Practica de Auditoria de Sistemas y TI para MI BANCO Colombia

Freddy Santiago Joya Rangel

Informe de práctica empresarial para optar el título de Ingeniero de Telecomunicaciones.

Director

Yuli Andrea Álvarez Pizarro

Magister en Ingeniería Eléctrica

Universidad Santo Tomás, Bucaramanga

División de Ingenierías y Arquitectura

Ingeniería de Telecomunicaciones

2022

Contenido

Lista de figuras

Lista de apéndices

Resumen

El presente informe tiene como objetivo presentar los aportes y el trabajo realizado durante la practica empresarial para MI BANCO Colombia, Entidad que hace parte del grupo CREDICORP, que hoy en día atiende a más 497 mil clientes en 123 oficinas en todo el país. Su modelo operativo se basa en la oferta de soluciones de financiamiento y ahorro a través de crédito microempresarial, agropecuario, para remodelación, vehículo, libre inversión y vivienda, entre otros. Este informe tiene lugar en el área de *Auditoría Interna de TI*, la cual es un órgano de control para las distintas normativas y obligaciones que tiene el banco tanto internas como externas.

La supervisión y control a las distintas áreas con las que cuenta el banco se realiza a través de distintas auditorias establecidas en los planes anuales de Auditoria, adicionalmente se brinda apoyo de consultoría y regulación de buenas prácticas de TI (ITIL, COBIT, NIST).

Palabras clave: auditoria, control, supervisión, riesgo, financiera.

Abstract

This report aims to present the contributions and work done during the business practice for MI BANCO Colombia, an entity that is part of the CREDICORP group, which today serves more than 497 thousand clients in 123 offices throughout the country. Its operating model is based on the offer of financing and savings solutions through microenterprise credit, agriculture, remodeling, vehicle, free investment, and housing, among others.

This report takes place in Internal Audit of IT, area that is a control body for the different regulations and obligations that the bank has, internal and external regulations (Financial Superintendence), this control is conducted through different audits established in the annual audit plans, additional provides consulting support and regulation of good IT practices (ITIL, COBIT, NIST).

Keywords: Financial Superintendence, NIST, COBIT, ITIL, Control, Risk.

Introducción

MI BANCO es una institución financiera supervisada por la Superintendencia Financiera de Colombia, que surge tras la fusión por absorción de Encumbra (Edyficar S.A.S.) por parte de Bancompartir (Bancompartir S.A.). el objetivo principal de la practica fue apoyar la ejecución de las auditorias de TI y Ciberseguridad con base en los proyectos de TI definidos en el Plan Anual del Banco, aportando conocimientos técnicos de distintas áreas relacionadas con TI y así obteniendo conocimiento en los distintos marcos de referencia de tecnologías de la información (COBIT, ITIL, ISACA) aplicadas al sector Bancario. Una de las actividades principales fue realizar seguimiento a los observaciones de las Auditorias que ya habían sido formalizadas, contactando a las áreas auditadas y a la persona encargada de solventar dicha observación con el fin de mes a mes recolectar evidencias e información que determina el porcentaje de avance de la observación, en el tiempo que no se estaba realizando seguimiento de Auditoria, se brindó apoyo en distintas pruebas de Auditorias que se encontraban en proceso, pruebas que requerían ciertos conocimientos tanto como en programación, redes y computación. Dando así un apoyo fundamental en la Auditoria interna.

El aporte fundamental que se dejó en la empresa fue un repositorio en SharePoint automatizado para la recolección de evidencias de las distintas observaciones de la Auditoria y porcentaje de avance de dicha observación. En el presente documento se encontrara más a detalle este aporte realizado así como la justificación de esta práctica, los objetivos específicos de la práctica, marco referencial el cual ayudo como soporte teórico en la realización de las practicas, adicionalmente se encontrara el perfil de la empresa, un detalle más específico de las actividades realizadas en el transcurso de la práctica, los distintos aportes que se realizaron al área de Auditoría interna de TI de MI BANCO Colombia, lecciones aprendidas y por ultimo las conclusiones de dicha práctica.

1.2 Justificación

El periodo de prácticas es muy importante de primera mano para tener un primer contacto con un ámbito laboral y profesional, en donde se tiene que mantener todo momento protocolos, tiempos, horarios y fechas, si bien la universidad da un acercamiento a esto, tener una experiencia en un ámbito profesional es una experiencia muy enriquecedora, en algunas ocasiones cuando se llega a los semestres finales de un pregrado ciertamente es complicado definir de qué forma voy a aplicar mis conocimientos, a la hora de realizar las practicas puedes empezar el camino para definir en que área de la telecomunicación quieres ejercer.

El área de Auditoria de TI brinda amplios conocimientos de las partes normativas, buenas prácticas y documentación de las distintas partes que conforman al área de TI, estos conocimientos pueden ser aplicados ya sea de manera general en TI como al área específica de telecomunicaciones como en programación, redes, base de datos, ciberseguridad, etc.

1.3 Objetivos

1.3.1 Objetivo general

Apoyar la ejecución de las auditorias de TI y Ciberseguridad con base en los proyectos de TI definidos en el plan anual del banco, aportando conocimientos técnicos de distintas áreas relacionadas con TI y así obteniendo conocimiento en los distintos marcos de referencia de tecnologías de la información (COBIT, ITIL, ISACA) aplicadas al sector bancario.

1.3.2 Objetivos específicos

- Dar cumplimiento a la asignación de las actividades y pruebas de Auditoria conforme el plan anual y trabajos asignados.
- Garantizar el cumplimiento de las disposiciones normativas internas y externas del Banco.
- Garantizar la integridad, confidencialidad y disponibilidad de la información.
- Aplicar el Marco Internacional para la práctica profesional de la auditoría interna y código de ética del auditor, en el desarrollo de las funciones.

2. Marco referencial

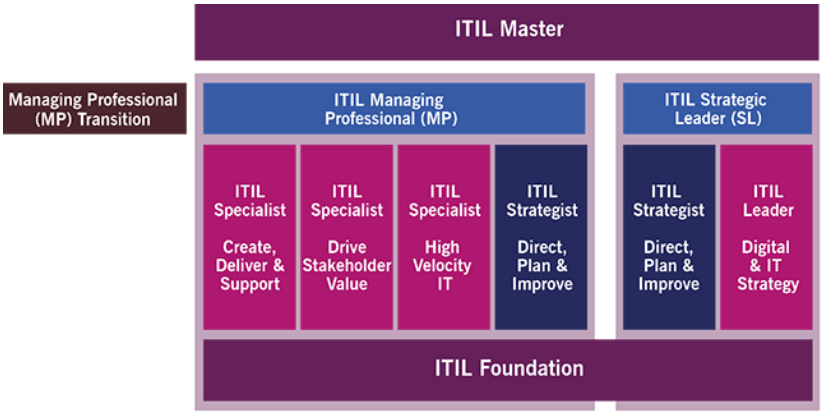
2.1 Marco teórico

2.1.1 ITIL

ITIL 4, la última evolución de ITIL, se basa en la guía central de versiones anteriores para proporcionar una orientación completa, práctica y comprobada [1]. ITIL es muy compatible con la gestión de cambios, gestión de incidentes e incluso hoy en día con distintas tecnologías como la nube o sistemas basados en cloud.

También funciona a la perfección con DevOps, Lean y Agile, y los productos de Axelos como PRINCE2® y AgileSHIFT®. Es la base de la norma internacional ISO20000 y los flujos de trabajo en muchas plataformas de software de gestión de servicios [2].

Figura 1 *ITIL*

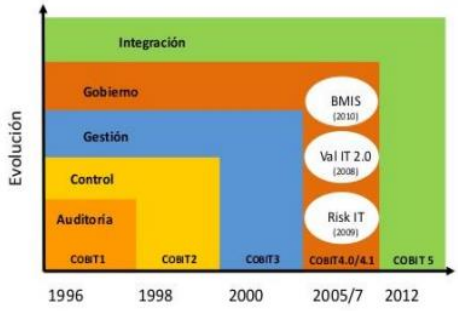


Tomada de Framework de ITIL V4

2.1.2 COBIT

COBIT brinda un marco de trabajo integral, que ayuda a las organizaciones a lograr sus objetivos en base a la implementación de procesos de Gobierno y de Gestión de TI [3]. COBIT involucra a toda la organización considerando los intereses de cada área de la organización con TI lo que genera una cadena de valor ya que es una herramienta que permite solventa la brecha existente entre los requerimientos de control, riesgos, tecnicismos y Auditorias ya que deja una política clara de buenas prácticas de control TI a nivel mundial.

Figura 2. *COBIT*



Tomado de Manual COBIT® 5,

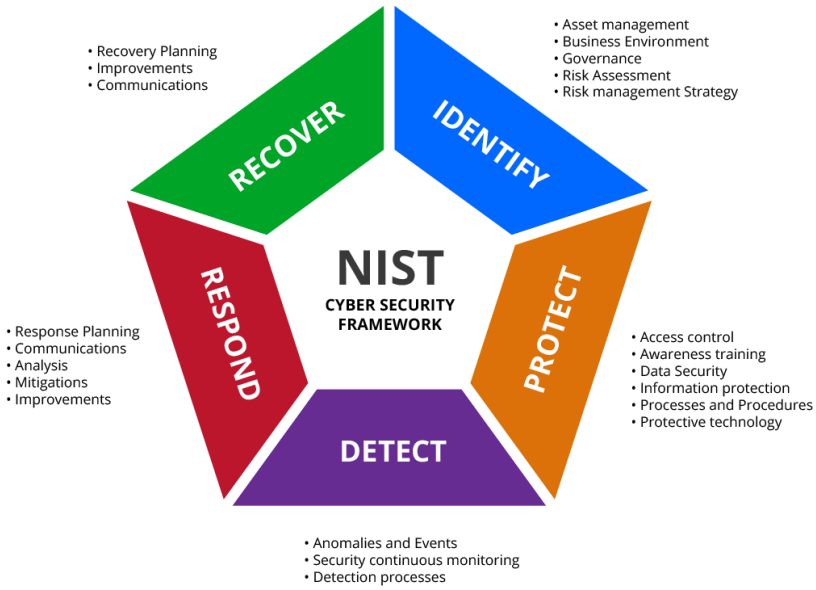
2.1.3 CISA/ISACA

CISA es una certificación para los Auditores respaldada por ISACA dentro de los requisitos de esta certificación se encuentra no solo pasar el examen, sino que también contar con 5 años de experiencia en Auditoria de Sistemas, por otra parte, ISACA (Asociación de Control y Auditoría de Sistemas de Información) proporciona orientación, puntos de referencia y herramientas de gobernanza para las empresas que utilizan sistemas de información. ISACA también organiza una serie de conferencias internacionales que se centran en temas técnicos y de gestión relacionados con la garantía, el control, la seguridad y la gobernanza de TI de IS. También coordina varios programas de certificación, incluyendo Auditor Certificado de Sistemas de Información, Gerente Certificado de Seguridad de la Información, Certificado en el Gobierno de TI Empresarial y Certificado en Riesgos y Control de Sistemas de Información credenciales [4].

2.1.4 NIST

El Instituto Nacional de Estándares y Tecnología (NIST) fue fundado en 1901 y ahora es parte del Departamento de Comercio de los Estados Unidos. El NIST es uno de los laboratorios de ciencias físicas más antiguos del país [5]. Estos estándares de tecnología son utilizados por múltiples empresas a nivel mundial, ya que estos estándares abarcan muchos posibles riesgos, controles y mitigaciones de riesgos, permitiendo así a las empresas adoptar distintos estándares que más se acomoden a su perfil de empresa.

Figura 3. *NIST*



Tomado de página web corcystems.com

2.1.5 ISO 27000

ISO/IEC 27000 proporciona la visión general de los sistemas de gestión de seguridad de la información (SGSI). También proporciona términos y definiciones comúnmente utilizados en la familia de normas ISMS [6]. Hoy en día ISO 27000 se encuentra en su 5ta edición publicada en 2018.

2.1.6 Superintendencia Financiera

La Superintendencia Financiera de Colombia surgió de la fusión de la Superintendencia Bancaria de Colombia en la Superintendencia de Valores mediante el Decreto 4327 de 2005, modificado posteriormente por el Decreto 2555 de 2010, la Ley 1480 de 2011 y el Decreto 710 de 2012 [7]. Adicional es la entidad que vela por lo derechos de los consumidores en las entidades bancarias, obligando a estas entidades a cumplir con sus circulares y leyes emitidas tanto de protección

de datos, ciberseguridad, requerimientos, informes y continuidad del servicio todo esto con el fin de proteger a los colombianos y controlar a las entidades bancarias.

2.1.7 Riesgos Inherentes

Los riesgos inherentes son aquellos propios de la naturaleza de la entidad y que son independientes de su sistema de control interno. En otras palabras, son los riesgos que se encuentran presentes en la entidad antes de considerar las actividades de control establecidas por la gerencia para mitigarlos [8]. Conocer este tipo de riesgos en la entidad facilita que el Auditor pueda realizar el planteamiento del plan anual de Auditoria.

2.1.8 Riesgos de control

Las entidades deben establecer actividades de control que les permitan prevenir, detectar y corregir las desviaciones que se presentan en sus procedimientos. Dichas actividades de control deben apuntar a mitigar los principales riesgos a los que se expone la entidad [9]. Dentro de la planeación de las Auditorias siempre se debe tener en cuenta de que este tipo de control falle.

2.1.8 TLS 1.2

TLS, **Transport Layer Security**, es un protocolo criptográfico que permite una comunicación segura en internet. No recurrir a TLS 1.2 podría hacer que se hiciera uso de los exploits del protocolo para interceptar los mensajes y poner en peligro las comunicaciones. De ahí que algunos servicios, como PayPal, no permitan realizar transacciones en esta versión del protocolo TLS.[10]

2.1.9 VPN

la función principal de una VPN es ocultar su dirección IP de su ISP y otros terceros. Esto le permite enviar y recibir información en línea con la tranquilidad de que nadie, excepto tú y el proveedor de la VPN, tendrá acceso a lo que hagas [11]. En el caso de MI BANCO la VPN era usada principalmente para realizar la conexión remota al Servidor del banco donde se almacenaba la información más sensible y formalizada, adicionalmente se realizaba la sincronización don el directorio activo a través de la conexión VPN.

Figura 4. *VPN*

Tomado de página web surfshark.com

2.1.10 FIREWALL

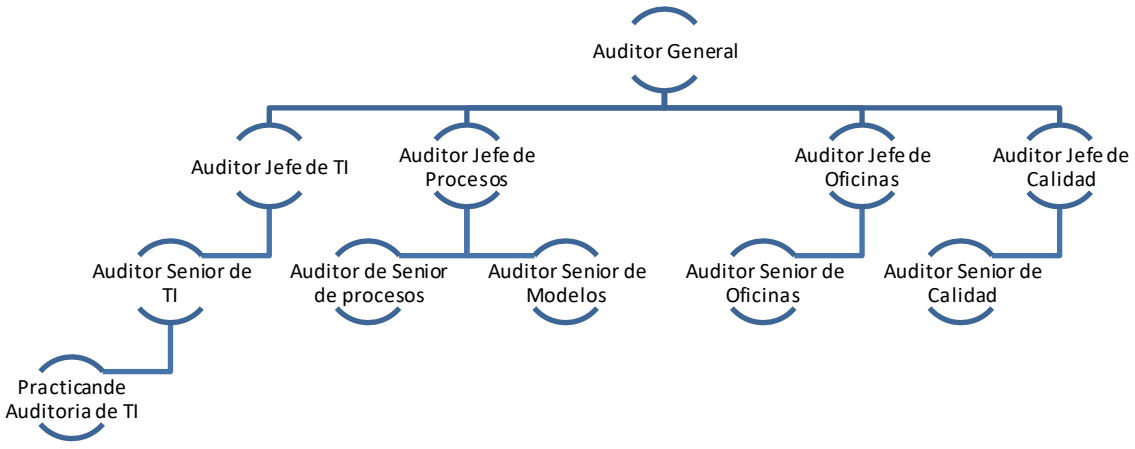
Un firewall es un sistema diseñado para proteger las redes privadas del acceso no autorizado y no verificado en una conexión a Internet. Estos pueden ser de tipo hardware o software, o una combinación de ambos [12]. En MI BANCO esta herramienta era utilizada para realizar la canalización y distribución de los accesos al servidor central e información.

3. Perfil de la Empresa

MI BANCO es una institución financiera supervisada por la Superintendencia Financiera de Colombia hoy en día atiende a más de 492 mil clientes en 126 oficinas en todo el país. Su modelo se basa en la oferta de soluciones de financiamiento y ahorros a través de crédito microempresarial, agropecuario, para remodelación, vehículo, libre inversión, vivienda, entre otros. Su principal enfoque son las microempresas colombianas, por ello dentro de su propósito principal se encuentra **"Escribimos juntos historias de progreso".**

El área de Auditoría interna, área donde se realizó la practica está conformada por Auditores que apoyan o Auditan al banco en distintas áreas, como procesos, contabilidad, oficinas, riesgos y tecnología e informática, la Auditoria de tecnología e informática (TI) se enfoca en realizar seguimiento, auditoria, consultoría y control a las áreas de TI del banco, este enfoque se realiza a través del plan anual de Auditoria, dicho plan se realiza de acuerdo a los intereses internos de la entidad y los intereses de la sede principal Credicorp para sus sucursales.

Figura 5. Organigrama Auditoría Interna de MI BANCO Colombia



Estructura Organizacional Auditoría Interna.

La anterior imagen hace referencia a la estructura organizacional del área de Auditoría Interna, para el caso de esta práctica como practicante de Auditoria de TI se estuvo apoyando tanto al Auditor jefe de TI como al Auditor Senior de TI en las distintas labores impartidas.

4. Activades Realizadas

Inicialmente en la práctica profesional se realizó una capacitación en la cual se informaron los principales valores, misión, visión, divisiones, estructura y normativa del banco. Una vez terminada esta capacitación se inició una etapa de aprendizaje y empalme, en la cual se indicaron las tareas a realizar dentro de la práctica y cada actividad realizada era previamente supervisada y revisada por un superior.

Como primera actividad se realizaron pruebas de Auditoria, las cuales consistían en validar algoritmos seguros dentro de la configuración del Firewall y VPN, generando concepto de buenas prácticas como el uso de TLS 1.2 en la configuración del Firewall. Una vez realizadas las pruebas, se documentaron los hallazgos y conceptos de la prueba, dando así una calificación cuantitativa al control que se tiene sobre el riesgo de no tener los canales de comunicación cifrados. Siguiendo con el proceso, se generaba una calificación cuantitativa para la Auditoria, la cual permite indicar en qué nivel se encuentra el área auditada. Esta calificación se da de manera porcentual e indica en que intervalo de buenas prácticas se encuentra la empresa. Con esto, era posible verificar si dichos intervalos eran deficientes, aceptables, destacados o superiores.

Luego de generar la calificación, la siguiente tarea en la práctica profesional consistió en dar apoyo a la formalización de la Auditoria, la cual consistía en generar un Informe que permitiera indicar la calificación de la Auditoria, observaciones u oportunidades de mejora encontradas en el transcurso de las pruebas. En segundo lugar, era necesario entrar en contacto con las áreas auditadas y solicitar

información del porcentaje de avance para la implementación de la observación. Como hallazgo, se pudo observar que el banco no contaba con una base de datos para recopilar evidencias de avance e información de las áreas y se procedió a crear un repositorio en SharePoint para que las áreas auditadas pudieran cargar la información solicitada y a su vez el área de Auditoria centralizara esta información. Adicional a esto, se elaboró un script que permitía extraer la información física y software instalados en el equipo de cómputo, sin necesidad de usar un programa externo en el anexo 1 a este documento se encontrara más información acerca de este script.

Una de las Auditorias finales fue la Circular 042, esta auditoria es de suma importancia ya que brinda confianza y seguridad a la entidad bancaria para dar cumplimiento a todas las normativas propuestas por la Superintendencia Financiera como la regulación y protección de datos de los clientes, seguridad en la comunicación interna evitando la filtración de información sensible, cifrado del canal de comunicación de los Cajeros automáticos.

En el transcurso de esta última etapa se brindó apoyo aportando ideas sobre que pruebas se podrían realizar para validar que control existe sobre los activos de información, equipos de conexión en las oficinas, canales de comunicación, computadores, servidores y que se cuente con un servidor NTP para que el reloj de cada servidor y aplicación sea acorde con la hora local que exige la superintendencia de industria y comercio.

5. Aportes y recomendaciones

El ambiente laboral en el área de Auditoría interna de MI BANCO Colombia es un ambiente excelente, un área llena de personas muy respetuosas, amables y profesionales, en el que también se tiene muy en cuenta las pausas activas cada cierto tiempo. Esta área es el órgano de control interno del banco, la cual prepara y supervisa a las demás áreas para que cumplan con todas las obligaciones que

impone la Super Intendencia Financiera de Colombia a las entidades bancarias, un aporte que se dejó al área fue un repositorio en el cual se puede cargar evidencias y reportar avances en las observaciones de Auditoria, este repositorio está directamente conectado a un Excel el cual contiene el Informe de Auditoría y descripción de cada observación a su vez se dejó el inicio para la conexión de ese repositorio con el Aplicativo Power BI, herramienta la cual se puede hacer reportes gráficos de los avances reportados.

Una recomendación al área de auditoria es en la delegación de tareas, si bien entre Auditores se pueden brindar apoyo para realizar las distintas Auditorias, cada Auditor debe responder por las Auditorias a su cargo, en su totalidad y no solo una parte de ellas, otra recomendación es el tema horario, en muchas ocasiones no se respetó el horario laboral establecido, si bien en algunas ocasiones por cumplimiento o cierres se deben extender un poco los horarios, en estos casos fueron situaciones injustificadas, situaciones que los superiores pueden perfectamente hacerse cargo de ellas como por ejemplo el color de una diapositiva.

6. Lecciones Aprendidas

La práctica como Auditor TI para MI BANCO Colombia brindo un aprendizaje amplio en los distintos marcos internacionales de buenas prácticas de TI, como ITIL, COBIT, NIST, ISO, así como un aprendizaje amplio en habilidades blandas como la comunicación asertiva, este tipo de aprendizaje se obtiene con experiencias de este tipo ya que en la universidad se enfoca más en el aprendizaje técnico y teórico, sin embargo; todo el aprendizaje obtenido en el transcurso de la carrera pudo ser aplicado en la práctica adicionalmente se obtuvo mucho aprendizaje en la Autonomía ya que al tener muchas tareas impartidas de manera simultánea se tenía que investigar y aprender distintas manera de realizar dichas tareas. En el aprendizaje de los distintos marcos de buenas prácticas de TI, se

evidenciaron distintos conceptos los cuales requirieron una investigación para poder dar entendimiento al marco, lo cual indica un aprendizaje en la habilidad investigación.

En la práctica se tuvo mucho contacto en las configuraciones de los distintos equipos de un Core basado en un modelo OSI, por lo cual se obtuvo experiencia en un ámbito real acerca de las configuraciones de los equipos de Capa 3, 4, 5 del modelo OSI. Por último, se obtuvieron distintos conocimientos en los aplicativos de Office 365 como Excel, PowerPoint, SharePoint, PowerBI, Teams.

7. Conclusiones

Durante el desarrollo de la práctica profesional se evidencio la importancia del área de Auditoría Interna, la cual ha permitido dar cumplimiento a los requerimientos de entidades gubernamentales como la Superintendencia Financiera de Colombia.

Gracias a las auditorias desarrolladas en MI BANCO Colombia, la entidad ha podido certificarse en los distintos marcos Internacionales de buenas prácticas, convirtiéndose en un referente nacional. Inicialmente la Auditoria Interna se considera un órgano de control, sin embargo; también funciona como consultoría para que las distintas áreas auditadas obtengan la información de los procesos que requieren mejoras.

El aplicar los distintos marcos internacionales de buenas prácticas brinda una oportunidad constante de mejora, renovación, cambio sin que el riesgo se considerable, adicionalmente se tiene un mayor control de los activos de TI y en general una administración más efectiva.

El dar cumplimiento a los objetivos planteados inicialmente deja como resultado.

- Conocimiento amplio de los Marcos Internaciones de buenas prácticas de TI
- Mejora en las habilidades de comunicación asertiva
- Conocimiento en las distintas herramientas de Office 365
- Construcción de Un repositorio automatizado
- Cierre de 4 Auditorias en el transcurso de la Práctica.

De igual forma, destacar la experiencia laboral de 6 meses en un órgano de control de TI, lo cual permite conocer el entorno laborar y adquirir experiencia para los retos que se presenten después de la formación como Ingeniero de Telecomunicaciones.

Referencias

[1] AXELOS, «AXELOS,» 4 Abril 2018. [En línea]. Available: https://www.axelos.com/certifications/itil-service-management/what-is-itil. [Último acceso: 2 Agosto 2022].

[2] Proactivanet, «Proactivanet,» 18 Octubre 2020. [En línea]. Available: https://www.proactivanet.com/blog/proactivanet/ultima-version-itil-v4-certificacion/. [Último acceso: 1 Agosto 2022].

[3] J. Hernandez Hernandez, «COBIT, una metodología que genera valor en las,» Universidad Piloto de Colombia, Bogota, 2017.

[4] ISACA, «ISACA Web site,» 15 Mayo 2022. [En línea]. Available: https://www.isaca.org/. [Último acceso: 4 Agosto 2022].

[5] NIST, «NIST,» 16 Enero 2022. [En línea]. Available: https://www.nist.gov/cybersecurity. [Último acceso: 5 Agosto 2022].

[6] ISO/IEC, «International Organization for Standardization,» Febrero 2018. [En línea]. Available: https://www.iso.org/standard/73906.html. [Último acceso: 6 Agosto 2022].

[7] SFC, «La Superintendencia Financiera de Colombia,» 27 Julio 2022. [En línea]. Available: https://www.superfinanciera.gov.co/inicio/nuestra-entidad-20483. [Último acceso: 7 Agosto 2022].

[8] Actualícese, «Actualícese Web site,» 17 Junio 2022. [En línea]. Available: https://actualicese.com/tipos-de-riesgo-de-auditoria.. [Último acceso: 5 Agosto 2022].

[9] Actualícese, «Actualícese Web site,» 17 Junio 2022. [En línea]. Available: https://actualicese.com/tipos-de-riesgo-de-auditoria-inherentes. [Último acceso: 6 Agosto 2022].

[10] W. R. Marchand-Niño y E. E. Rueda Liberato, «Encryption with TLS Protocol version 1.2 and Web,» Universidad Del Rosario, Bogota, 2019.

[11] Kaspersky, «Kaspersky,» Junio 2022. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn. [Último acceso: 8 Agosto 2022].

[12] hp, «HP TECH,» 31 Agosto 2021. [En línea]. Available: https://www.hp.com/cl-es/shop/tech-takes/que-es-un-firewall-de-red-y-como-funciona. [Último acceso: 6 Agosto 2022].

Apéndices

Apéndice A. *Script extracción de programas instalados a través del instalador de Windows*

Ver Apéndice A para más información acerca del Script elaborado.