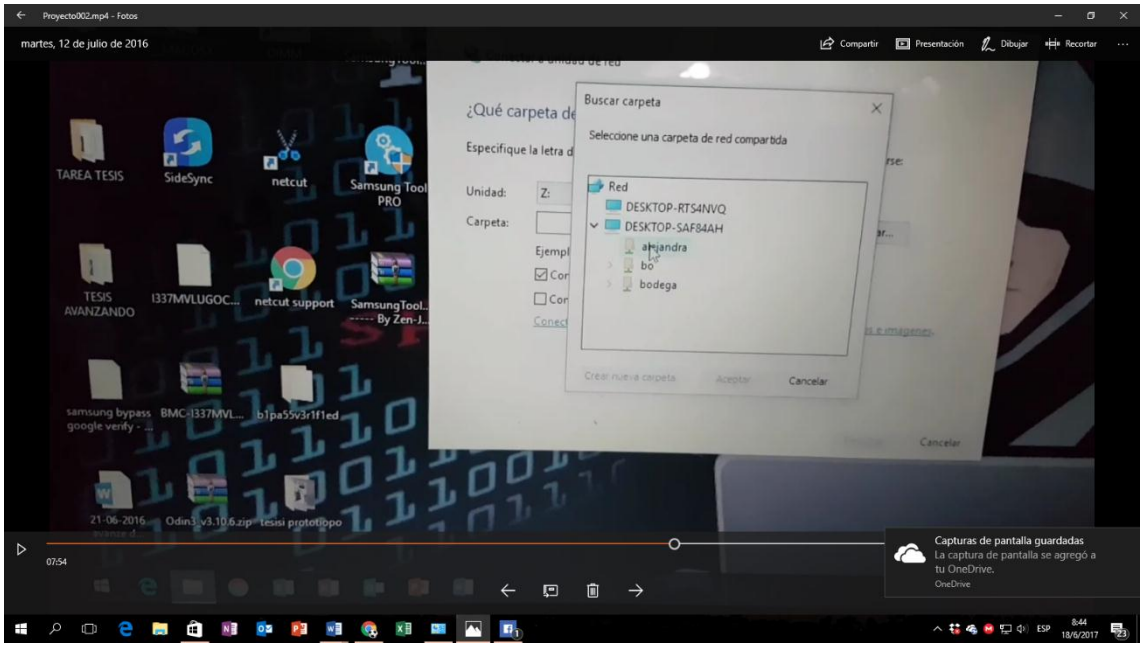


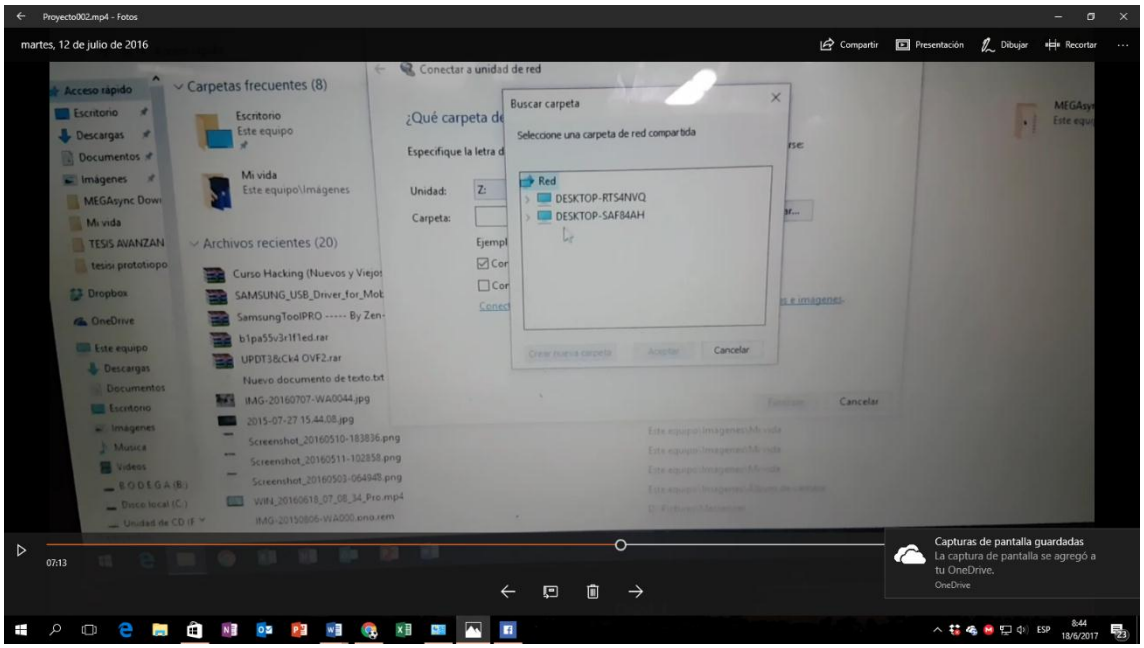
Documentos compartidos en la red.



Conexión a las unidades de red compartidas

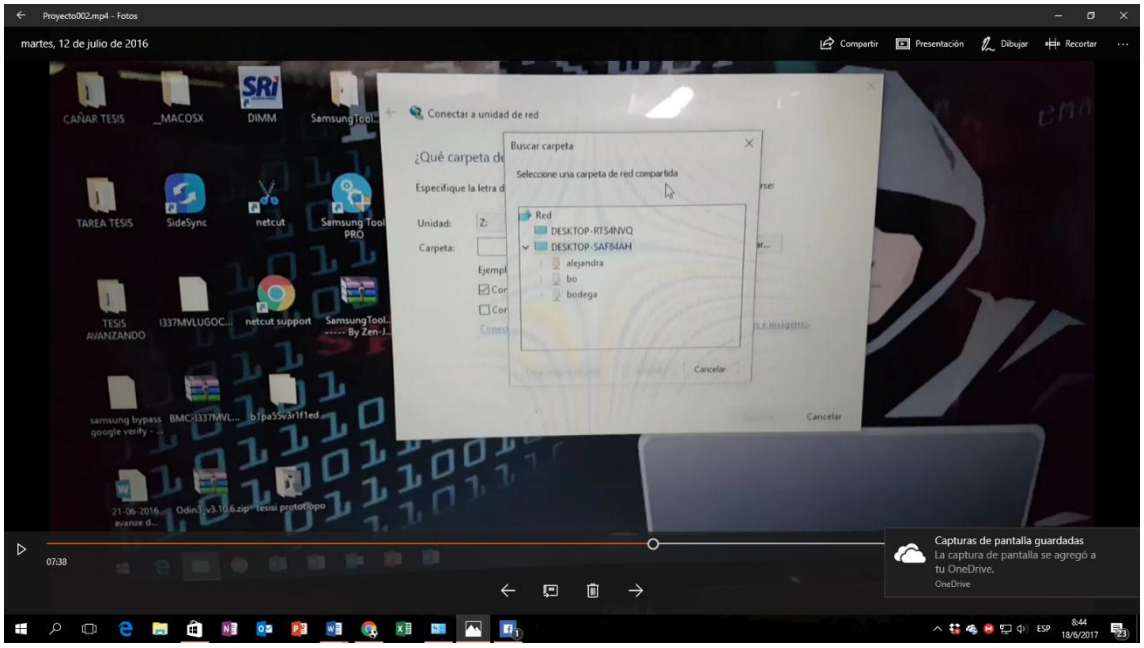
Conexión a las unidades de red compartidas





Conexión a las unidades de red compartidas.

Elección de carpetas compartidas, en la unidad de red.



Los recursos ya en la maquina intrusa, con todos los documentos t carpetas compartidas.