Información Importante

La Universidad Santo Tomás, informa que el(los) autor(es) ha(n) autorizado a usuarios internos y externos de la institución a consultar el contenido de este documento a través del Catálogo en línea del CRAI-Biblioteca y el Repositorio Institucional en la página Web de la CRAI-Biblioteca, así como en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

Se permite la consulta a los usuarios interesados en el contenido de este documento, para todos los usos que tengan **finalidad académica**, nunca para usos comerciales, siempre y cuando mediante la correspondiente cita bibliográfica se le dé crédito al trabajo de grado y a su autor.

De conformidad con lo establecido en el Artículo 30 de la Ley 23 de 1982 y el artículo 11 de la Decisión Andina 351 de 1993, la Universidad Santo Tomás informa que "los derechos morales sobre documento son propiedad de los autores, los cuales son irrenunciables, imprescriptibles, inembargables e inalienables."

Centro de Recursos para el Aprendizaje y la Investigación, CRAI-Biblioteca

Universidad Santo Tomás, Bucaramanga

Estudio y análisis para la gestión de seguridad de la información y demás actividades en la empresa NTICS S.A.S.

Marly Daniela Gómez Arias

Trabajo de grado para optar por el título de Ingeniera de Telecomunicaciones

Directora

Yudy Natalia Flórez Ordoñez

Universidad Santo Tomás, Bucaramanga

División de Ingenierías y Arquitectura

Facultad de Ingeniería de Telecomunicaciones

2019

Agradecimientos

Gracias a Dios, a mi familia y amigos, sobre todo gracias a mis padres por haberme forjado como la persona que soy en la actualidad, todos mis logros se los debo a ustedes, son la motivación de mi vida, mi orgullo de ser lo que seré.

Gracias a mis maestros por su tiempo y conocimiento, gracias a las personas que, de una u otra, han sido claves en mi vida profesional.

"Vayas a donde vayas, ve con todo tu corazón…"

Tabla de contenido

Pág.

Resumen…..……..…… 05

Abstract……...……..…… 06

Introducción…….…… 07

1 Estudio y análisis para la gestión de seguridad de la información y demás actividades en la empresa NTICS S.A.S.……..…...08

1.1 Objetivos…… 08

1.1.1 Objetivo general……...08

1.1.2 Objetivos específicos……...08

2 Justificación…….08

3 Marco referencial…….09

4 Perfil de la empresa…… 15

5 Actividades realizadas…… 16

6 Aportes y recomendaciones…… 19

7 Lecciones aprendidas…… 20

8 Conclusiones…… 21

Referencias bibliográficas ……..…… 22

Lista de tablas

Pág.

Tabla 1. Ciclo PDCA……... 10

Tabla 2. Inventario de activos……... 11

Tabla 3. Vulnerabilidades, amenazas y riesgos inicialmente identificados...…….... 12

Resumen

El presente trabajo consiste en la descripción y análisis de las actividades gestionadas durante las prácticas empresariales al interior de la empresa NTICS SAS Servicios y Soluciones, estás en su mayoría dentro del área de ingeniería y de proyectos; dichas labores se relación con la seguridad de la información, el proceso de certificación ISO 27001 que la empresa lleva a cabo en la actualizadas y la gestión del área comercial y de ventas.

Palabras clave: Prácticas empresariales, Seguridad de la información, ISO 27001, Certificación, Cotización.

Abstract

The present work consists of the description and analysis of the activities managed during business practices, within the company 'NTICS SAS Services and Solutions', most of the activities in the area of engineering and projects; These tasks are related to information security, the ISO 27001 certification process… activity that the company currently carries out and the management of the commercial and sales area.

Keywords: Business practices, Security of the information, ISO 27001, Certification, quotation.

Introducción

La empresa NTICS S.A.S Servicios & Soluciones tiene la misión de establecer y mantener alianzas sólidas y duraderas con los clientes, ofreciéndoles productos, soluciones y servicios que garantice la satisfacción de objetivos y/o necesidades, los cuales se gestionan de manera eficaz con profesionales y colaboradores; dentro de su portafolio de servicios se encuentra el Outsourcing tecnológico, infraestructura tecnológica, montaje e instalación de servidores, auditoría de seguridad de redes y comunicaciones, ethical hacking, software, antivirus, entre otras.

A continuación, se presenta el informe final del trabajo realizado durante el periodo de prácticas, se describen los objetivos de la práctica, un soporte teórico sobre los temas de seguridad de la información, descripción de la empresa NTICS, las actividades realizadas para cumplir los objetivos de la práctica, los aportes y recomendaciones, lecciones aprendidas y finalmente las conclusiones.

En el transcurso de la práctica se gestionó las actividades de seguridad de la información y demás funciones del departamento de proyectos e ingeniería de NTICS S.A.S, se realizó un apoyo constante al área comercial de la compañía, en actividades de preventa y venta de productos tecnológicos, elaboración de informes y manejo de portales para partners. Otra actividad en la que se participó consistió en la certificación de la empresa en ISO 9001, ISO 14001, ISO 45001 y ISO 27001; cabe resaltar que este proyecto no se terminó antes del cinco de agosto, fecha en que expiraba el contrato de aprendizaje.

1. Estudio y análisis para la gestión de seguridad de la información y demás actividades en la empresa NTICS S.A.S

1.1. Objetivos

1.1.1 Objetivo general.

Gestionar las actividades de seguridad de la información y demás funciones del departamento de proyectos e ingeniería de NTICS S.A.S.

1.1.2 Objetivos específicos.

- Brindar soporte en la administración de la seguridad de la información.
- Apoyar actividades multidisciplinares en otros departamentos al interior de la empresa.
- Gestionar servicios prestados por NTICS.

2. Justificación

En la formación del ingeniero de telecomunicaciones es necesario incluir un periodo de prácticas laborales como parte del proceso formativo de un estudiante, dado que el proceso le ayuda en la adquisición de habilidades, competencias, destrezas y un constante desarrollo.

Adicionalmente las prácticas universitarias permiten realizar un primer acercamiento del estudiante al interior de las empresas dándoles la oportunidad de enfrentar nuevos desafíos en ámbitos administrativos y comerciales, aprenden sobre el sector en el que se desarrolla, trabajan en equipo e incluso definen sus aspiraciones profesionales.

Es importante comenzar a obtener una experiencia profesional poniendo en práctica los conocimientos adquiridos en asignaturas, seminarios, congresos, certificaciones y cursos a lo largo de la vida universitaria; en una mejor situación este encuentro del estudiante con el 'trabajo' no debería darse solo al final de sus estudios sino DURANTE los mismos.

Para la empresa fue de utilidad el tiempo transcurrido igualmente, pues en ese espacio de tiempo me transmitieron aprendizaje y experiencia con el fin de determinar y considerar un contrato laboral finalizando el contrato de aprendizaje. Al final destacaron la responsabilidad, desempeño y eficiencia del practicante al atender las diferentes labores desempeñadas.

3. Marco referencial

La seguridad de la información "es un conjunto de medidas tomadas (tanto preventivas, cómo reactivas) en las organizaciones y los sistemas tecnológicos donde es resguardada información de tipo sensible buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma" [1].

La seguridad de la información se relaciona con la seguridad informática, siendo la primera más incluyente, la seguridad informática se encarga de la protección exclusivamente en medios informáticos, al contrario de la primera que tiene en consideración que la información se puede encontrar en diferentes medios o formas, y no solo en medios informáticos; pues un gran porcentaje de empresas como NTICS SAS hacen aún uso de papelería en muchas de sus labores, la información y los procesos no se han logrado digitalizar completamente.

Debido a lo mencionado anteriormente se vuelve de gran importancia adquirir certificaciones como la ISO 27001 en la actualidad, siendo ésta "la norma internacional por excelencia de protección de datos personales" [2].

Contar con un Sistema de Gestión de Seguridad de la Información (SGSI) adecuado es clave para asegurar la transparencia y hacer más confiable a la organización ante el mercado; en otras palabras, establecer un SGSI y certificarlo "aumentará sus beneficios y reputación empresarial y reducirá el riesgo de incidentes de seguridad." [2]

En primer lugar, es esencial elegir bien la empresa certificadora, la cual debe estar reconocida internacionalmente. Una vez elegida, esta enviará un auditor a su empresa con el que se sostendrá una relación de tres años.

Es de gran ayuda que los auditores estén familiarizados con la industria de su organización, ya que podrán detectar mejor cualquier brecha de seguridad y ofrecerle consejos más detallados y apropiados, de no ser así el proceso se vuelve tedioso y complicado de adoptar, debido a que aparecerán una cantidad de formatos y/o documentos a diligenciar; que serían innecesarios.

El proceso de certificación consta de varias etapas que a grandes rasgos serían la revisión de la documentación, la auditoría donde el auditor verifica la aplicación del SGSI y por último la obtención del certificado.

El tiempo de obtención de la certificación puede constar entres tres meses y un año, todo esto depende de factores como el tamaño de la empresa y disposición al cambio de la misma.

Si se incumple la entidad que certifica puede retirar la certificación, por ello el cambio que se adopta en la empresa debe ser definitivo y se debe seguir revisando sistema de gestión de seguridad de la información

"Como ocurre con todas las normas ISO, la 27001 es un sistema basado en enfoque basado en el ciclo de mejora continua o de Deming. Dicho ciclo consiste, como ya sabemos, en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas

en inglés Plan-Do-Check-Act)" [3]. Este ciclo es el empleado en todas las normas ISO, en la tabla 1 se aprecia las actividades a realizarse en cada paso.

Tabla 1. *Ciclo PDCA*

Planificación	Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias Establecer un mapa de procesos Definir autoridades y responsabilidades
Hacer	Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles
Controlar	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección
Actuar	Adoptar acciones correctivas Adoptar acciones de mejora

Para la 'auditoría a la seguridad de la información' donde aparece el ente 'auditor', se divide el proceso en varias etapas consecutivas donde se establecen objetivos y entregables.

Fase 1. Determinación de vulnerabilidades, amenazas y riesgos: Como lo indica el título en esta fase se hace estudio de los factores mencionados, en los sistemas implementados actualmente en la organización. Para ello primero se debe determinar un inventario de activos, dando como resultado lo que se observa en la Tabla 2.

Tabla 2. *Inventario de activos*

INVENTARIOS DE ACTIVOS IMPORTANTES

Tipo de activo	Nombre de activo
Activo de información	Datos de clientes, datos de proveedores, Documentos Físicos, manuales. Inventarios de hardware, contratos con terceros, otros.
de software y licencias	Software SO licenciado, Software ofimático licenciado, licencias de uso de software en outsourcing, otras licencias.
hardware	Características del hardware de equipos, dispositivos de red, dispositivos móviles, equipos de protección eléctrica, otros.
Instalación red eléctrica	Red e instalaciones eléctricas para computadores, (norma RETIE), sistema de protección de aterrizaje eléctrico (polo o malla a tierra).
Servicios de terceros	Conectividad a internet, mantenimiento y soporte de hardware, mantenimiento y soporte de software, soporte y actualizaciones en software en outsourcing.
Personal	Personal área informática, usuarios de los sistemas.

Fuente: [4]

Seguidamente ha de ser tabulada y/o extraída en documentos las vulnerabilidades, amenazas y riesgos de cada uno de los activos de la empresa. Un ejemplo de éstos factores a ser encontrados se puede apreciar en la tabla 3.

Tabla 3. *Vulnerabilidades, amenazas y riesgos inicialmente identificados*

VULNERABILIDAD	AMENAZAS	RIESGOS POTENCIALES
HARDWARE		
Falta de equipos UPS para contingencias	Cortes de energía o sobrecargas en los equipos.	Pérdida de información, daños en los equipos, pérdida de tiempo en procesos repetidos.
SOFTWARE		
Software no licenciado	Virus informáticos, malware, utilizar exploit.	Mal funcionamiento de sistemas, destrucción de SO, destrucción o modificación de aplicativos e inf.
Software con problemas de seguridad en el desarrollo	Ataques de Inyección SQL, información inconsistente, errores de integridad de datos	Pérdida o modificación de información, robo de claves de usuario, modificación de datos, bases de datos inseguras por permisos y privilegios no definidos
Actualización del SO en los equipos	Utilización de ataques exploit	Intrusión no autorizada en los equipos de usuarios para modificación, borrado o robo de información, ataques de DoS, consecución de privilegios.
SEGURIDAD FÍSICA		
No existe control de acceso físico a las oficinas y equipos informáticos	Manipulación de información sin control de acceso, ataques intencionados a equipos, desastres provocados.	Robo, destrucción, modificación o borrado de información, destrucción o desarticulación física de equipos.
SEGURIDAD LÓGICA		

Deficiente control de acceso a los sistemas	Suplantación de identidad	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios, robo de claves de usuarios
REDES DE COMUNICACIONES		
Vulnerabilidad de navegadores utilizados	Inyección de código SSI, ataques con código XSS	Alteración en el funcionamiento del código, programas y sitios, información sin autorización.
PERSONAL		
Falta de una política de seguridad clara	Ataques no intencionados, ingeniería social, phishing.	Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal.

Fuente: [4]

Fase 2: Análisis de riesgos y diagnóstico de la seguridad de la información: en esta fase se evalúan los riesgos identificando las causas por las que se generan para poder definir un control de seguridad disminuyendo impacto y la probabilidad de ocurrencia. Preferiblemente se debe elaborar escala de probabilidad de los riesgos estimados.

Fase 3: Determinación de los controles para el diseño del SGSI incluyendo políticas y procesos que disminuyan riesgos: como es descrito en el encabezado se definen controles de riesgos y conductas de acuerdo a la norma ISO adaptándolos a la organización y a las políticas de la misma. Un entregable de esta fase debe ser un "informe para el diseño e implementación del SGSI teniendo en cuenta el ciclo de mejora continua PHVA que permita las actividades para planear, hacer, verificar y actuar, que intervengan y permeen todos los procesos y servicios dentro de la organización" [4].

Por último, pero no menos importante, es imperativo el apoyo de altos cargos, de gerencia y/o administración; si los entes mencionados no se muestran verdaderamente comprometidos para la implementación de un SGSI se expondría a que no se adapte adecuadamente a la compañía.

4. Perfil de la empresa

NTICS S.A.S Servicios & Soluciones es una compañía enfocada en establecer y mantener alianzas sólidas y duraderas con sus clientes, ofreciendo productos, soluciones y servicios en nuevas tecnologías de la información y la comunicación (NTIC); la cobertura del servicio se da a través de oficinas físicas y virtuales en Colombia.

El modelo del cual dispone la empresa está basado en ofrecer calidad, flexibilidad y productividad, con la finalidad de conseguir soluciones de valor agregado, el nivel de servicio acordado, reducciones de costos y confianza en todos sus clientes; para esto NTICS goza de acuerdos y colaboraciones con los principales fabricantes TIC de hardware y software, e igualmente con el fin ofrecer seguridad y mostrar un mejor perfil y/o imagen como empresa frente a sus clientes y proveedores, la empresa tiene como objetivo certificarse a finales del presente año en ISO 27001; certificación que le obliga a gestionar las actividades de seguridad de la información de la compañía S.A.S. En éste proceso participo activamente siendo un apoyo para la empresa, trabajando de la mano con el auditor enviado para alcanzar la certificación, organizando los procesos de la empresa y del personal de la misma, para poder luego encontrar las brechas de seguridad que deben ser cubiertas.

Dentro del portafolio de servicios se encuentra el outsourcing tecnológico, infraestructura tecnológica, montaje e instalación de servidores, auditoría de seguridad de redes, comunicaciones unificadas, ethical hacking, software, antivirus, cableado estructurado, entre otros.

En la actualidad NTICS S.A.S cuenta con más de 25 profesionales cualificados, gestiona más de 20000 reparaciones/mantenimientos y más de 8000 tickets de help desk y Service desk anuales.

5. Actividades realizadas

Las actividades desarrolladas durante el periodo de prácticas son descritas a continuación, cada una de ellas se desarrolla dentro de un objetivo específico.

Objetivo 1. Brindar soporte en la administración de la seguridad de la información.

- Actividad 1 'Elaboración de políticas de seguridad de la información en la empresa': Se dejó establecido un documento el cual cuenta con información detallada del plan Dropbox de la empresa, del servidor de la misma, del acceso remoto que se le configuró al servidor, del uso compartido de la red dependiendo de los usuarios del sistema (Admin, contador, comercial…), de la copia de seguridad que se le estableció al servidor; seguidamente se establecieron políticas de conducta del personal las cuales apoyan y/o ayudan a proteger la información sensible de la empresa.

Se realizó seguimiento del cumplimiento de dichas políticas y finalmente para apoyar todo el tema de certificación en seguridad de la información se estudió la ISO 27001.

- Actividad 2 'Gestión de dispositivos': Se adquirió un formato correspondiente para equipos informáticos con el cuál se montó la ficha técnica de cada equipo de la empresa dejando en él la información de donde se encuentra ubicado, el usuario responsable de su uso, marca, modelo, serial, características, nombre del mismo, nombre del grupo de trabajo, dirección IP, máscara, puerta de enlace, DNS, garantía y demás información útil. En el mismo documento se lista el software instalado en la máquina.

- Actividad 3 ‘Gestión de contraseñas’: En el primer mes de práctica se recolectó todas las contraseñas de la empresa (servidor, equipos informáticos, correos electrónicos, portal partners), y se realizó gestión de las mismas; según las políticas establecidas en la actividad 1 las mismas eran modificadas cada 3 meses.
- Actividad 4 ‘Backups de las cuentas de correo electrónico de la empresa’: Como el título de la actividad lo indica se realizaron copias de seguridad a los correos electrónicos, la frecuencia de ésta actividad era de 2 meses según lo establecido en las políticas.

Objetivo 2. Apoyar actividades multidisciplinares en otros departamentos al interior de la empresa.

- Actividad 1 ‘Apoyo a personal comercial’: Se elaboraron tickets en el portal de Domotes donde se solicitaban capacitaciones y/o actividades de apoyo o soporte; igualmente se hizo registro de todas las oportunidades presentadas (negocios) en los portales para socios correspondientes.
- Actividad 2 ‘Realizar trabajo de campo’: Se brindó acompañamiento a un cliente que adquirió un producto con la empresa (Firewall Sophos), éste cliente solicitó transferencia de conocimiento en el manejo del mismo. Para esto se realizó primeramente la certificación en el manejo del Dashboard del producto y seguidamente se procedió a instalaciones del cliente para capacitación.
- Actividad 3 ‘Gestionar procesos del área comercial’: siendo el área comercial la más débil en su momento se brindó apoyo total recibiendo y gestionando todas las solicitudes de los clientes de NTICS, mejorando considerablemente el tiempo de respuesta a las mismas; el trabajo en ésta área fue completo desde el momento en que la solicitud de cotización entraba hasta que el producto estaba en manos del cliente, el paso a paso real sería… solicitud de cotización, seguimiento de la

misma, entrada de orden de pedido por parte del cliente, compra de equipos a mayoristas, comprobación de mercancía y finalmente se daba paso al área de cartera para respectivos pagos y facturación. Un paso adicional se daba cuando el cliente solicitaba garantías de productos.

Objetivo 3. Gestionar servicios prestados por NTICS.

- Actividad 1 'Gestión a los servicios prestados a clientes': Mensualmente se solicitó reportes de los servicios que le son prestados al cliente mayor de la empresa, con el fin de realizar informes; éstos informes contenían información como la disponibilidad de equipos como enrutadores y switches ubicados en cada sede del cliente, gráficas donde se evidenciaba la calidad de los enlaces de internet y datos; también cuentan con servicio de firewall con la empresa, obteniendo datos como usuarios de acceso remoto, uso web, cantidad de veces que se denegaron dominios, aplicaciones y/o usuarios, cantidad de ataques detectados. El cliente solicita estos informes mensualmente para realizar pagos.
- Actividad 2 'Participación en el proyecto de control de acceso ara universidades': Uno de los proyectos grandes de la empresa consiste en prestar el servicio de control de acceso a universidades, se apoyó en éste proyecto al auxiliar de carnetización estableciendo escritorio de acceso remoto al servidor de una de esas universidades y registrando la información de los distintos usuarios en la base de datos pre establecida para controlar dicho acceso. Para poder registrar correctamente la información en la base se prepararon archivos Excel con información específica de cada usuario (estudiante, administrativo u otros), en especial el código leído del carnet personal.

6. Aportes y recomendaciones

Los aportes realizados a la compañía fueron entre otros: montaje inicial del documento sobre las políticas de seguridad, listado completo de proveedores y clientes con respectivos datos de contacto (solicitados en proceso de certificación), fichas técnicas de todos dispositivos de la empresa, todas las contraseñas en el administrador de passwords 'Keepass', backups de correos electrónicos, todos los informes entregados al cliente mayor desde marzo a julio y entre otros resalto la organización de todo el proceso en área comercial, que aceleró tiempos de respuesta hacia el cliente, fortaleciendo las ordenes de compras entrantes a la empresa.

Como recomendación al programa de Ingeniería de Telecomunicaciones veo bastante necesario una interacción mayor con la industria para poder lograr un programa más actualizado con las necesidades del mercado; debe hacerse un poco más de hincapié en temáticas de legislación, licitaciones y todo lo que fortalezca un perfil más comercial de ese profesional integral que busca formar la Universidad Santo Tomas. También estudiar la posibilidad de hacer acercamientos a empresas desde semestres como séptimo u octavo, no solo como visitantes sino también como laborantes, esto permitirá crear una visión más específica a los estudiantes, ayudándolos a crear aspiraciones laborales y fortaleciéndolos en cuanto a habilidades y destrezas.

7. Lecciones aprendidas

En el transcurso de las prácticas laborales se abordó diferentes áreas de desarrollo de la ingeniería a las vistas durante los estudios, estas fueron el área comercial y de ventas, donde se buscó dar soluciones tecnológicas a los clientes, fortaleciendo el conocimiento de la situación actual del mercado (proveedores/mayoristas/productos) y todo el tema de atención y de servicio al cliente.

Desde inicio de prácticas se buscó organizar la información entregada del área comercial, fortaleciendo los formatos de la empresa por códigos permitiendo así que la búsqueda futura de información de ventas de equipos y/o servicios, ordenes de compras, proveedores, garantías y demás fuese más sencilla; en otras palabras, se organizaron los procesos comerciales agilizando actividades, ahorrando tiempos y fortaleciendo la presentación y/o imagen de la empresa antes los clientes y proveedores.

Como aspecto favorable, se recalca el trabajo en equipo y los aportes de todo el grupo NTICS de las diferentes áreas, en diversas actividades, si bien cada empleado tenía definida cada una de sus funciones y objetivos, se desarrollaban reuniones y había un flujo positivo en la comunicación favoreciendo que todo el equipo fuese conocedor de las novedades comerciales, operativas, de compras y de proyectos.

8. Conclusiones

Al finalizar la práctica empresarial se logra cumplir con cada uno de los objetivos planteados inicialmente, dando respuesta de forma efectiva y con precisión a las actividades desarrolladas en las diferentes áreas, en forma ordenada, comprensible, por medios digitales y/o presencial; siguiendo los parámetros establecidos por la empresa, logrando incorporar y fortalecer conocimientos técnicos al área comercial, aportando valor a la compañía en procesos de atención al cliente.

Se logra brindar el soporte en temas de administración de seguridad al participar activamente en el proceso de certificación ISO 27001, dejando entregables como lo son el documento donde se establecen políticas de seguridad de la información, los backups y el programa que administra todas las claves de la empresa; El aporte realizado a la elaboración de políticas de seguridad de información brindará a la empresa un marco de trabajo que asegure la integridad, disponibilidad y privacidad de los datos.

Se realizaron actividades en otros departamentos al interior de la empresa, principalmente en área comercial; resaltando que inicialmente dicha área no contaba con una estructura de procesos, la cual se mejoró considerablemente con el desarrollo de la práctica.

De la trayectoria de estos meses en la empresa se puede concluir que los empleados no son conscientes de los objetivos que se pretende con el sistema de control de seguridad de la información. Por tanto, es fundamental el proceso de certificación ISO 27001 que se estuvo apoyando y la auditoría que se prestó al interior de la empresa, pues ayudó a reunir al personal y a direccionarlo en todo el proceso.

Referencias bibliográficas

[1] ISOTools Excellence, «SGSI,» 21 Mayo 2015. [En línea]. Available: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/. [Último acceso: 21 08 2019].

[2] IT Governance Blog ES Copyright ©, «IT Governance European Blog,» 14 Agosto 2019. [En línea]. Available: https://www.itgovernance.eu/blog/es/la-importancia-de-certificar-la-norma-iso-27001-en-su-empresa.

[3] isotools.org, «ISOTools,» [En línea]. Available: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf. [Último acceso: 14 08 2019].

[4] F. N. Solarte Solarte, E. R. Enriquez Rosero y M. d. C. Benavides, «Revista tecnologica ESPOL,» *Revista tecnologica ESPOL - RTE,* vol. 28, nº 5, 2015.

[5] Publicaciones Vertice S.L., Gestión de la calidad (ISO 9001/2008), España: Publicaciones Vertice, 2008.

[6] G. Disterer, «SerWisS,» Abril 2013. [En línea]. Available: https://serwiss.bib.hs-hannover.de/frontdoor/index/index/start/0/rows/10/sortfield/score/sortorder/desc/searchtype/simple/query/pdca/docId/938. [Último acceso: 1 Agosto 2019].