ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES / Index A LOS AUTORES / To the AUTORS

Vol. 40 (Nº 30) Año 2019. Pág. 22

Determinación de aspectos clave de la seguridad de la información, procesos informáticos y recursos tecnológicos

Assessment of key aspects of information security, computer processes and technological resources

CAÑIZARES GALARZA, Freddy Pablo 1; GUILLIN SANABRIA, Alexander Adrián 2; MENDEZ GARCES, Erick Fernando 3; ARROBO LAPO, Estalin Vladimir 4 y BUENAÑO PESÁNTEZ, Carlos Volter 5

Recibido: 17/06/2019 • Aprobado: 23/08/2019 • Publicado 09/09/2019

Contenido

RESUMEN:
Se realizó una investigación descriptiva, de campo con los funcionarios de la Comisión de Tránsito del Ecuador UCT2 del cantón Santo Domingo, durante el período 2018-2019. Se utilizó la técnica de la observación para determinar aspectos clave de la seguridad de la información, procesos informáticos y recursos tecnológicos; además se utilizó la técnica de la encuesta con la finalidad de requerir información a un grupo socialmente significativo de personas acerca del problema en estudio.
Palabras clave: Comisión de Tránsito del Ecuador, seguridad de la información, procesos informáticos y recursos tecnológicos

ABSTRACT:
A descriptive, field investigation was carried out with the officials of the Traffic Commission of Ecuador UCT2 of the Santo Domingo canton, during the period 2018-2019. The technique of observation was used to determine key aspects of information security, computer processes and technological resources; In addition, the survey technique was used to request information from a socially significant group of people about the problem under study.
Keywords: Ecuador Transit Commission, information security, computer processes and technological resources

1. Introducción

Debido al desarrollo de las Nuevas Tecnologías de la Información y la Comunicación (NTIC), los adelantos en los servicios y modelos de comunicaciones e información, **y** el empleo sostenido y estandarizado a nivel mundial de la Internet; se han incrementado los ataques a los sistemas informáticos, situación que ha obligado a las empresas a buscar opciones que les faciliten la ejecución de análisis que adviertan, controlen y disminuyan los riesgos relacionados con la violación o vulnerabilidad de sus datos. Para dicha cuestión resulta

significativo dominar los principios que conforman cada modelo, entre ellos se encuentran los recursos del sistema de información requeridos para que la entidad marche positivamente y el alcance de los objetivos planteados, los eventos que pueden desatar un acontecimiento que ocasione daños en sus activos, la posibilidad de la efectivización de una amenaza, sus resultados, la probabilidad de que se cree un impacto en los bienes de la organización y en último lugar los procedimientos que se realizan para disminuir un riesgo (Abril, Pulido y Bohada, 2013).

Los riesgos de la información se manifiestan cuando concurren dos componentes: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades se encuentran estrechamente conectadas, y no puede establecerse ninguna derivación sin su existencia conjunta. Las amenazas deben tomar ventaja de las debilidades y pueden proceder de cualquier parte, interna o externa, conectada con el contexto de las entidades. Las vulnerabilidades se conforman como una debilidad en la tecnología o en los procesos que tienen que ver con la información, y como tal, resultan rasgos propios de los sistemas de información o de la infraestructura que la sostiene. Una amenaza, en términos escuetos, es cualquier situación o suceso que puede perjudicar la capacidad de que las organizaciones o los individuos puedan desarrollar sus actividades incidiendo negativamente sobre la información o los sistemas que la decodifican (Tarazona, 2007).

Los empresarios deben recibir instrucciones claras y decisivas que los auxilien para certificar la seguridad de la información en el complejo espacio de los negocios. Cada vez más se encuentran gerentes preocupados por comprender las normativas del negocio, sobre todo las relacionadas con las políticas de seguridad informática. El brindar productos o servicios mediante Internet sin tener en consideración la seguridad informática no solamente indica negligencia, sino que instituye una invitación para que sucedan eventos de seguridad que podrían perjudicar duramente la reputación y perturbar las fases del negocio (Dussan, 2006).

No obstante, los procedimientos aplicados en los distintos contextos resultan disímiles y eso ha establecido un escenario en el que los sistemas no siempre pueden dialogar entre sí o comprenderse (capacidad conocida como interoperabilidad) y en el que las semánticas, técnicas y organizativas o administrativas se encuentran todavía por superar. Dicha problemática supone el peligro, no solo de que las mejoras logradas para el individuo no se establezcan más que dentro de los límites geográficos de su país, sino de que el acceso a la información fuera de estos resulte más limitado que previamente (Abad, Carnicero, Etreros, Muñoz y Vaquerizo, 2009).

Sin dejar de lado estas consideraciones, la presente investigación determinó aspectos clave de la Comisión de Tránsito del Ecuador UCT2 del cantón Santo Domingo, Ecuador, referentes a la seguridad de la información, procesos informáticos y recursos tecnológicos, al no existir procedimientos a seguir en caso de ocurrir algún problema con los servicios o recursos informáticos requeridos para el ejercicio profesional.

2. Metodología

Se realizó una investigación descriptiva, de campo con los funcionarios de la Comisión de Tránsito del Ecuador UCT2 del cantón Santo Domingo, durante el período 2018-2019.

La población estuvo conformada por los 92 funcionarios de la Comisión de Tránsito del Ecuador UCT2 del cantón Santo Domingo, donde 66 fueron del personal operativo y 26 del administrativo.

En el presente estudio se utilizó la técnica de la observación para determinar aspectos clave de la seguridad de la información, procesos informáticos y recursos tecnológicos; además se utilizó la técnica de la encuesta con la finalidad de requerir información a un grupo socialmente significativo de personas acerca del problema en estudio para luego, mediante un análisis de tipo cualitativo, sacar las conclusiones que se correspondieran con los datos.

Como parte de los instrumentos a utilizarse en complemento de las técnicas de investigación se utilizó un cuestionario con el objetivo de lograr recolectar información para entender con mayor profundidad la problemática planteada.

Se utilizó la estadística descriptiva a través del cálculo de la frecuencia absoluta y la relativa, esta última en porcentajes y acompañada del intervalo de confianza (IC 95%) a través del método de la Normal ya que se cumplió la condición de np< 5 y nq> 5.

En realidad, aunque se trabajó con la población se quiso realizar inferencia a todos los que han pertenecido y pertenecerán a dicha comisión; por ello se emplearon además de las técnicas de la estadística descriptiva, las técnicas de la estadística inferencial, como los IC 95% y pruebas de hipótesis.

Se buscó asociación entre el tipo de personal, administrativo u operativo y las diferentes variables del estudio a través de la prueba no paramétrica Ji-cuadrado para lo cual hubo que emplear la corrección por continuidad, al tratarse de tablas 2x2 sin frecuencias esperadas menores que cinco y variables nominales dicotómicas.

Para ver la efectividad de la aplicación del Plan informático 2018 – 2022, basado en las normas ISO/IEC 27001:2013 para mejorar la seguridad de la información, procesos informáticos y recursos tecnológicos en la Comisión De Tránsito Del Ecuador UCT2 del cantón Santo Domingo, se aplicó la prueba no paramétrica McNemar al ser una comparación de tipo antes-después en variables nominales dicotómicas.

Para todas las pruebas de hipótesis se empleó un nivel de significación del 5%.

---

3. Resultados

3.1. Caracterización del sector

La comisión de Tránsito fue creada en la provincia del Guayas el 29 de enero de 1948, la misma que mantenía el nombre de Comisión de Tránsito del Guayas (CTG); para luego de 63 años con fecha el 17 de marzo del 2011, mediante la ley de Transporte Terrestre, Tránsito y Seguridad Vial ser reemplazada por la Comisión del Tránsito del Ecuador (CTE). Esta institución tiene como propósito el cumplir con los objetivos que la comunidad reclame, por ende, se ha generado por parte de las autoridades de tránsito, actitudes e índices de trabajo, proyectos y normativas que están determinando un cambio fundamental en la Institución.

3.2. Misión Institucional

Dirigir y controlar la actividad operativa de los servicios de transporte terrestre, tránsito y seguridad vial, en la red vial estatal y sus troncales nacionales y demás circunscripciones territoriales que le fueren delegadas por los Gobiernos Autónomos Descentralizados, con sujeción a las regulaciones emanadas por la ANT, la investigación de accidentes de tránsito y la formación del Cuerpo de Vigilantes y de Agentes Civiles de Tránsito.

3.3. Visión Institucional

Ser líder del control operativo técnico del tránsito en la red vial estatal, la formación de agentes y la investigación eficaz de los accidentes, procurando la disminución de la accidentabilidad, la fluidez y la seguridad del tránsito en las vías de la red estatal y sus troncales nacionales, con la activa participación de personal especializado.

3.4. Valores Institucionales

- Responsabilidad: Cumplir con el deber.
- Excelencia: Rendimiento sobresaliente y liderazgo de gestión.
- Eficiencia: Lograr la máxima productividad con los recursos que se disponen.
- Innovación: Aplicar la tecnología de punta en los procesos.
- Transparencia: Mantener a disposición de la ciudadanía todos los actos inherentes a la gestión.

3.5. Resultados del diagnóstico de la situación actual

El 100% de los encuestados dio a conocer que no existen procedimientos a seguir en caso de ocurrir algún problema con los servicios o recursos informáticos que necesita para laborar. También dijeron que no existe ningún manual que contenga normas o políticas de seguridad dirigidas al personal de la Comisión del estudio. Plantearon todos que en la institución no se controla el uso de dispositivos de almacenamiento, así como tampoco existe un plan de contingencia.

En la tabla 1 se encuentran respuestas de los encuestados acerca de la existencia de políticas, la entrega de contraseñas y la existencia de procedimiento para crear, cambiar o recuperar contraseñas y su asociación según el tipo de personal (administrativo u operativo).

Puede verse que 67 personas (73%, IC 95%: del 63% al 82%) dijeron que no existe política o normativa que indique el periodo o lapso de tiempo para el respaldo de la información institucional de los equipos de cómputo, en tanto hubo 25 personas que dijeron que sí existe esa normativa (27%, IC 95%: del 18% al 37%).

Más del 70% de los encuestados (71%, IC 95%: del 61% al 81%) respondieron que sí han facilitado sus contraseñas a otra persona fuera de la institución, mientras que alrededor del 30% (IC 95%: del 20% al 39%) manifestó que nunca ha entregado contraseñas a personas fuera de la institución.

Hubo 63 personas encuestadas (69%, IC 95%: del 58% al 78%) afirmaron que el departamento de tecnología de la CTE no cuenta con algún procedimiento para recuperar, cambiar o crear contraseñas de un ordenador; solamente 29 (31%, IC 95%: del 22% al 42%) dijeron que sí.

Al realizar la prueba Ji-cuadrado que buscó asociación entre el tipo de personal, administrativo u operativo y en las respuestas dadas no se encontró significación desde el punto de vista estadístico (p> 0.05). Puede decirse con una significación del 5% que el ser administrativo u operativo no condicionó ninguna de las respuestas dadas.

Tabla 1
Respuestas de los encuestados acerca de la existencia de políticas, la entrega de contraseñas y la existencia de procedimiento para crear, cambiar o recuperar contraseñas, y su asociación según el tipo de personal, administrativo u operativo

PARÁMETRO	FRECUENCIA	TOTAL	PRUEBA ESTADÍSTICA	
			JI-CUADRADO	p
EXISTE POLÍTICA O NORMATIVA				
SÍ	25	27	1,857	0,173
NO	67	73		
HA ENTREGADO CONTRASEÑAS				
SÍ	65	71	2,640	0,104
NO	27	29		
EXISTE PROCEDIMIENTO PARA CREAR, CAMBIAR O RECUPERAR CONTRASEÑAS				
SÍ	29	31	1,326	0,250
NO	63	69		

54 de los encuestados (59%, IC 95%: del 48% al 69%) afirmaron que sí han tenido algún

tipo de problema con la suspensión de los servicios que necesitan para realizar su trabajo diario en la oficina. Hubo 38 personas (41%, IC 95%: del 31% al 52%) que nunca han tenido ese problema. No se encontró asociación entre la existencia de problemas y el tipo de personal que labora en la oficina (X2CC= 2,963 y p-valor= 0,085); por lo tanto, la existencia o no de problemas no está condicionada por el ser administrativo u operativo de la oficina.

Consideraron 76 encuestados (83%, IC 95%: del 74% al 91%) que los equipos informáticos no se encuentran ubicados y distribuidos con las precauciones y seguridades necesarias para precautelar su integridad. En esta ocasión también se buscó asociación con el tipo de personal, administrativo u operativo, pero tampoco estuvieron asociados (X2CC= 2,279 y p-valor= 0,131); por ello se puede afirmar que ambas variables fueron independientes.

Tabla 2
Respuestas de los encuestados acerca de la existencia de algún tipo de suspensión de servicios necesarios y la ubicación de equipos informáticos, y su asociación según el tipo de personal, administrativo u operativo

PARÁMETRO	FRECUENCIA	TOTAL	PRUEBA ESTADÍSTICA	
			JI-CUADRADO	p
SUSPENSIÓN DE SERVICIOS				
SÍ	54	59	2,963	0,085
NO	38	41		
UBICACIÓN DE EQUIPOS				
SÍ	16	17	2,279	0,131
NO	76	83		

Todos los encuestados coincidieron en que un plan informático mejoraría la seguridad de información, infraestructura y recursos tecnológicos de la institución.

Posteriormente se procedió a aplicar el Plan Informático 2018 – 2022 basado en las normas ISO/IEC 27001:2013.

Resultados parciales de la aplicación del Plan Informático:

En la tabla 3 se muestran los resultados de la comparación antes-después de la aplicación parcial del Plan Informático, con lo cual se obtuvo significación estadística (p= 0,003). Con un nivel de significación del 5% existió suficiente evidencia para plantear que con la aplicación parcial del Plan Informático existió mejora en la seguridad de la información, procesos informáticos y recursos tecnológicos en la Comisión de Tránsito del Ecuador UCT2 del Cantón de Santo Domingo.

Tabla 3
Resultados de la comparación antes-después de la aplicación parcial del Plan Informático

RESULTADOS	SEGURIDAD DE LA INFORMACIÓN	PRUEBA McNEMAR
		p
ANTES DE LA APLICACIÓN PARCIAL	27,2%	0,003
DESPUÉS DE LA APLICACIÓN PARCIAL	72,8%	

Ante estos resultados de la aplicación parcial se logró reducir los riesgos operativos de la Comisión de Tránsito del Ecuador UCT2 del Cantón de Santo Domingo con respecto a la seguridad de la información, procesos informáticos y recursos tecnológicos.

4. Discusión

Varias investigaciones (Voutssas, 2010), (MANTILLA, 2018) estudian las aristas de diferentes modelos implementados en empresas, en función de conseguir una óptima seguridad de la información, mediante el correcto manejo de procesos informáticos y recursos tecnológicos.

El modelo propuesto por Burgos y Campos (2009) toma como base el análisis de los estándares y normativas de la seguridad de la información mostrada, junto a los alcances y tipos de aplicación, más el papel de la Oficina de Seguridad del Internauta y la efectivización de controles. Su medular contribución es constituirse como un facilitador en la implementación y/o aplicación de la seguridad de la información para TIC en cualquier clase de entidad. El diseño del modelo se establece sobre la aplicación práctica y real referida a las acciones que faciliten brindar seguridad a la entidad, la que, teniendo en cuenta sus propios requerimientos, lineamientos y visiones de negocio, busca conservar su información asegurada. Otro factor substancial que aporta este modelo, es que, por su diseño simple puede ser correlacionado sin mayor problema con las acciones que ejecuta cualquier clase de entidad, de forma tal que ella consiga asegurar la información según la realidad de TIC que posea.

Para instituir y gestionar un sistema de gestión de la seguridad de la información se puede emplear el ciclo PDCA (denominado también ciclo Deming), habitual en los sistemas de gestión de la calidad. El ciclo PDCA es un concepto generado inicialmente por Shewhart, pero adaptado a lo largo de décadas por teóricos del área de la calidad. Esta metodología ha probado su aplicabilidad y ha facilitado el establecimiento de la mejora continua en entidades de diferente naturaleza. El modelo PDCA o Planificar-Hacer-Verificar-Actuar (Plan-Do-Check-Act, por sus siglas en inglés), presenta una serie de etapas y acciones que aprueban establecer un modelo de indicadores y métricas comparables en el tiempo, de forma tal que se pueda cuantificar el desarrollo en la mejora de la entidad (Gómez y Álvarez, 2012).

Solarte, Enríquez y Benavides (2015) proponen una metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Los autores concluyen que no se muestra un compromiso positivo de las directivas, que los empleados no son consecuentes con los objetivos trazados referentes al sistema de control de seguridad de la información y que el personal del área informática no se encuentra capacitado para adjudicarse esta responsabilidad. Por ende, resulta esencial que las organizaciones tengan un marco normativo de seguridad, que posibilite la implementación de la auditoría basada en la norma ISO/IEC 27002.

Por su parte, Martelo, Madera y Betín (2015) diseñan un software para facilitar el control de los documentos creados a partir del proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Dicho software permite recibir, administrar y organizar la documentación producida en el proceso de implantación del SGSI. Para soportar dicho software, se estructura y efectúa un modelo que concreta actividades de gestión requeridas para la aprobación, revisión, actualización, estados y legibilidad en documentos mientras dure el ciclo de vida del SGSI. Esta propuesta engendró como derivación un módulo para la gestión documental que posibilita el control de documentos durante el proceso de implantación de un SGSI, bajo procedimientos del estándar ISO 27001.

5. Conclusiones

La evaluación del riesgo a escala empresarial resulta un conveniente instrumento para crear planes de contingencia y continuidad de la empresa, gracias a que posibilita a las entidades aminorar el riesgo y certificar el rendimiento de los sistemas informáticos. Resulta improbable eliminar un riesgo en su totalidad, lo que se puede ejecutar con la aplicación de metodologías es disminuirlo para que no forme ningún daño significativo al sistema

informático de la entidad.

No existe ninguna medida que pueda avalar un contexto libre de amenazas o sin riesgos para la información y para las entidades o sujetos que la necesitan. Por ende, resulta urgente acoger modelos apropiados de gestión de la seguridad de la información que posibiliten conseguir niveles positivos de protección, asentados en la correspondencia sistematizada de los disímiles mecanismos existentes, fundamentalmente, los componentes físicos de protección cimentados en hardware y software, los elementos administrativos como políticas y procedimientos, y el talento humano que administra, opera y emplea los recursos informáticos.

Con la aplicación parcial del Plan Informático existió mejora en la seguridad de la información, procesos informáticos y recursos tecnológicos en la Comisión de Tránsito del Ecuador UCT2 del Cantón de Santo Domingo.

Referencias bibliográficas

Abad, I., Carnicero, J., Etreros, J., Muñoz, J. F. y Vaquerizo, C. (2009). Algunas consideraciones sobre seguridad de la información en el Proyecto Europeo de Historia Clínica Digital (Proyecto epSOS). Derecho y Salud, 18(1), 87-98.

Abril, A., Pulido, J. y Bohada, J. A. (2013). Análisis de riesgos en seguridad de la información. Revista Ciencia, Innovación y Tecnología (RCIYT), 1, 39-53.

Burgos, J. y Campo, P. G. Modelo Para Seguridad de la Información en TIC. Concepción, Chile: Universidad del Bío-Bío.

Dussan, C. A. (2006). Políticas de seguridad informática. Entramado, 2(1), 86-92.

Gómez, L. Y Álvarez, A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España: AENOR Ediciones.

MANTILLA, Aníbal, R. Gestión de seguridad de la información con la norma ISO 27001:2013. Revista Espacios. Vol 39, Año 2018, Número 18, Pág. 05. Recuperado de: http://www.revistaespacios.com/a18v39n18/a18v39n18p05.pdf

Martelo, R. J., Madera, J. E. y Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información Tecnológica, 26(2), 129-134.

RINCÓN, I. K., SUAREZ-CASTRILLON, S. A. y SUAREZ-CASTRILLON, A. M. (2018). Incorporación de las TIC a los escenarios de emprendimiento para generar una cadena de valor en la creación de servicios online. Revista ESPACIOS Vol. 39 (Número 53). Recuperado de http://www.revistaespacios.com/cited2017/cited2017-13.html

Solarte, F. N., Enríquez, E. R. y Benavides, M. C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL – RTE, 28(5), 492-507.

Tarazona, C. H. (2007). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología, 28(84), 137-146.

Voutssas, J. (2010). Preservación documental digital y seguridad informática. Investigación Bibliotecológica, 24(50), 127-155.

1. Doctor en Ciencias de la Educación. Director de la Extensión Santo Domingo de la Universidad Regional Autónoma de los Andes (UNIANDES). Email: dir.santodomingo@uniandes.edu.ec

2. Ingeniero en Sistemas. Graduado de la carrera de Sistemas de la Universidad Regional Autónoma de los Andes (UNIANDES). Santo Domingo. Email: ss.alexanderguillin@uniandes.edu.ec

3. Magister en Sistemas de Control y automatización. Docente de la carrera de Sistemas de la Universidad Regional Autónoma de los Andes (UNIANDES). Santo Domingo. Email: us.erickmendez@uniandes.edu.ec

4. Magister en Evaluación y auditoría de Sistemas Tecnológicos. Docente de la carrera de Sistemas de la Universidad Regional Autónoma de los Andes (UNIANDES). Santo Domingo. Email: us.estalinarrobo@uniandes.edu.ec

5. Doctor en Ciencias de la Educación mención Informática Educativa, Magister en Informática Aplicada, experto en educación virtual. Trabajo como docente investigador en la Escuela Superior Politécnica de Chimborazo, especialista en infraestructuras de redes y comunicaciones, en generar, gestionar, implementar y administrar proyectos de tecnologías de la información y comunicación, así como también en el manejo de aplicaciones informáticas. Correo

Electrónico: cbuenano@espoch.edu.ec

Revista ESPACIOS. ISSN 0798 1015
Vol. 40 (Nº 30) Año 2019

[Índice]