Información Importante

Apoyo en el desarrollo del modelo de Gestión de Seguridad y Privacidad de la información perteneciente a la política de Gobierno Digital.

Jhosep Said Ropero Martínez

Informe de Practica para optar el título de Ingeniero de Telecomunicaciones

Director

Edgar Mauricio Velasco Diaz

Universidad Santo Tomás, Bucaramanga

División de Ingenierías y Arquitectura

Facultad de Ingeniería de Telecomunicaciones

2020

Tabla de contenido

Pág.

Lista de Figuras

Pág.

Resumen

El presente trabajo describe las actividades realizadas durante la práctica empresarial en la Alcaldía de Arauca, desarrolladas en el área de sistemas; las actividades realizadas dentro de la práctica empresarial están principalmente enfocada en apoyar el Desarrollo de la política de Gobierno Digital dentro de la organización con énfasis en los Planes de Seguridad y Privacidad de la Información, Plan de Tratamiento de Riesgos de la Información.

Palabras Clave: Privacidad, Información, Política, Riesgos.

Abstract

The present work describes the activities carried out during the business practice in the Arauca Mayor's Office, developed in the systems area; The activities carried out within the business practice are mainly focused on supporting the development of the Digital Government policy within the organization with emphasis on the Information Security and Privacy Plans, the Information Risk Treatment Plan.

Key Words: Privacy, Information, Policy, Risk.

Introducción

El municipio de Arauca, es un ente territorial, que en el marco de sus competencias adelanta la gestión para la prestación de servicio públicos y sociales, el desarrollo físico local, la convivencia ciudadana y el control territorial, proyectados hacia el desarrollo económico y sostenible mediante acciones que fortalecen sus finanzas públicas. La práctica fue desarrollada en la administración municipal de Arauca, en el área de sistemas, enfocado en el apoyo al desarrollo de la política de gobierno digital, especialmente en la elaboración de los planes de seguridad y privacidad de la información, el plan de tratamiento de riesgos de seguridad digital, el catálogo de servicios, el mapa de riesgos de seguridad digital, que hacen parte de sus componentes transversales, con el fin de sentar las bases de seguridad digital en la entidad y sus servicios internos.

Este informe tiene como finalidad dar a conocer el proceso y funcionalidad de la política de gobierno digital desarrolla dentro de la administración municipal de Arauca, así como su importancia en una organización.

A continuación, se presenta el informe final del trabajo realizado en la práctica empresarial durante un periodo de seis meses, se describen los objetivos de la práctica, un marco referencial con conceptos básicos y fundamentales de la práctica, el perfil de la empresa, las actividades realizadas para dar cumplimiento a los objetivos, los aportes y recomendaciones, lecciones aprendidas y finalmente, las conclusiones

1. Justificación

La práctica empresarial es de vital importancia en el desarrollo de un estudiante universitario ya que esta permite un acercamiento al ámbito laboral y profesional, permitiendo al estudiante desarrollar sus capacidades y actitudes frente a un trabajo, aprendiendo de forma directa el trabajo en equipo, el trabajo bajo presión, aplicar los conocimientos teóricos a la práctica conocer la dinámica de una empresa real, todo esto foja la vida profesional de un estudiante, explotando todo el potencial de ellos y abriendo el camino en su vida profesional.

Hoy en día, realizar una práctica profesional permite adquirir experiencia y abrir oportunidades a futuros empleos, considerando la dificultad de conseguir un empleo o incluso una práctica, debido a la alta oferta de estudiantes en busca de empleo y prácticas profesionales, el mercado laboral se ha vuelto cada vez más exigente por esto es necesario que los estudiantes sean capaces de afrontar estos retos y puedan adquirir las herramientas necesarias para progresar y destacar en el ámbito profesional.

Gracias a todo esto las Universidades serán beneficiadas al formar profesionales íntegros, capaces de afrontar cualquier reto, generando orgullo por hacer parte del claustro universitario que les brindó la oportunidad explotar su potencial.

2. Objetivos

En esta sección se relacionan los objetivos de la práctica, tanto el general como los específicos.

2.1 Objetivo General

Brindar apoyo en el área de sistemas con la temática referente a la seguridad y privacidad de la Acompañamiento en el desarrollo del Modelo de Gestión de Seguridad y Privacidad de la información en la Alcaldía de Arauca siguiendo los lineamientos establecidos por el MinTIC el cual establece una guía metodológica para el desarrollo de políticas para la Seguridad y Privacidad de la información, creación de controles y procedimientos, gestión de riesgo y planeación general.

2.2 Objetivos Específicos

- Apoyar en el desarrollo de un Sistema de Gestión de Seguridad de la Información.
- Actualizar el Catálogo de Servicios.
- Actualizar la Política de Seguridad.
- Apoyar la creación del plan de Tratamiento de Riesgos de Seguridad de la Información.
- Apoyar en el Levantamiento de Activos de Información.
- Apoyar en la Gestión de Riesgos de Seguridad de la Información.

3. Marco Teórico

- **La Política de Gobierno Digital** tiene como objetivo promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores que generen un público en un entorno de confianza Digital, la política de gobierno digital consta de dos componentes que son TIC para el Estado y Tics para la Sociedad, orientados al desarrollo y la implementación de la política, y cuenta con tres habilitadores transversales que son la Arquitectura, Seguridad y Privacidad y Servicios Ciudadanos Digitales, estos permiten el desarrollo de los componentes de la política. [1]

Figura 1. Elementos de la política de Gobierno Digital. Adaptado del "Manual de Gobierno Digital" [2]

- **Seguridad y Privacida**d, este habilitador transversal busca preservar la confidencialidad, Integridad y disponibilidad de los activos de información de las entidades del estado, implementando los lineamientos de seguridad de la información en todos sus procesos, servicios,

sistemas de información, con el fin de garantizar el buen uso y la privacidad de los datos, a través de un modelo de seguridad y privacidad de la información. [1]

- **El Activo de Información** en relación con la privacidad de la información, se refiere al, activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. [3]

- **Modelo de Seguridad de la información** consiste en general los lineamientos de buenas prácticas en Seguridad y Privacidad de la Información para las entidades del estado, convirtiéndose en una herramienta para el uso estratégico de la identificación de riesgos potenciales y preservar la confidencialidad, integridad y disponibilidad de los activos de información. [4]

- **Políticas de Seguridad y Privacidad de la Información** establece los objetivos, controles Alcances y el nivel de cumplimiento, que garanticen seguridad y Privacidad de la Información para las entidades del estado, convirtiéndose en una herramienta para el uso estratégico de la identificación de riesgos potenciales y preservar la confidencialidad, integridad y disponibilidad de los activos de información. [5]

- **La gestión del Riesgo** en seguridad de la información es de vital importancia para brindar un marco de gestión de riesgos de seguridad en el cual se puedan identificar amenazas y vulnerabilidades que la entidad y sus activos de información pueda estar expuesta desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control, aumentar la confianza de las partes interesadas reduciendo el riesgo de ataque cibernéticos. [6]

- **Catálogo de Servicios TI** es el documento que sirve para describir todos los servicios de TI con los que cuenta la entidad; así como también para darle una idea a los funcionarios, terceros, aprendices, practicantes, proveedores de la Alcaldía de Arauca y la ciudadanía en general. de cuáles son estos servicios. [7]

4. Perfil de la Empresa

El Municipio de Arauca como entidad fundamental de la división Política/Administrativa del estado, le corresponde garantizar la prestación de los servicios públicos en los términos que determine la normatividad legal vigente, construir obras que demande el progreso, local, ordenar el desarrollo territorial, promover la participación ciudadana, realizar obras sociales y culturales, cumplir con las demás funciones que asigne la constitución y la ley. [8]

El Municipio de Arauca mediante la implementación de políticas de gestión y desempeño se proyecta a convertirse en un modelo de desarrollo socio-económico basado en los principios democráticos y de inclusión social participativa que agregar valor a su territorio y genera confianza en sus habitantes. [9]

La Administración Municipal de Arauca, orientará su gestión a satisfacer las necesidades y expectativas de la comunidad araucana a través de procesos claros que propicien el mejoramiento continuo la trasparencia y el control; basados en el desarrollo intégralo de su talento humano para que su desempeño garantice el cumplimiento y el goce efectivo de los derechos de los ciudadanos. [9]

La estructura organizacional de la Alcaldía de Arauca comienza con el Alcalde de Arauca, luego la oficina de Asesoría Jurídica y después se divide en las diferentes secretarias, Secretaria de Planeación, Secretaria de Gobierno, La Secretaria de Hacienda y Finanzas Publicas, Secretaria de Desarrollo Económico Sostenible, Secretaria General, Secretaria de Salud, Secretaria de Educación, Cultura, Deporte y Recreación, Secretaria de infraestructura, Secretaria de Inclusión Social y la Secretaria de Movilidad y Transporte. [10]

5. Actividades Realizadas

Las actividades desarrolladas durante el periodo de la práctica empresarial son descritas a continuación, cada una de ellas dándole cumplimiento a los objetivos específicos.

Objetivo 1: Apoyar en el desarrollo de un Sistema de Gestión de Seguridad de la Información.

- Analizar y estudiar la guía para el diseño un plan de seguridad y privacidad de la información.
- Estudiar el contexto actual de la entidad para definir los definir los objetivos y alcance del plan a diseñar.
- Diseñar y definir políticas y controles acordes la normatividad legal vigente con el fin de proteger los activos de información de la entidad.
- Definir controles para: manejo de equipos de cómputo, adquisición y mantenimiento de software/hardware, uso de la red, manejo de redes sociales, manejo de impresoras, computadores, portátiles y servidores, uso de dispositivos móviles, manejos de control de virus, manejo de switches y routers, uso del correo institucional, manejo de bases de datos, respaldo de la información, manejo de contraseñas y control de acceso, para el cumplimiento de las políticas de seguridad y privacidad de la información, garantizar la confidencialidad, disponibilidad e integridad de la información y controles para la protección de datos y privacidad de la información personal.

Objetivo 2: Actualizar el Catálogo de Servicios.

- Identificar los principales servicios que presta entidad tanto, y definir sus características en el catálogo de servicios.

- Identificar los funcionarios públicos responsables de los correos institucionales y actualizar el inventario de correos institucionales de la entidad.
- Actualizar el inventario de impresoras de la entidad.
- Realizar el inventario de teléfonos VoIP, Verificar que funcionario tiene asignado el dispositivo y que extensión maneja.
- Realizar el inventario de usuarios y equipos de planta.
- Identificar y realizar el inventario de los sistemas de información, con sus respectivas características.

Objetivo 3: Actualizar la Política de Seguridad.

- Alinear la Política de Seguridad sacada por resolución 0544 de 2013, que era justificable por la política de gobierno en línea, con el nuevo marco normativo legal vigente establecido por la política de gobierno digital. [11]

Objetivo 4: Apoyar la creación del plan de Tratamiento de Riesgos de Seguridad de la Información.

- Definir un modelo de gestión del riesgo, el cual se basó en la norma ISO/IEC 27005 aprobado por la agencia nacional de infraestructura.

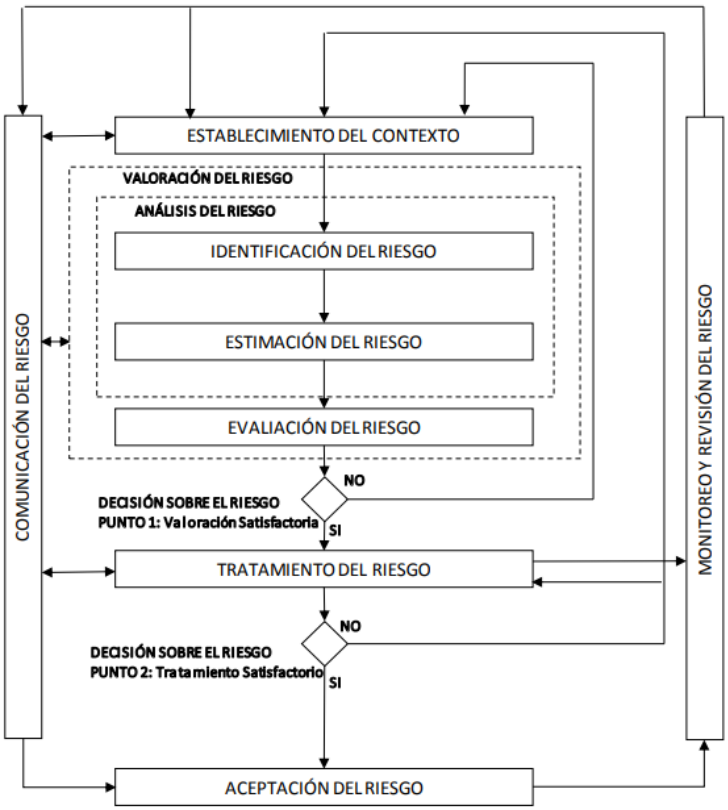

Figura 2. Modelo de Gestión del Riesgo, Adaptado de la norma NTC-ISO/IEC 27005 para la gestión del riesgo de la información. [12]

- Definir los criterios de impacto y que consideraciones a tomar.
- Definir los Criterios de aceptación del riesgo según lo definido por el MinTIC para las medidas contra el riesgo residual.
- Establecer como llevar a cabo la valoración del riesgo de seguridad y privacidad de la información.
- Definir el procedimiento para la identificación del riesgo y cuáles son los responsables del mismo.
- Definir como se debe estimar el riesgo según su probabilidad e impacto.
- Diseñar la matriz de riesgo para el análisis del riesgo inherente y residual, así como las zonas de riesgo y sus opciones de tratamiento.

- Proponer métodos de seguimiento de los riesgos de seguridad de la información.
- Proponer un cronograma para llevar a cabo la gestión del riesgo.

Objetivo 5: Apoyar en el Levantamiento de Activos de Información

- Crear formato/plantilla para el levantamiento de activos de información.
- Realizar una guía para el levantamiento de activos de información donde se establece los objetivos, el alcance, como se deben clasificar los activos de información, como determinar su criticidad y que metodología llevar a cabo para el levantamiento de los activos de información.
- Alimentar el banco de activos de información con información suministrada en la base de datos de la entidad priorizando los procedimientos y procesos misionales de la entidad.

Objetivo 6: Apoyar la gestión de Riesgos de Seguridad de la información.

- Realizar el formato/platilla del Mapa de Riesgos.
- Identificar y analizar los riesgos, amenazas, vulnerabilidades y consecuencias de seguridad digital, así como los activos de la entidad que pueden ser afectados.
- Identificar el riesgo inherente y residual.
- Realizar la valoración de los controles.
- Proponer Medidas de Respuesta como planes de contingencia y acciones preventivas.
- Proponer Periodos de Seguimiento.
- Realizar una Guía correspondiente para el Mapa de Riesgos.

6. Aportes y Recomendaciones

Los aportes realizados a la Alcaldía de Arauca fue la creación de los planes de seguridad y privacidad de la información, el plan de tratamiento de riesgos de la información, identificar falencias, opciones de mejora, establecer políticas y controles entorno a la seguridad digital con el fin de proteger los activos de información y los principios de integridad, confidencialidad y disponibilidad de estos, actualizar el catálogo de servicio de la entidad definiendo cada una de sus características, esto sirve para que los funcionarios públicos y demás involucrados con los procesos y procedimientos de la entidad conozcan los servicios que se están prestando, identificar los activos de información y elaborar una guía para la valoración y el levantamiento de los activos de información, también se realizó la gestión de riesgos de seguridad digital identificando las principales riesgos, amenazas y durabilidades que tienen presente los activos, así como las medidas de respuesta a tomar para reducir y mitigar el riesgo.

Como recomendación para la Alcaldía de Arauca seria aumentar la participación y disponibilidad de las diferentes áreas involucradas en el mapa de procesos de la entidad, esto con el fin de aumentar la eficacia y eficiencia en las labores entorno a la seguridad digital y demás procedimientos que requieran la participación de varios involucrados.

Como recomendación al programa de Ingeniera de Telecomunicaciones de la Universidad Santo Tomas de Bucaramanga, seria replantear el pensum académico teniendo en cuenta el avance de la tecnología, así como las principales necesidades que tengan las empresas en pro de formar un profesional íntegro y con habilidades que permita aplicar rápidamente en el mercado laboral, también me parece pertinente fomentar a los estudiantes a certificarse en los temas que se hayan

visto en algunas materias, como viene siendo: En Gestión de Proyectos-PMI(Certificación PMP), Certificación en ITIL, Certificación CCNA R&S, entre otras, esto es de vital importancia para destacar en el mercado laboral.

7. Lecciones Aprendidas

El estudiante a largo de su vida universitaria adquiere los conocimientos y habilidades básicas, al momento de ingresar a la vida profesional y laboral, estos conocimientos y habilidades van avanzando y creciendo poco a poco, esto se debe a que le permite al estudiante afrontar nuevos retos, trabajar bajo presión, a proponer soluciones e identificar oportunidades, por lo tanto, una práctica empresarial es una experiencia que todo estudiante debería tener,

En la vida laboral se puede observar grandes cambios, hoy puedes estar enfocado en área de la carrera y mañana otra, por lo tanto, es importante adquirir múltiples habilidades para adaptarnos en el entorno laboral al que ingresemos, para esto es necesario seguir estudiando y actualizarse con el fin de aspirar mejores oportunidades.

La investigación y actualización fue de vital importancia para el desarrollo de la práctica empresarial, es necesario estar informado del área laboral en la que se está desempeñado, estar pendiente de las capacitaciones, conferencias y demás información para los temas que se están desarrollando, en mi caso, asistí a múltiples conferencias virtuales sobre la Política de Gobierno Digital, resolviendo las dudas y demás preocupaciones sobre la ejecución de mi práctica empresarial.

Es necesario conocer la organización de empresa, ya que esto proporciona los métodos para que las procedimientos y procesos que se realicen puedan ejecutarse de forma correcta, agilizando las tareas y funciones de los involucrados mejorando la productividad.

8. Conclusiones

La política de Gobierno Digital nos plantea los lineamientos y parámetros para desarrollar e implementar la correcta practica para un modelo de gestión de seguridad de la información, nos describe la importancia y aporta las guías para el desarrollo de la misma, proteger y preservar los principios de integridad, confidencialidad y disponibilidad de los activos de información es de suma importación para una organización, por lo tanto el desarrollo de los documentos elaborados en la práctica empresarial, sirven como base para proteger los activos de información de la Alcaldía de Arauca, gestionar los riesgos de seguridad digital que pueden suceder, establecer contramedidas apropiadas y aumentar la confianza de la población entorno a la seguridad de la información que se maneja dentro de la entidad.

Referencias Bibliográficas

[1] M. d. T. d. l. I. y. l. Comunicaciones, «GobiernoEnLinea,» Ministerio de Tecnologías de la Información y las Comunicaciones , 07 04 2019. [En línea]. Available: https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf.

[2] MinTIC, «gobiernoenlinea,» 09 2018. [En línea]. Available: https://estrategia.gobiernoenlinea.gov.co/623/articles-74968_recurso_16.pdf. [Último acceso: 07 2020].

[3] MinTIC, «MinTIC,» 03 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf. [Último acceso: 07 2020].

[4] MinTIC, «MinTIC,» 07 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf. [Último acceso: 07 2020].

[5] MinTIC, «MinTIC,» [En línea]. Available: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/. [Último acceso: 07 2020].

[6] Funcion Publica, «Funcionpublica,» 10 2018. [En línea]. Available: https://www.funcionpublica.gov.co. [Último acceso: 07 2020].

[7] MinTIC, «Gobierno en Line,» [En línea]. Available: https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-8017.html. [Último acceso: 07 2020].

[8] Alcaldia de Arauca, «Arauca-Arauca,» [En línea]. Available: arauca-arauca.gov.co/NuestraAlcaldia/Paginas/Objetivos-y-Funciones.aspx. [Último acceso: 07 2020].

[9] Alcaldia de Arauca, «Arauca-Arauca,» [En línea]. Available: http://arauca-arauca.gov.co/NuestraAlcaldia/Paginas/Mision-y-Vision.aspx. [Último acceso: 07 2020].

[10] Alcalida de Arauca, «Arauca-Arauca,» 2020. [En línea]. Available: http://www.arauca-arauca.gov.co/Transparencia/PlanIntegrado2020/Plan%20Estrategico%20de%20Tecnologias%20de%20la%20Informacion%20PETI%202020%20-%202023.pdf. [Último acceso: 07 2020].

[11] Alcaldia de Arauca, «arauca-arauca,» 07 2013. [En línea]. Available: http://arauca-arauca.gov.co/Transparencia/Normatividad/RESOLUCI%C3%93N%200544%20SEGURIDAD%20EN%20LA%20INFORMACI%C3%93N%202013.pdf. [Último acceso: 07 2020].

[12] ICONTEC, NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27005, Bogota, 2009.