ISSN: 1692-7257 - Volumen 1 – Número 37 - 2021

Revista Colombiana de
Tecnologías de Avanzada

Recibido: 15 octubre de 2020
Aceptado: 5 de diciembre de 2020

SEGURIDAD DE LA INFORMACIÓN DE LA JURISDICCIÓN ESPECIAL PARA LA PAZ

INFORMATION SECURITY OF THE SPECIAL JURISDICTION FOR PEACE

M. A. Caballero-Paredes*, T. Velásquez-Pérez, L. Flórez-Villamizar ***.**

* **Universidad Francisco de Paula Santander Ocaña**, Maestría en Gobierno de TI,
Ocaña Colombia,
Correo Electrónico: macaballerop@ufpso.edu.co.
****Universidad Francisco de Paula Santander Ocaña**, Grupo de Investigación GITYD,
Ocaña Colombia,
Correo Electrónico: tvelasquezp@ufpso.edu.co.
*****Universidad Pedagógica Experimental Libertador UPEL**,
Rubio Venezuela
Correo Electrónico: Libardo.florez.lf@gmail.com

Resumen: La JEP es una víctima potencial de un ataque informático ya sea causado intencionalmente por terceros o por descuido del personal, lo que expone la necesidad de la presente investigación cuyo diseño es de corte cuantitativo con enfoque descriptivo y que tiene como propósito fortalecer los procesos, actividades y servicio es que realiza la JEP, así como el cumplimiento de lineamientos; para esto, se parte del diagnóstico de los riesgos inherentes al proceso, la identificación e integración de componentes de buenas prácticas para un modelo de gobierno de TI en la jurisdicción con énfasis en la seguridad de la información.

Palabras clave: seguridad informatica, ataques informaticos, jurisdiccion especial para la paz

Abstract: "JEP" is a potential victim for a cybernetic attack, either caused intentionally by third parties or in a way of personal carelessness, and that expose the necessity of this investigation that has a quantitative design with a descriptive aim and that has as a purpose to enhance processes, activities and services that "JEP" does, and as well the fulfillment of guidelines, and to do so, it starts from diagnosing risks that are part of the process, identification and integration of components of well practice for a government model of IT (Information Technologies) in jurisdiction with an information security emphasis.

Keywords: Informatic security, informatic attacks, special jurisdiction for peace.

1. INTRODUCCIÓN

El delito de mayor impacto en el 2018 fue el hurto a través de medios electrónicos, con más del 55% de los casos asociados a afectación patrimonial de los colombianos por ataques a sus cuentas bancarias. El "Malware" tiene como uno de sus propósitos tomar información y dinero, el ransomware es una de las ciber amenazas más

comunes y por las que se obtienen más lucro (Rubio, 2019).

Con la migración a la nube tanto de empresas públicas como privadas trae consigo muchas vulnerabilidades, unos estudios han orientado modelos de control informático y su incidencia en la seguridad de la información en el sistema de control de calificaciones de las universidades (Morante, 2019).

Por otro lado, se han diseñado modelos de seguridad informática con aplicaciones en la alcaldía de Fusagasugá, basados en la gestión del riesgo informático (Pulido y Mantilla, 2016, p. 19), así como, el diagnostico de seguridad al sistema informático de gestión de contratos de prestación de servicios (CPS) para la Universidad del Rosario, implementando protocolos de seguridad informática (Peñaranda, 2017, p. 1).

La Jurisdicción Especial para la Paz no se encuentra ajena a esta problemática y actualmente no cuentan con protocolos de respuesta en caso de que este siendo víctima de un ciber ataque. Esto aumenta los riesgos ante un ataque informático causado intencionalmente, por terceros o descuido del personal de la oficina.

En este trabajo se parte de la identificación de los estándares o buenas prácticas aplicables para la seguridad de la información, incluye un diagnóstico previo de los riesgos inherentes a la jurisdicción especial para la paz que permitan proponer un modelo de gobierno de TI enfocado a la seguridad de la información para la entidad.

2. ANTECEDENTES

Según la United Nations Office on Drugs and Crime (UNODC) para el 2011 a más de un tercio de la población mundial tenía acceso a internet, con una alta incidencia en los países desarrollados, con una edad menor a 25 años casi la mitad de los usuarios. Se proyectó que para el presente año, una proporción de seis dispositivos por una persona, poniendo en riesgo la evidencia electrónica vinculada con la conectividad del protocolo de internet "IP" (ONUDC, 2013).

Se pone en manifiesto el chantaje informático, como una amenaza real y requiere capacidad de adaptación con el establecimiento de esquemas que permitan enfrentarlo, siendo esto una tarea compleja que requiere una visión multidisciplinar (Cano,2016). Se ha debatido sobre reformas al código penal en materia de delitos informáticos, donde se tipifica como delito la conducta de aquellas personas que sin autorización modifiquen, destruyan o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad que sean tanto de particulares, como del gobierno federal (Rivera, Espinoza, Macgluff, & Fragozo , 2019)

Trabajos han abordado esta temática desde los estándares de gobierno de TI en el Hospital San Luis de Otavalao, se realizó el análisis de gestión de riesgos según el estándar NTE INEN-ISO/IEC 27005:2012 (Lopez, 2019). En el trabajo Gobernanza Corporativa de la TI según la Norma UNE-ISO/IEC 38500:2013) desarrollado en España, se elabora una guía de implantación de gobierno de TI y un modelo de autoevaluación, diseñado para mejorar el gobierno de las operaciones TI y hacerlas mas eficientes (Gomez, 2015).

En cuanto a delitos informáticos, se realizó un trabajo para el Sistema Penal Colombiano, proponeniendo un concepto sobre la seguridad informática, y su conexión con la realidad jurídica nacional, para entender como llego a ser objeto de protección por parte del estado (Montañez, 2017).

Con el trabajo "Delitos informáticos y Marco normativo en Colombia", se analiza el acceso a la tecnología y las dinamicas para el intercambio de información, así como el procedimiento criminal de los ciberdelincuentes, con el propósito de regular el uso de nuevas tecnologías en el territorio nacional, creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio (Montañez, 2017).

En el Modelo de Gobierno de Tratamiento de la información para la empresa Colombiana en la Globalización en la prospectiva del desarrollo Organizacional, proyectado como un elemento fundamental en la organización permitiendo la protección de datos personales, en cumplimiento de los derechos fundamentales de sus titulares". (Camargo, 2019)

3. METODOLOGÍA

Esta investigación se plantea bajo el paradigma cuantitativo y tiene un alcance descriptivo, Según Rodríguez, Erazo y Narváez, tienen como objetivo "Cuantificar los resultados, deben ser

estadísticamente representativas mediante la aplicación de un muestro representativo, de tal forma que, la información obtenida pueda sacar conclusiones estadísticas de la población en estudio" (2019, p. 4) Por otro lado, Valdiviezo, la investigación cuantitativa es aquella que: "Se encarga de la recopilación y análisis de información, se pone a prueba o comprueba mediante hipótesis, para lo cual utiliza un análisis estadísticos basadas en valores numéricos, lo cual tiene como propósito explicar el fenómeno estudiado" (2019, p. 8).

Según Valdiviezo, el alcance descriptivo: "describe las características o funciones de personas o cosas en un determinado espacio y en tiempo real, es requerido para obtener datos relevantes y precisos que han sido descubiertos por las investigaciones exploratorias" (2019, p. 9).

La población que se tomó como objeto de estudio para la realización del proyecto fueron todos los funcionarios que conforma la Jurisdicción Especial para la Paz; teniendo como muestra toda la población que conforma la unidad dentro de la JEP.

.

4. RESULTADOS

Partiendo de la revisión de estándares se parte de tres buenas prácticas como son la aplicación de la ISO 27000, los lineamientos legales establecidos por el MINTIC, y finalmente los componentes establecidos en COBIT 5.

La norma ISO 27002 es una recopilación de buenas prácticas para implementar en una empresa, se toman como una herramienta que permite reducir riesgos, asegurando la continuidad del negocio. Esto permite la toma de decisiones que apoya la seguridad de la empresa reduciendo las amenazas.

El ministerio de las TIC, mediante su modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

COBIT 5, es robusto, flexible e integrador, facilita que las empresas alinear sus objetivos estratégicos con TI apoyando el uso adecuado de recursos, gestionando adecuadamente los riesgos y disminuyendo los costos (Olivares, 2019). Por otro lado, Pinto y Cañón, explican que, provee un marco de trabajo integral que ayuda a: "las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas, ayudando a las empresas a crear valor manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo" (Pinto & Cañón, 2017).

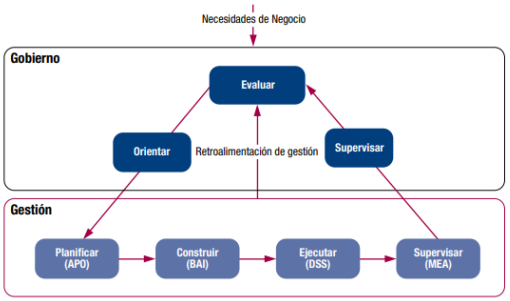

Figura 1. Gobierno y Gestión de TI
Fuente: (Isaca, 2012)

Se continúa con el diagnóstico previo de los riesgos inherentes a la jurisdicción especial para la paz. Es importante señalar que en el Acuerdo Final para la Terminación del Conflicto y la Construcción de una Paz Estable y Duradera- firmado el 24 de noviembre del 2016, El punto cinco del acuerdo busca la creación de un Sistema Integral de Verdad, Justicia, Reparación y no Repetición para garantizar los derechos de las víctimas el conflicto, lo cual conllevo a la creación de La Jurisdicción Especial para la Paz (JEP).

La jurisdicción en materia informática, dispone de una infraestructura tecnológica extensa, conformada por software, hardware, comunicaciones y más de 2000 usuarios que manipulan los equipos, tecnologías de la información, servicios tecnológicos como lo es el internet, los sistemas de información, plataformas Web.

Con el fin de apoyar y dar soporte a los desafíos institucionales de acuerdo al modelo de gestión para la administración de justicia – justicia digital, las operaciones y funcionalidades de las TI de la JEP, ha definido una arquitectura de aplicaciones y/o soluciones informáticas cuya vista de alto nivel se presenta a continuación:

Figura 2. Servicios tecnológicos JEP

El diagnóstico realizado permitió identificar las actividades pendientes de ejecutar, las cuales son:

- Implementación de diversos tipos de roles y permisos (secretaría general, subsecretarías, despachos, abogados)
- Radicación manual
- Asignación manual de radicados
- Creación/modificación de informaciones radicadas
- Asignación manual de Trámites
- Generación de Actuaciones y cambios de estado
- Cálculo de los términos de acuerdo con las actuaciones
- "Timeline" de todas las actuaciones de proceso
- Consulta estado proceso por comparecientes/victimas/apoderados

En la revisión de la aplicabilidad de los estándares, leyes y modelos, se evidenciaron falencias las cuales van desde la desorganización del flujo de la información por parte de los diferentes autores y usuarios de la información, hasta la reserva de la información manejada por los funcionarios (Ver Figura 3).

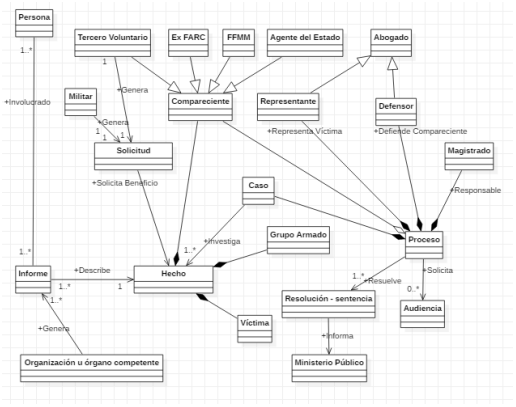

Figura 3. Esquema de hallazgos

Considerando los lineamientos anteriormente mencionados y en especial las buenas practicas establecidos en COBIT 5, se diseña un flujo de información que permite plantear una solución, como propuesta para la optimización del almacenamiento de la información con los criterios establecidos (Ver Figura 4).

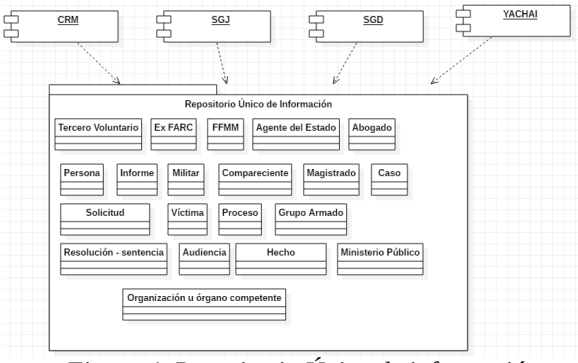

Figura 4. Repositorio Único de información

La figura plantea repositorio único de información, que incluye un conjunto de sistemas definitivos como son:

- Sistema CRM (Customer Relation Management) responsable de la gestión de todas las solicitudes a la JEP.
- Sistema SGJ (Sistema Gestión Judicial) responsable de gestionar todos los procesos asociados con la misionalidad de la JEP.
- Sistema SGD (Sistema de Gestión Documental) responsable gestionar transversalmente la gestión documental de la JEP.

Sistema YACHAY, responsable de la gestión con los entes externos de la JEP

5. CONCLUSIONES

Considerando los estándares aplicables a la seguridad de la información en el contexto de la JEP, se identificaron previamente el manejo de la información de los usuario internos y externos, donde se muestra como el flujo de información no mantiene una línea auditable, así mismo se plantean las buenas prácticas y las legislaciones y modelos adecuados para las organizaciones públicas, como son la ISO27000, los lineamientos de la MINTIC y el COBIT 5, con el cual se propone un repositorio único de información, el cual nos brinda una seguridad de la información, acorde a lo establecido en los planes tecnológicos de la jurisdicción especial para la paz.

REFERENCIAS

Rubio, I. (2019). El PAIS. Obtenido de "Antes debía entrar en tu casa. Ahora puedo conseguir toda tu información desde un ordenador": https://elpais.com/tecnologia/2019/10/17/actualidad/1571331272_536501.html

Pulido Barreto, A., & Mantilla Rodriguez, J. (2016). *Modelo para la implementacion del sistema general de seguridad informatica y protocolos de seguridad informatica en la oficina TIC de la alcaldia municipal de fusagasuga basados en la gestion del riesgo informatico*. Fusagasuga: Universidad Nacional Abierta y a Distancia.

Peñaranda Suarez, J. (2017*). Diagnostico de seguridad al sistema informatico de gestion de contratos de prestacion de servicios (CPS) de la universidad del rosario.* Ocaña: Universidad Francisco de Paula Santander Ocaña.

Cano, J. (2016). *Fraude informático: viejos trucos, nuevos entornos.* Medellín: ACIS.

Levet Rivera, C., Espinoza Maza , J., Macgluff Issasi, A., & Fragozo Teran, J. (2019). *La inconclusa reforma al Código Penal Federal en materia de delitos informáticos.* Interconectando Saberes, 12.

Lopez Quilumbanco, C. (2019). *Gobierno de TI basado en el esquema Gubernamental de seguridad de la información EGSI en el Hospital.* Ibarra - Ecuador: Universidad Técnica del Norte.

Gomez Gonzalez, E. (2015). *Gobernanza Corporativa de la Tecnologia de la informacion (T.I)* (Auditoria y control según la norma UNE-ISO/IEC 38500:2013). Leganés: Universidad Carlos III de Madrid.

Montañez Parraga, A. (2017). *Análisis de los delitos informáticos en el actual sistema penal* Colombiano. Bogotá: Universidad Libre.

Morante Mosquera, D. M. (2019). *Uso de los Modelos de Control Informático y su incidencia en la Seguridad de la Información en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo* (Bachelor's thesis, BABAHOYO).

Parra Calderon, J. (2019). *Delitos informáticos y Marco Normativo en Colombia.* Pitalito - Huila: Universidad Nacional Abierta y a Distancia UNAD.

Camargo Barbosa, J. (2019). *Modelo de Gobierno de tratamiento de la información para la empresa Colombiana en la Globalización en la prospectiva del Desarrollo Organizacional.* Ocaña: Universidad Francisco de Paula Santander Ocaña.

Olivares, C. (2019). Elementos para una metodología de gestión de identidad digital en la empresa.

ONUDC. Estudio exhaustivo sobre el delito cibernetico. *(informe borrador).* Oficina de las naciones unidas contra la droga y el delito, new york.

Pinto Ramírez, N. M., & Cañón Castillejo, M. (2017). Diseño de propuesta de una guía para la implementación de un modelo de arquitectura empresarial en los entes de control del estado colombiano para la gestión estratégica de riesgos de TI (Master's thesis, Universidad del Norte).

Rodríguez, D., Erazo, J., & Narváez , C. (2019). *Técnica cuantitativas de investigación de mercados aplicadas al consumo de carne en la generación millenial de la Ciudad de Cuenca (Ecuadro).* Revista Espacios, 1-12.

Valdiviezo Suarez, X. (2019). *Metodología de investigación cuantitativa en trabajos de graduación de la modalidad de titulación de la carrera de contabilidad y auditoría.* Universidad Técnica de Machala, 1-22.

Rubio, I. (24 de Octubre de 2019). El PAIS. Obtenido de "Antes debía entrar en tu casa. Ahora puedo conseguir toda tu información desde un ordenador": https://elpais.com/tecnologia/2019/10/17/actualidad/1571331272_536501.html

Pulido Barreto, A., & Mantilla Rodriguez, J. (2016). *Modelo para la implementacion del sistema general de seguridad informatica y protocolos de seguridad informatica en la oficina TIC de la alcaldia municipal de fusagasuga basados en la gestion del riesgo informatico*. Fusagasuga: Universidad Nacional Abierta y a Distancia.

Peñaranda Suarez, J. (2017*). Diagnostico de seguridad al sistema informatico de gestion de contratos de prestacion de servicios (CPS) de la universidad del rosario.* Ocaña: Universidad Francisco de Paula Santander Ocaña.

Cano, J. (2016). *Fraude informático: viejos trucos, nuevos entornos.* Medellín: ACIS.

Levet Rivera, C., Espinoza Maza , J., Macgluff Issasi, A., & Fragozo Teran, J. (2019). *La inconclusa reforma al Código Penal Federal en materia de delitos informáticos.* Interconectando Saberes, 12.

Lopez Quilumbanco, C. (2019). *Gobierno de TI basado en el esquema Gubernamental de seguridad de la información EGSI en el Hospital*. Ibarra - Ecuador: Universidad Técnica del Norte.

Gomez Gonzalez, E. (2015). *Gobernanza Corporativa de la Tecnologia de la informacion (T.I)* (Auditoria y control según la norma UNEISO/IEC 38500:2013). Leganés: Universidad Carlos III de Madrid.

Montañez Parraga, A. (2017). *Análisis de los delitos informáticos en el actual sistema penal* Colombiano. Bogotá: Universidad Libre.

Parra Calderon, J. (2019). *Delitos informáticos y Marco Normativo en Colombia.* Pitalito - Huila: Universidad Nacional Abierta y a Distancia UNAD.

Camargo Barbosa, J. (2019). *Modelo de Gobierno de tratamiento de la información para la empresa Colombiana en la Globalización en la prospectiva del Desarrollo Organizacional.* Ocaña: Universidad Francisco de Paula Santander Ocaña.

Rodríguez, D., Erazo, J., & Narváez , C. (2019). *Técnica cuantitativas de investigación de mercados aplicadas al consumo de carne en la generación millenial de la Ciudad de Cuenca (Ecuadro).* Revista Espacios, 1-12.

Valdiviezo Suarez, X. (2019). *Metodología de investigación cuantitativa en trabajos de graduación de la modalidad de titulación de la carrera de contabilidad y auditoría.* Universidad Técnica de Machala, 1-22.

ISACA, COBIT® 5 Framework. IL, USA: ISACA, 2012