LA CIBERSEGURIDAD ES CLAVE EN EL ÉXITO EMPRESARIAL.

AUTOR:

TANIA VALENTINA PULIDO PULIDO 1401329

TUTOR:

LEONARDO JUAN RAMÍREZ LÓPEZ

FACULTAD DE INGENIERÍA

UNIVERSIDAD MILITAR NUEVA GRANADA

INGENIERÍA EN TELECOMUNICACIONES

BOGOTÁ D.C

2 DE DICIEMBRE DE 2022

LA CIBERSEGURIDAD ES CLAVE EN EL ÉXITO EMPRESARIAL.

INTRODUCCIÓN.

En los últimos años, la ciberseguridad se ha convertido en una herramienta muy importante debido a que el avance en la tecnología obliga a entregar datos personales a las distintas entidades y empresas ya sean públicas o privadas, tales como entidades financieras, de manejo de datos e información personal, los entes jurídicos y de control para poder acceder a bienes y servicios de todo tipo, esto genera que no se pueda tener control de esta información y que cualquier organización, institución o persona pueda acceder con facilidad a los mismos. Teniendo en cuenta los riesgos que trae consigo la falta de control de los datos se deben tomar medidas de precaución desde lo básico en lo personal como por ejemplo no entregar la información de tipo financiero, como los datos de las tarjetas de crédito y débito, o cualquier tipo de contraseñas personales de acceso a sistemas y entidades en donde manejemos información importante ya sea laboral o institucional, de carácter privado y de proyectos, programas e inclusive ideologías de tipo religioso o político que puedan ser usadas en contra nuestra en un eventual proceso penal, fiscal, disciplinario o simplemente para desacreditar o empañar el buen nombre con propósitos maliciosos o como medio de venganza o retaliación (Cando-Segovia, M. R., & Chicaiza, R. P. M. (2021)).

La implementación de la ciberseguridad ha sido todo un reto para las empresas, esta se define como el área encargada de preservar diferentes redes, sistemas y programas de los ciberataques; estos ciberataques son acciones contra sistemas de información que tienen como fin acceder a los datos ya sean personales, empresariales, comerciales o financieros y a través de ellos deshonrar, calumniar, desprestigiar y en muchas ocasiones hurtar recursos e información que pueda beneficiar al atacante (Manuel, J., & Aguilar, A. 2020).

Algunos preliminares. A continuación, se presentan algunos conceptos importantes para la óptima comprensión de este escrito.

-Ciberseguridad: Se define como la actividad encargada de proteger redes, sistemas y programas de ciberataques (*Cisco*, 2022).

-Ciberataque: Ataque organizado por personas maliciosas en contra de un sistema informático que apuntan a acceder de manera ilegal a un sistema, modificar o robar los datos confidenciales de personas o empresas (*Cisco*, 2022).

-Virus informático: Programa malicioso que se mete en los dispositivos sin previo aviso o permiso, estos se caracterizan por propagarse rápidamente por todo el sistema (Avast, 2022).

-Antivirus: Es un software que brinda protección y seguridad a los diferentes sistemas contra ataques virtuales, identificándolos y eliminándolos (Arias Cardona, D, 2022)

-Cortafuegos: Parte de un sistema informático que se encarga de detectar y bloquear el acceso que no ha sido autorizado de un equipo a la red (Tello Baquero, K. I., & Freire Cobo, L, 2020).

-Pirata informático: Persona que tiene muchos conocimientos sobre sistemas informáticos y que los usa con el fin de atacar a otros (Esquivel, N. S. 2022).

-Tipos de amenazas: Existen cuatro principales tipos de amenazas que son ***phishing, ransomware, malware*** **e ingeniería social.** La primera también conocida como suplantación de identidad consiste en el envío de correos electrónicos engañosos que se parecen a los de las fuentes originales con el fin de realizar robo o manipulación de información, es de los ataques cibernéticos más comunes, el ejemplos más típico es el hurto de datos de tarjetas de crédito, teniendo como fin provocar problemas financieros a la víctima. El segundo, ***ransomware*** o secuestro de datos, realiza encriptación de la información de la víctima para después pedir un rescate en muchas ocasiones monetario. El tercero, ***malware*** consigue acceso sin autorización a un equipo y puede causar daños irreparables al mismo. Por último, la **ingeniería social** es una combinación de las amenazas anteriores que tiene como objetivo que la víctima dé clic en un enlace para perjudicar por medio del malware, solicitar un rescate y hacer creer que es una fuente confiable (Olmedo, J. I., & Gavilánez, F. L, 2018). Estos ataques se pueden clasificar en dos, externos e internos según sea el caso, los externos se caracterizan en ser más difíciles de realizar, ya que se necesita buscar la manera de conocer la red para saber cómo atacar, en cuanto a los internos suele ser un ataque más serio y complicado ya que es realizado por personas que conocen la red y su funcionamiento, esto genera que pueda ser peor y traer consecuencias irreparables para la empresa (Escalante Quimis, O. A, 2021).

-Industria 4.0: Tuvo sus inicios en el año 2011, esta surgió viendo la necesidad de la industria de generar cambios y avances tecnológicos para hacer la vida de los usuarios más sencilla, automatizada y poder suplir sus necesidades, se caracteriza por tener más dispositivos inteligentes, abarcar conceptos como macrodatos también conocido como big data, Internet de las cosas - IoT (por sus siglas en inglés, Internet Of Things), inteligencia artificial - IA (por sus siglas en inglés, artificial intelligence), realidad aumentada, computación en la nube, ciberseguridad, entre otros. La cuarta revolución industrial se puede definir como el modelo de automatización de diferentes sistemas al día de hoy. La ciberseguridad al hacer parte de la nueva revolución industrial permite que las empresas que la implementan automáticamente puedan ser parte de la industria 4.0 (Basco, A. I., Beliz, G., Coatz, D., & Garnero, 2018).

LA CIBERSEGURIDAD EMPRESARIAL.

La ciberseguridad pretende cuidar los datos e integridad de las personas y empresas, para esto cuenta con un gran campo normativo necesario para alcanzar el éxito en las empresas, como lo es la normatividad de la Organización Internacional de Normas –ISO por sus siglas en inglés (International Organization for Standardization) adoptado por las Normas Técnicas Colombianas -NTC, NTC/ISO27001:2013, esta genera muchos beneficios, como por ejemplo la reducción de posibilidades de vulneraciones de seguridad digital, confidencialidad de la información, minimización de peligros de Tecnología de la Información -TI, ventaja competitiva a nivel de mercado, aumenta la confianza a socios y clientes, cumplimiento de requisitos internacionales, detección sistemática de vulnerabilidades, reducción de costos y el control de riesgos de Tecnologías de la Información (Cazar, J. C. Y., & Contero, C. V. N. 2022).

Con el aumento del número de transacciones realizadas según (Cajamarca, I., & Villa, C. F., 2021) al mes se hacen 35 millones de transacciones por medio de Pago Seguro Electrónico -PSE, es necesario la creación de estándares para la protección de datos de estas transacciones virtuales y físicas, es por esto que se requiere una normativa para la protección de estos datos como lo es el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago -PCI/DSS del año 2004 por sus siglas en inglés (Payment Card Industry Data Security Standard), el cual ayuda a las empresas con controles estrictos para el amparo de los datos sensibles de las

transacciones que se realicen y aumentar la certidumbre de los usuarios para comprar en sus comercios (Universalpay, 2021). Uno de los sectores que maneja datos confidenciales acerca de la reputación de las personas es el sector médico, en el que se deben establecer medidas para la divulgación de información, uno de los estándares de este sector es la Ley de Responsabilidad y Portabilidad del Seguro de Salud -HIPAA del año 1996 por sus siglas en inglés (Health Insurance Portability and Accountability Act) (Sabatino, C. 2021), se encarga de proteger la privacidad y acceso al expediente médico, para el que se establecen una serie de estándares para proteger la información privada que se guarda o transfiere de forma electrónica, la normativa HIPAA se encarga de proteger el derecho a la privacidad de los datos, una correcta implementación de esta normativa permite que se mantenga un alto nivel de reputación para la prestación de los servicios médicos, sin embargo existen algunos vacíos en esta normativa respecto a quienes y en qué casos se permite el acceso a esta información y que puede ocasionar fracasos en empresas de este sector (Laval, C. 2022).

El cumplimiento normativo cuenta con múltiples estándares a nivel mundial como lo son NTC/ISO27001:2013, PCI/DSS e HIPAA, sin embargo a nivel territorial cada país cuenta con políticas enfocadas para la protección de la información, para la república de Colombia se cuenta con el Consejo Nacional de Política Económica y Social -CONPES 3995 del año 2020, de la política nacional de confianza y seguridad digital en el que se busca fortalecer la capacidad en materia de la seguridad digital de los ciudadanos en el sector privado o público y aumentar la confianza en el manejo de la información digital del país, es por ello que las empresas que no cumplan con estándares en materia de ciberseguridad pueden llegar a incurrir en sanciones que pueden llegar a causar el fracaso de una empresa (Conpes 3995, 2020).

ESTUDIO DE CASOS.

A continuación, presento algunos casos de grandes empresas del mundo que han sido atacadas cibernéticamente, como es el caso de playstation, apple y google.

-**En el primer caso,** Sony ha tenido varios ataques de denegación de servicios -DDOS por sus siglas en inglés (Distributed Denial of Service) que consisten en el uso de diferentes sistemas secuestrados para atacar a otro, este constante envío de datos logra que los recursos del servidor sean insuficientes y genera que el sistema

colapse y deje de funcionar (De la Rosa Téllez, M., Reyes, M. A., & Pérez, A. C, 2021), ataque realizado a ***playstation networks*** plataforma creada por Sony para la venta de diferentes contenidos digitales accesibles por medio de los sistemas de playstation 3, 4 y 5, estos ataques han sido enviados a los servidores de red de playstation -PSN por sus siglas en inglés (playstation network), lo cual generó problemas a sus usuarios, Sony en su momento puso un anuncio de que se encontraba en mantenimiento, lo cual era muy extraño para sus clientes pues no hubo un previo aviso de esto, finalmente no pudo ocultar el ataque y se disculpó por no tener una medida preventiva y así poder garantizar a sus clientes un buen servicio (Rivera, N, 2014).

-**Segundo caso,** en el año 2020 Apple empresa pilar en creación de equipos eléctricos, software, hardware y servicios en línea, fue víctima de un ataque de phishing que apuntó al servicio ***iCloud de Apple*** y pudo obtener acceso a las fotos, videos y otra información personal de los usuarios (Hickling, J, 2022).

-**Como tercer caso**, en junio del año 2022 Google, empresa especializada en servicios y productos relacionados con el internet, bloqueó el mayor ataque DDoS que ha existido, el cuál tuvo una cumbre de 46 millones de solicitudes por segundo. Para dar una noción de la magnitud del ataque, es como recibir todas las solicitudes diarias a Wikipedia en 10 segundos (Erard, G, 2022).

PLANTEAMIENTO.

Desde mi punto de vista es muy importante proteger la información y datos personales, al igual que la protección de estos dentro de las empresas, y organizaciones e instituciones ya sean públicas o privadas puesto que cada una de ellas tiene un objeto social dependiendo de su función, del propósito comercial o industrial a la cual se dedique y que por obvias razones debe cuidar su información y sus datos debido a que puede ser objeto de ataques cibernéticos como medio de desprestigio o simplemente para robar información importante en cuanto a fórmulas, o procesos industriales y organizacionales que puedan afectar la productividad, la competitividad y destruir su buen nombre, su trayectoria, e inclusive su estabilidad económica y financiera.

Por esto, las empresas requieren implementar un sistema de protección, control y vigilancia permanente y seguro, para lo cual deben conformar un equipo humano y técnico suficientemente capacitado y perfilado adecuadamente para contrarrestar a

través de un trabajo permanente y confiable los posibles ataques o la pérdida de información importante para la sostenibilidad, la seguridad en todo su proceso administrativo y productivo, y garantizar que la empresa se desarrolle adecuadamente con el fin de lograr los objetivos para los cuales ha sido conformada y proyectarse al futuro con seguridad. Un óptimo sistema de ciberseguridad se conforma de un equipo técnico y profesional especialista en estas labores, también en la instauración de medidas y certificaciones normativas de ciberseguridad y contar con sellos de calidad que puedan garantizar el funcionamiento de todo el sistema. También es importante capacitar constantemente a los miembros del equipo con el fin de mantener los conocimientos actualizados, tener diferentes métodos de autenticación para así lograr que los datos estén más blindados y hacer uso de la nube para tener copia de seguridad de los datos de la empresa. Las empresas que carecen de un óptimo sistema de ciberseguridad son vulnerables a los ataques informáticos y están expuestas a ser desprestigiadas, calumniadas, a que se les hurte o manipule su información confidencial siendo blanco fácil de otras empresas con objetivos sociales y productivos similares que a través de ello puedan ser llevadas a la quiebra por la manipulación maliciosa de su información y la competencia desleal que esto podría provocar en contra de sus intereses de productividad, económicos y financieros.

Al aplicar la norma NTC/ISO27001:2013 se podrían evitar incidentes de seguridad, por lo cuál la inversión en certificaciones normativas de ciberseguridad es excelente para el progreso exponencial de una empresa. Las instituciones certificadas en esta norma evitan riesgos de seguridad informática y están preparadas para un posible ataque por parte de personas maliciosas que tienen como objetivo perjudicar de manera crítica la empresa ya sea robando o manipulando información. Algunas de las razones por las cuales las empresas no tienen la certificación de la NTC/ISO27001:2013 es el costo y que requiere un seguimiento constante, pero si nos ponemos a analizar, cuesta más solucionar un ataque que puede acabar con la empresa, que evitarlos haciendo uso de la normativa en ciberseguridad. Con respecto a el estándar -PCI/DSS considero que es de las certificaciones más importantes que debe tener y cumplir una empresa, ya que hoy en día son muy pocos los casos en los que se va al banco a realizar pagos seguros, pues para evitar filas y ser más eficaces se prefieren las transacciones

virtuales, en la gran mayoría de los casos es eficiente, seguro e instantáneo; por esto esta norma debe asegurar la protección de la información sensible de las tarjetas débito o crédito ingresadas en algún portal de pagos en línea. En cuanto a -HIPAA su importancia para mi es aún mayor ya que se encarga de proteger y asegurar la integridad de los pacientes, pues en algunos casos los enfermos terminales por ejemplo; prefieren que sus familiares no sepan su real estado de salud para mantener su estabilidad emocional y es una decisión que debe ser respetada sin importar la posición moral de los integrantes de un sistema de salud, por esta razón es importante su implementación. El -CONPES 3995 tiene como principal objetivo que en Colombia se pueda garantizar la seguridad digital con el fin de que la sociedad cada vez sea más incluyente y esto permita el avance de la industria.

OTROS PUNTOS DE VISTA.

De acuerdo a mi planteamiento algunos autores opinan similar y otros tienen su propio y discutible punto de vista, en el caso de (Hernández, E. F. T, Canizales, R. R, & Páez, A. V, 2021) opinan que los esfuerzos realizados por las empresas en cuanto a tecnología y desarrollo pueden llegar a ser en vano si los empleados o miembros de la misma no siguen los procesos que han sido definidos para efectuar la ciberseguridad, con temas como autenticación segura, claves dinámicas y completa confidencialidad, ya que según ellos en muchos casos este tema es llevado muy a la ligera por parte de los funcionarios lo cuál hace que los datos e información al interior de la empresa resulten con cierto grado de vulnerabilidad, enfocan su punto de vista en que es de gran importancia la concienciación de la ciberseguridad en los empleados. Mientras que (Blasyk. N, 2021) habla del porqué la gran mayoría de pequeñas y medianas empresas -PyMes no invierten en ciberseguridad y algunas de las razones son porque creen que al ser pequeñas no son blanco de un ataque cibernético, piensan también que con tener políticas de privacidad sólidas es suficiente y para ellos no es necesario la implementación de tecnología para la seguridad de la empresa, pero la posición de el es que sí es necesaria la implementación de ciberseguridad ya que con el simple hecho de tener datos en un sistema existe la posibilidad de que sean atacados, manipulados o robados, no es suficiente tener un software de antivirus, pues cada día el avance de la tecnología crea también nuevas formas de ataque. Sin embargo según (González

A, 2020) existe confusión en las empresas respecto a la implementación de los controles de ciberseguridad con los que deben contar y considera que no les garantiza a las empresas protección respecto a las violaciones de datos y fraudes. Por otro lado (Peña, A. 2022) opina que las empresas sin importar a lo que se dediquen o su objetivo deben atender la infraestructura crítica, lo que quiere decir que deben generar políticas de seguridad para todo lo que guarde datos digitales de vital importancia, pues existe una gran posibilidad de que otros aprovechen las vulnerabilidades de ciberseguridad para realizar actividades maliciosas. Desde otro punto de vista (Cano J, 2021) dice que la ciberseguridad empresarial hoy en día es el nuevo referente de las empresas modernas que tienen como objetivo marcar la diferencia entre sus clientes y sus productos y servicios en el entorno digital. Cree que no es necesario sólo contar con una estrategia de ciberseguridad, sino que también se necesita tener un marco de operaciones básicas que permitan mayor flexibilidad y agilidad para navegar en medio de los retos e inestabilidad de la actual realidad.

CONCLUSIONES

- Con base al estudio de casos abarcado en este ensayo se puede asegurar que las empresas garantizan su productividad y crecimiento si implementan sistemas óptimos de protección de su información por medio del uso de tecnologías que pueden además fortalecer la publicidad y masificación de sus bienes, productos y servicios para crecer y satisfacer adecuadamente las expectativas de sus clientes.
- Se debe generar conciencia de la gran importancia de la responsabilidad de todas las empresas con el fin de que hagan uso de la ciberseguridad y se protejan adecuadamente, para que sea una cultura más que una obligación que asegure el éxito en el crecimiento exponencial y desarrollo de las empresas.
- Los gerentes y directivos de las empresas deben ser capacitados y concientizados para que inviertan e implementen eficientes sistemas de ciberseguridad y le den la mayor importancia en el desarrollo de su gestión sabiendo además que esto les asegurará la productividad y los protegerá de ataques, sabotajes y evite además la competencia desleal y para esto es necesario el uso de la normatividad vigente y las certificaciones existentes,

que puede además generar beneficios económicos y financieros ya que suele ser más barato autoprotegerse que exponerse al fraude y la calumnia que podría desencadenar un ataque cibernético. De acuerdo a lo consultado en este ensayo referente a la normatividad que existe en materia de ciberseguridad a nivel mundial y en Colombia, para mi es un tema de gran importancia que las empresas implementen estos controles de ciberseguridad ya que representa una ventaja competitiva respecto a empresas que no cuenten con cumplimiento normativo, se tiene un estándar para proteger la información y causa una mayor confianza en los clientes que comparten sus datos, por lo tanto las empresas deben destinar un presupuesto considerable en ciberseguridad que les permita certificarse en los marcos normativos más importantes como NTC/ISO27001:2013, PCI/DSS e HIPAA ya que además, en algunos casos es obligatorio que las empresas cuenten con estas certificaciones para poder operar.

- Para finalizar, está claro que es un excelente negocio invertir en sistemas, métodos y personal capacitado, no solo académicamente si no con principios, valores y una ética profesional a prueba de sobornos y chantajes que puedan en algún momento exponer a las empresas a infiltrados y corruptos que aprovechándose de su rol puedan vender y exponer la integridad de la información y datos a los que tienen acceso, esto con ayuda de métodos como el polígrafo y un exigente estudio de selección y seguridad al personal incorporado para tal fin.

REFERENCIAS

Arias Cardona, D. (2022). Formulación Sistema de Monitoreo y Evaluación: Antivirus para la Deserción.

Avast. ¿Qué es un virus informático? | Definición de virus en un PC. (2021, November 25). Avast 2022, Reccuperado 08/09/2022, del sitio web https://www.avast.com/es-es/c-computer-virus

Basco, A, Beliz, G, Coatz, D, & Garnero. (2018). *Industria 4.0: "fabricando el futuro"* (Volumen 647). Inter-American Development Bank.

Blasyk, N. (2021, August 7). *¿ciberseguridad en las PYMES?* El Periódico. Recuperado 08/09/2022, del sitio web: https://www.elperiodico.com/es/activos/empresas/20210807/invierten-ciberseguridad-pymes-11970393

Cajamarca, I., & Villa, C. F. (2021, September 9). *"Cada mes se realizan 35 M de operaciones en promedio a por medio del botón PSE"*. LaRepublica.co. Recuperado 06/09/2022, del sitio web: https://www.larepublica.co/finanzas/al-mes-se-realizan-35-millones-de-transacciones-en-promedio-a-traves-del-boton-pse-3229711

Cando Segovia, MR y Chicaiza, R. (2021). Prevención de ciberseguridad: enfatizada en los procesos de infraestructura tec. *TIC: cuadernos de desarrollo aplicados a las TIC*, 17-41.

Cano, J. J. (2021). Maneras de operación de la ciberseguridad empresarial: Capacidades básicas importantes para navegar en el contexto digital. *Global strategy reports* 44 - 1.

Cazar, J. C. Y., & Contero, C. V. N. (2022). Aplicaciones de la ISO 27001 para la seguridad de los sistemas de TI. *Dominio de las Ciencias*, 1025-1041.

Cisco. ¿Qué es la ciberseguridad? Cisco (2022). Recuperado 07/09/2022 del sitio web: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

CONPES Política Social la distribución territorial y sectorial (2020, July 1). CONPES para la Política Social la distribución territorial y sectorial del. Recuperado 06/09/2022, del sitio web: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

De la Rosa Téllez M, Reyes M, y Pérez A. (2021). Estrategia cognitiva evita ataques Ddos (denegación de servicios) en servidores web.*Opuntia Brava*, 102-112.

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de BD en organizaciones públicas para mitigar ataques de ciberseguridad en Latam* (Bachelor's thesis).

Erard, G. (2022, August 19). *Google bloquea ataque DDoS.* Hipertextual. Recuperado 26/08/22 del sitio web: https://hipertextual.com/2022/08/google-bloquea-mayor-ataque-ddos-registrado-a-la-fecha

Esquivel, N. S. (2022) ¿ Qué es la cultura hacker?. Question/Cuestión, 3(71).

González, A. (2020, December 30). Seguridad lógica en informática. ¿En qué consiste? *Ayuda Ley Protección Datos*. Recuperado 06/09/2022, del sitio web: https://ayudaleyprotecciondatos.es/2020/12/30/seguridad-logica/

Hernández, E, Canizales R, y Páez A (2021). La importancia de la ciberseguridad y los DH en el entorno virtual. 142-158.

Hickling J (2022, February 18). *Apple cyber attacks:* Pentest People. Recuperado 26/08/22, del sitio web: https://www.pentestpeople.com/apple-cyber-attacks-mobile-devices-still-at-risk/

Laval C (2022, March 10). *¿Qué es la ley HIPPA y cómo protege nuestra privacidad?* Recuperado 06/09/2022, del sitio web: https://www.abogado.com/recursos/ley-de-seguro/seguro-de-salud/

Manuel, J., & Aguilar, A. (2020, December 3). *La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas: DOI: http://dx.doi.org/10.18847/1.12.2*. Grupo de Estudios en Seguridad Internacional (GESI). Recuperado 20/08/22, del sitio web: http://www.seguridadinternacional.es/resi/index.php/revista/article/view/303

Olmedo, J y Gavilánez F (2018). Análisis de los ciberataques en Latam. *INNOVA Research Journal*, 172 - 181.

Peña, A. (2022, January 31). C*iberseguridad nunca pasa de moda*. Business Insider México Recuperado 26/08/2022, del sitio web: https://businessinsider.mx/ciberseguridad-no-pasa-moda-ana-pena-tech-talk_opinion/

Rivera, N. (2014, Agosto 24). *PlayStation Network caído por un ataque de DDo (Actualizado)*.Hipertextual. Recuperado 26/08/2022, del sitio web: https://hipertextual.com/2014/08/playstation-network-caido

Sabatino C (2021). *La confidencialidad y la ley HIPAA - Fundamentos - Manual MSD versión para público general*. MSD. Recuperado 06/09/2022, del sitio web: https://www.msdmanuals.com/es-co/hogar/fundamentos/asuntos-legales-y-%C3%A9ticos/la-confidencialidad-y-la-hipaa-ley-de-portabilidad-y-responsabilidad-de-seguros-de-salud-en-estados-unidos

Tello Baquero y Freire Cobo (2020). Implementación de un clúster de firewall-checkpoint para reemplazar el firewall-router (Master's thesis).