Dom. Cien., ISSN: 2477-8818
Vol. 7, núm. 2, Abril-Junio 2021, pp. 835-857

DOI: http://dx.doi.org/10.23857/dc.v7i2.1831

Ciencias técnicas y aplicadas
Artículo de investigación

La Seguridad Informacional en el Ministerio de Transporte y Obras Públicas en Portoviejo

Information Security in the Ministry of Transport and Public Works in Portoviejo

Segurança da Informação no Ministério dos Transportes e Obras Públicas de Portoviejo

Leonardo Ramón Marín-Llaver [I]
leonardomarinllaver@gmail.com
http://orcid.org/0000-0002-2360-2472

Gregoria Gissela Loor-Intriago [II]
gisela01cq@gmail.com
http://orcid.org/0000-0001-9494-4288

Jeny Giselle Cobacango-Villavicencio [III]
jenny.cobacango@utm.edu.ec
http://orcid.org/0000-0002-2755-8712

Leonardo Vera-Viteri [IV]
verasleonardo2@yahoo.com
http://orcid.org//0000-0003-2822-0374

Correspondencia: leonardomarinllaver@gmail.com

Recibido:** 20 de febrero del 2021 ***Aceptado:** 20 de marzo del 2021 ** **Publicado:** 08 de abril del 2021

I. Doctor en Ciencias Pedagógicas, Magister en Ciencias Pedagógicas, Licenciado en Educación, Profesor Universidad Técnica de Manabí, Portoviejo, Ecuador.

II. Egresada de la Escuela de Bibliotecología y Ciencias de la Información de la Facultad de Ciencias Humanísticas y Sociales, Universidad Técnica de Manabí, Portoviejo, Ecuador.

III. Magister en Educación y Desarrollo Social, Licenciada en Contabilidad y Auditoría, Coordinadora de la Carrera Bibliotecología, Documentación y Archivología en la Universidad Técnica de Manabí, Portoviejo, Ecuador.

IV. Doctor en Ciencias de la Información, Magister en Relaciones Internacionales y Diplomacia, Sociólogo de profesión, Tercer Secretario del Servicio Exterior Ecuatoriano Ministerio de Relaciones Exteriores del Ecuador, Ecuador.

Resumen

El tema seleccionado para este estudio, tiene pertinencia, se trata de la Seguridad Informacional en el Ministerio de Obras Públicas. El mismo tiene gran significación, pues prepara a las empresas en el empleo de medidas preventivas, favoreciendo el resguardo y protección de la información. Es objetivo de este artículo evaluar el estado actual de la Seguridad Informacional en el Ministerio de Transporte y Obras Públicas en Portoviejo. La metodología aplicada fue de tipo descriptivo y retrospectivo con un enfoque cuantitativo-cualitativo, a través de la aplicación de métodos y técnicas, tales como: histórico-lógico, inductivo-deductivo, analítico-sintético, que ayudaron a fundamentar la investigación. También se aplicaron, encuestas al personal directivo y subordinados de la empresa, se empleó la observación participativa. Los resultados mostraron su nivel de efectividad en este sentido y se determinó que la empresa cuenta con buena Seguridad Informacional.

Palabras Clave: Seguridad informacional; obras públicas; información; resguardo; protección.

Abstract

The topic selected for this study is relevant, it is Information Security in the Ministry of Public Works. It has great significance, since it prepares companies in the use of preventive measures, favoring the safeguarding and protection of information. The objective of this article is to evaluate the current state of Information Security in the Ministry of Transport and Public Works in Portoviejo. The applied methodology was descriptive and retrospective with a quantitative-qualitative and bibliographic approach, through the application of methods and techniques, such as: historical-logical, inductive-deductive, analytical-synthetic, which helped to support the research. Surveys were also applied to the managerial and subordinate personnel of the company, participatory observation and the composition technique were used. The results showed its level of effectiveness in this regard and it was determined that the company has good Information Security.

Keywords: Informational security; public works; information; guard; protection.

Resumo

O tema selecionado para este estudo é relevante, trata-se de Segurança da Informação no Ministério das Obras Públicas. É de grande relevância, pois prepara as empresas na utilização de medidas

preventivas, favorecendo a salvaguarda e proteção das informações. O objetivo deste artigo é avaliar o estado atual da Segurança da Informação no Ministério dos Transportes e Obras Públicas de Portoviejo. A metodologia aplicada foi descritiva e retrospectiva com abordagem quantitativo-qualitativa, por meio da aplicação de métodos e técnicas, tais como: histórico-lógico, indutivo-dedutivo, analítico-sintético, que auxiliaram no suporte à pesquisa. Também foram aplicadas pesquisas a gerentes e subordinados da empresa, utilizando-se a observação participativa. Os resultados mostraram seu nível de eficácia neste quesito e constatou-se que a empresa possui uma boa Segurança da Informação.

Palavras-chave: Segurança da informação; obras Públicas; em formação; guarda; proteção.

Introducción

El auge que experimenta el desarrollo de las Tecnologías de la Información y la Comunicación (TIC), ha favorecido el progreso hacia una cultura digital, a la vez que se ha acentuado la necesidad de dar seguridad a la información que atesora los diferentes sectores, ya sean sociales, económicos, culturales, educativos, entre otros.

La información es un recurso de importancia capital para toda organización, por lo que su uso eficiente, puede representar la diferencia entre el triunfo o la frustración para una empresa; pues el triunfo de una organización, no depende únicamente de la forma en que cada persona maneja sus recursos materiales, sino que también considera de manera relevante el buen aprovechamiento de del conocimiento tanto del cliente como de directivos y empleados. Ante esta situación, las empresas a nivel mundial han decidido realizar tratamiento a la información generada.

Gracias al uso de la tecnología, el procesamiento y almacenamiento de la información de datos, en los actuales momentos es más sencillo su tratamiento, debido a que se encuentra un gran flujo de estos, principalmente en las redes, donde hay gran cantidad de textos e información orientados a la digitalización, haciendo que las tecnologías y las redes de información se sitúen en la frontera de una nueva revolución en la sociedad de la información, dando lugar entonces a la protección y seguridad informacional.

La seguridad informacional es empleada para proteger los datos que tiene, maneja y dispone una determinada organización. Es de significar que, a partir de la introducción de las nuevas

tecnologías, en el ámbito empresarial, se ha renovado la forma de utilizar la seguridad de la información, trayendo consigo incontables beneficios a nivel institucional.

En relación a lo expresado anteriormente a los efectos de este artículo la seguridad informacional, ha sido asumida como "la parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información de la misma". (Norma ISO 27001, 2007, p. 14)

Este tema ha sido ampliamente tratado y respaldado por documentos rectores, dándole su status legal. Entre los más significativos, pueden citarse los siguientes: Constitución de la República del Ecuador (Decreto Legislativo 0/ Registro Oficial 449 de 20-oct-2008, Ley Orgánica de Servicio Público, LOSEP (Ley 0 / Registro Oficial Suplemento 294 de 06-oct-2010), Ley Orgánica de la Contraloría General del Estado (Ley 73/ Registro Oficial Suplemento 595 de 11-ago-2009), Ley de Comercio Electrónico, Ley Orgánica de Transparencia y Acceso a la Información Pública. (Art. 12 literal C, Art. 18), Reglamento de la Ley Orgánica de la Contraloría General (Decreto Ejecutivo 548 / Registro Oficial 119 de 07-jul-2003), Acuerdo No. 166, Esquema Gubernamental de Seguridad de la Información EGSI (19 de septiembre de 2013), Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009 Código de Práctica para la Gestión de la Seguridad de la Información (Numeral 3.1, Numeral 4), entre otras.

A pesar de todos estos esfuerzos realizados por lograr avizorar a las entidades, empresas e instituciones en el logro de una permanente seguridad informacional, aún persisten irregularidades a nivel empresarial y social en este sentido, siendo las más representativas: escazas capacitaciones para preparar al personal directivo y empleados en general en la seguridad informacional; débil control de los dispositivos que se conectan a los computadores trayendo consigo en ocasiones la presencia de programas malignos; poco hábito de trabajar con copias de seguridad, por lo que la información puede correr el riesgo de perderla, ya sea por catástrofes de tipo natural o social.

Las consideraciones referidas anteriormente propiciaron el planteamiento del siguiente problema científico: ¿Cómo favorecer la Seguridad Informacional en el Ministerio de Transporte y Obras Públicas en Portoviejo?

Es objetivo de este artículo evaluar el estado de la Seguridad Informacional en el Ministerio de Trasporte y Obras Públicas en Portoviejo.

Metodología

Se realizó un estudio de tipo descriptivo, con enfoque cuali-cuantitativo, en el que se consultaron los fundamentos teóricos -metodológicos sobre el tema objeto de estudio, haciendo uso de los métodos histórico-lógico, inductivo–deductivo, analítico–sintético y el tránsito de lo concreto a lo abstracto: estos facilitaron la sistematización de los referentes teóricos acerca de la conceptualización de la seguridad informacional, importancia y actualidad, así como su metodología y valoración de la información derivada del estudio de los documentos.

La muestra fue seleccionada intencionalmente, participaron los 128 trabajadores y 27 directivos del Ministerio de Transporte y Obras Públicas en Portoviejo. También fue intencional la selección de la institución, pues precisamente en esta empresa la estudiante tutorada, realizó sus prácticas pre profesionales.

Métodos y técnicas

La complejidad del objeto de estudio, por su naturaleza y contenido, llevan a la utilización de diversos métodos y técnicas, con el propósito de poder interpretar, explicar y valorar el proceso investigativo.

A continuación, se ofrece una caracterización de los métodos y técnicas empleados para evaluar la variable: seguridad informacional.

Las encuestas a directivos para determinar el nivel alcanzado por estos en la gestión para asegurar la seguridad informacional. Por otra parte, también fueron aplicadas a los trabajadores del Ministerio de Transporte y Obras Públicas en Portoviejo, para obtener información acerca del estado real de la seguridad informacional.

La observación participativa; este tipo de observación, algunos autores la sitúan como una de las técnicas cualitativas más utilizadas para la recogida de información. La característica fundamental estriba en que el observador forma parte del grupo, propiciando un ambiente lo más natural posible. Estas observaciones fueron realizadas con el objetivo de valorar cómo se comportan los trabajadores y directivos en el cumplimiento de los indicadores de las dimensiones de la variable "seguridad informacional"; al igual que las encuestas, fueron ejecutadas en la empresa seleccionada para este estudio.

La revisión de documentos; fue utilizada con el interés de conocer cómo se comporta la seguridad informacional a partir de controles, auditorias, realizadas a la empresa. Así se trabajó con las actas de reuniones de directivos, consejos de dirección, actas de reuniones departamentales, resultados de controles internos, auditorias, visitas gubernamentales.

Los métodos utilizados aportaron datos necesarios acerca de la realidad del objeto de estudio de esta investigación, lo cual fue necesario procesar a través de tablas, análisis porcentuales, gráficos, entre otras.

Desarrollo

A propósito de la información como recurso en las organizaciones

La información como recurso tiene una gran importancia y significación, pues nuestra vida cotidiana está impregnada de ejecución de actividades, acciones, tareas, que exigen el conocimiento de algún tipo de información para garantizar el éxito en las mismas, para desenvolverse satisfactoriamente, o para evitar fracasos o riesgos. Además de contribuir a la mejora de los flujos informacionales, y optimizar los procesos organizacionales.

Los sistemas de información como activo intangible están presente en todas las organizaciones, por tales razones son considerados como un componente invisible, preciso, e inevitable para darle transparencia al resto de los recursos. Se coincide con Areito (2008), en que:

> "La seguridad de los sistemas de información es una disciplina en continua evolución. La meta final de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementando sistemas que tengan un especial cuidado y consideración hacia los riesgos relativos a las TIC de la organización, a sus socios comerciales, clientes, administración Pública, suministradores, etc.". (Areitio, 2008, p. 2).

Lo anteriormente expresado permite reconocer la relevancia de la información a nivel organizacional, al elevar el nivel de competitividad de las organizaciones a partir de una adecuada gestión de la información y el conocimiento. Es útil también señalar el rol estratégico que adquiere la información, aunque en ocasiones no se gestiona de forma efectiva, trayendo consigo un menor beneficio organizacional.

A decir de Fonquernie (2015). Se puede considerar que para que la información cumpla con sus objetivos es necesario que posea ciertas características, tales como: debe ser relevante: tiene que ser importante y la que necesitamos; debe estar actualizada: debe utilizarse en el momento de ser generada; debe ser comparable: que permita ser confrontada con datos similares; debe ser confiable: debe permitir que los usuarios puedan depender de ella al tomar sus decisiones; debe ser económica: debe ser más barata la obtención que la ganancia de su explotación; debe ser rápida: el acceso a la información debe realizarse de forma rápida y sencilla; debe ser de calidad: es importante que la información carezca de errores y sea completa; debe ser objetiva: no cabe opción a subjetividades; debe ser completa: el tener la información incompleta es peor que no tener nada; debe ser aplicable: la información debe ser adecuada para la toma de una decisión, además de ser importante y pertinente (Fonquernie, 2015, p. 1).

El acceso a la información de una empresa y su respaldo seguro es una necesidad latente en los momentos actuales, pues las organizaciones interactúan con disimiles y variados datos, los cuales pueden ser analizados, de tal manera que se pueda encontrar la información más actualizada y oportuna para la toma de decisiones y en este sentido las tecnologías de información juegan un papel rector, ya que pueden facilitar a las organizaciones la ventaja competitiva que garantiza el operar con información veraz, oportuna, certera y en tiempo real.

Lo expuesto en el párrafo anterior obedece a que el buen manejo de la información ofrece grandes ventajas a las instituciones, al constituir una herramienta insustituible para favorecer la planificación, ejecución y control de todos los procesos concernientes a la organización, e incluso permite planificar las actividades, tareas, y desarrollo futuro de cada organización.

Es de significar que en los momentos actuales las organizaciones están conscientes de ello y por eso hacen grandes inversiones para adquirir métodos sofisticados y seguros que faciliten la seguridad informacional en todos los órdenes; aspecto clave y determinante a la hora de tomar decisiones importantes para el funcionamiento de cualquier organización, institución o empresa.

A partir de experiencias expuestas por varias organizaciones y empresas tanto a nivel mundial como local, se puede advertir que el poco acceso, consulta, y resguardo de la información de una organización, o institución ha provocado, que algunas empresas subestimen este recurso, llegando a cometer errores nefastos en este sentido o en algunos casos emplearla solamente para alcanzar

cierto nivel de optimización y cumplimiento de las metas, en un momento determinado y luego prescindir de esta.

Es oportuno subrayar que la seguridad informacional, no se realiza de manera ocasional o temporal, pues su alcance tiene que ir más allá de todo este escenario, pues exige custodiar de manera permanente, toda la información que presenta una organización, de manera permanente, para que esta pueda ser objeto de estudio, análisis, balance, incluso auditables en diferentes momentos y de esta manera reconocer los aciertos y desaciertos de cada organización, entidad, empresa e institución, en concreto.

Los autores de este artículo coinciden plenamente con los criterios de Sánchez (2015), al reconocer que:

> La información archivada, resguardada y custodiada genera rendimientos, ya que puede revelar alternativas de inversión, reducir incertidumbres sobre ciertos procesos y, lo más importante, devela soluciones que pueden aplicarse de forma inmediata, al estudiar cierto proceso en la historia de la empresa, es decir ¿cómo fue concebido en un inicio?, ¿cómo ha ido evolucionando?, incluso si existe avance, estancamiento o retroceso en determinados procesos o estrategias trazadas en determinado momento. (Sánchez, 2015, p .19).

La idea expresada por Sánchez, J., acentúa la gran relevancia que tiene archivar, resguardar y custodiar la información, y no solo a nivel organizacional, sino personal también, por lo tanto, la palabra de orden en los momentos actuales respecto a la información, es garantizar su seguridad, y así evitamos a futuro tener que falsificar datos, ofrecer valores aproximados, y falsear la información.

En correspondencia con lo expresado con anterioridad, Córdova y González (2017), reconocen que "las entidades con una gran carga documental y ausencia de programas especializados, pueden tener incapacidad para procesar la información y por supuesto, para protegerla" (Córdova y González, 2017, p. 3)

Los autores de este articulo consideran que hay que resguardar, proteger y asegurar la información, pues ella en sí mismo representa poder, ya que las organizaciones e instituciones deben recurrir a ella en momentos en los que amerita tomar decisiones importantes para mantener los niveles de producción, analizar posibles crisis que pueden avecinarse, o mejorar los procesos, relacionados con su objeto social; sin perder de vista la inmediatez con que debe de actuarse, por lo que las

organizaciones, empresas e instituciones, deben adoptar nuevas formas de manejar los datos. Esto debe ser un lineamiento de estricto cumplimiento en todos los sectores, a partir de considerar la información y los recursos humanos, como los aspectos más valiosos de las empresas e instituciones.

Desde hace algún tiempo las organizaciones e instituciones han reconocido la importancia de asegurar, proteger y administrar los principales recursos con que cuentan, y la información se ha colocado en un lugar privilegiado en este sentido a nivel empresarial.

Es criterio de los autores de este artículo que, para poder revitalizar la significación de la información, las organizaciones e instituciones, deben dirigirla y controlarla de manera certera y eficiente, a la par de los demás recursos existentes. Los directivos y personal administrativo deben asumir con mayor conciencia y comprensión que hay costos asociados con la elaboración, distribución, seguridad, almacenamiento y recuperación de toda la información que es manejada en la organización. A partir de considerar que la información como recurso es de uso estrictamente estratégico para posicionar de forma ventajosa la empresa dentro de un negocio.

La seguridad de la información puede ser vista desde su rol estratégico en todos los procesos que genera la institución, al identificar con qué recursos (organización, procesos, tecnología), se debe contar para alcanzar la efectividad entre las actividades de resguardo o protección de los activos de información y la habilitación del acceso apropiado a los mismos. En este sentido, la seguridad de la información es un aspecto sumamente importante en la relación que se establece entre la institución, sus clientes, socios, proveedores y empleados.

Los autores de este artículo consideran que la seguridad de la información debe estar dirigida a proteger los activos de información de una organización, de hechos tales como: pérdida o uso indebido, para poder respaldar los objetivos en que se desarrolla la institución, aspecto que se abordará en el próximo epígrafe.

En torno a la seguridad informacional: conceptualización necesaria

La seguridad informacional en las organizaciones, reviste una importancia primordial, pues constituye la brújula que marca el nivel de competitividad de una organización o empresa, a partir de considerar que el poco control de la información puede llevar a un descenso que genera un

profundo impacto en el desarrollo de actividades, llegando al punto de poder desestabilizar todas las áreas.

El concepto de seguridad informacional, ha sido abordado por investigadores de diversas latitudes, siendo los más significativos para este estudio: Areitio y Bertolín (2008), Carmona, Nieto, Angelo, y Polo (2009), Whitman & Mattord (2011), Matalobos (2011). Areitio y Bertolín, (2008), definen la seguridad de la información como: "Un proceso que está compuesto de aspectos tecnológicos, organizacionales, de recursos humanos, económicos, de negocio, legales, de cumplimiento, etc. y es un factor crítico en las Instituciones públicas y privadas." (Areitio y Bertolín, 2008, p.7)

Carmona, Nieto, Angelo, y Polo (2009), aseguran que la seguridad de la información debe ser integral, empezando desde las personas involucradas, los procesos y los sistemas. (Carmona, Nieto, Angelo y Polo, 2009, p. 11). Por otro lado, Matalobos (2011) define a la seguridad de la información como "la aptitud para administrar acciones ilegales, malintencionadas o accidentales que puedan dañar los activos de información". (Matalobos, 2011, p. 2). Sin embargo, a los efectos de este artículo se asume la definición ofrecida por la Norma ISO, 27001, que la reconoce como "la parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información de la misma". (Norma ISO 27001, 2007, p.14)

Es importante advertir que el concepto de seguridad informacional, no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. Siguiendo con esta misma línea de pensamiento, se puede decir que la seguridad informacional, tiene un efecto significativo para el ser humano, ya que estimula la seguridad de respecto a su privacidad, la que cobra distintas dimensiones dependiendo de la cultura de la sociedad donde se desenvuelve.

El campo de la seguridad informacional ha evolucionado vertiginosamente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros. Se coincide con el ingeniero Fiallos (2020), durante su intervención en el Congreso Iberoamericano de Seguridad de la Información, en que:

> En la seguridad informacional es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. (Fiallos, 2020, p. 1)

A tenor de la expresado con anterioridad, se deja ver la gran importancia que tiene proteger y asegurar la información, para garantizar el éxito y despegue en una organización o institución.

La información puede clasificarse, según los estándares de la Norma ISO, 2011, de la siguiente forma:

- Crítica: es indispensable para la operación de la empresa.
- Valiosa: es un activo de la empresa y muy valioso.
- Sensible: debe de ser conocida por las personas autorizadas.
- Riesgo: es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.
- Seguridad: es una forma de protección contra los riesgos.

Se coincide con Fernández Barcell (2014), en que:

> Una correcta Gestión de la Seguridad de la Información estará dirigida a establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información. Si alguna de estas características falla no estamos ante nada seguro. (pp.1)

Lo expresado en el párrafo anterior deja ver el carácter procesal y de sistematicidad de la seguridad informacional, pues en su gestión hay que tener presente las fortalezas, debilidades y amenazas que se circunscriben sobre cualquier información, por lo que es necesario no subestimar las causas de riesgo y la probabilidad de que ocurran, además del impacto que puede tener.

En sentido generar se puede decir que la correcta gestión de la seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro.

Por la importancia que reviste la seguridad informacional para la sociedad en sentido general y para las organizaciones en particular, se ha estudiado sus bases legales, aspecto que se tratará en el epígrafe que se consigna a continuación.

Marco legal de la seguridad informacional: algunos puntos de vista

La información es uno de los activos más importantes en una institución o empresa, por lo que requiere ser asegurada y protegida de manera apropiada, incluso, respaldada desde los documentos legales e instruccionales, tanto a nivel de país, empresarial y hasta personal.

Primeramente, destacar que a nivel internacional la Organización Internacional de Normas Técnicas (ISO, International Organization for Standarization) en el año 2000, la norma ISO 17799 surge como la regla técnica de seguridad de la información, reconocida a nivel mundial. ISO 17799. Esta aboga por las prácticas exitosas de seguridad de la información.

Dentro de las bondades de esta ley, pueden citarse: protección de los bienes de la empresa (información y actividades), protección de la información en las comunicaciones y software, protección ante accesos malintencionados, prevenir alteraciones en las comunicaciones entre organizaciones, procesamiento seguro de la información, Mayor seguridad en la empresa, planeación y manejo de la seguridad más efectivos, mayor confianza en el cliente, auditorias de seguridad más precisas y confiables, menor responsabilidad civil, entre otras.

En medio de este escenario surgió la norma internacional ISO/IEC 27002, que se centra en las buenas prácticas para gestión de la seguridad de la información. En los días de hoy esa es fundamental para la consolidación de un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la continuidad y el mantenimiento de los procesos de seguridad, alineados a los objetivos estratégicos de la organización. En Ecuador la seguridad informacional también ha sido objeto de preocupación de políticos, empresarios, y población en general. Las primeras normas surgidas en aras de preservar la información, fueron las siguientes. En la Constitución de la Republica de Ecuador, Titulo segundo “De la información pública y su difusión”, se establece:

> Art. 6: Información Confidencial. Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, estatales y que las empresas tienen la obligación de proteger, empleando las vías y métodos establecidos por

la Ley. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. En la Sección tercera "Comunicación e Información", se refieren varios artículos con el propósito de salvaguardar la información. A continuación, referimos los mismos con el objetivo de establecer las bases legales de la información:

Art. 17, establece: EI Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto:

Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada.

Art. 18, reconoce:

Todas las personas, en forma individual o colectiva, tienen derecho a: (1) Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior; (2) Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Art. 19, plantea:

La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente. También en la Ley Orgánica de Protección de Datos Personales, aprobada el 19 de septiembre de 2019, pretende proteger la información de carácter personal que por cualquier motivo se deba compartir para tener acceso a ciertos productos o servicios.

Por su parte el Ministerio de Transporte y Obras Públicas (MTOP), elaboró el Acuerdo Ministerial N. 032-2017, el cual define las políticas internas respecto a la seguridad informacional, en el Ministerio de Transporte y Obras Públicas, estableciendo los lineamientos de actuación para los funcionarios (servidores y trabajadores), que laboran en la entidad, en relación con los recursos y

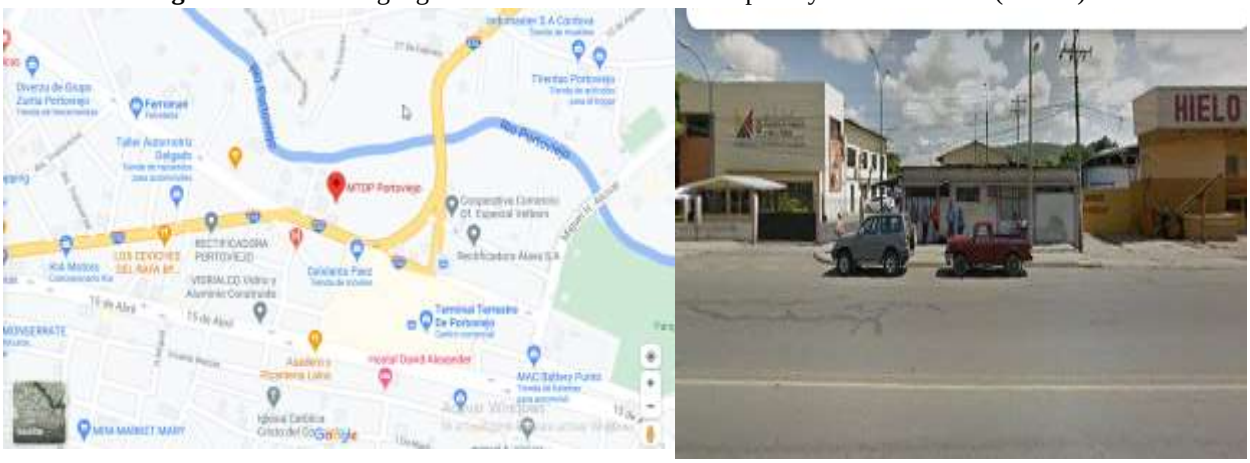
servicios de información, así como las sanciones para quienes violen las políticas seguridad de la información.

El Ministerio de Transporte y Obras Públicas: caracterización

El Ministerio de Transporte y Obras Públicas de Ecuador (MTOP) es un Ministerio del Estado Ecuatoriano, el cual es el rector del Sistema Nacional del Transporte. Fue creado por decreto ejecutivo N.8, del 8 de febrero del año 2007.

En Portoviejo el Ministerio de Transporte y Obras Públicas, se encuentra ubicado en la Av. Ejército y Cristo del Consuelo. Portoviejo, Manabí.

Figura 1: Ubicación geográfica del Ministerio de Transporte y Obras Públicas (MTOP).



Fuente: Elaboración propia con ayuda de Google maps

Su Misión, es formular, implementar y evaluar políticas, regulaciones, planes, programas y proyectos que garantizan una red de transporte seguro y competitivo, minimizando el impacto ambiental y contribuyendo al desarrollo social y económico del país.

Su Visión, es ser el eje del desarrollo nacional y regional mediante la gestión del transporte intermodal y multimodal y su infraestructura con estándares de eficiencia y calidad.

Su objeto social es, contribuir al desarrollo del país a través de la formulación de políticas, regulaciones, planes, programas y proyectos, que garanticen un Sistema Nacional del Transporte Intermodal y Multimodal, sustentado en una red de transporte con estándares internacionales de calidad, alineados con las directrices económicas, sociales, medioambientales y el plan nacional de desarrollo.

Valores que identifican la institución

- Apertura: admitir nuevas ideas, propuestas y enfoques, que nos permitan enriquecernos y mejorar el servicio a la ciudadanía.
- Calidad: hacer correctamente nuestro trabajo desde el inicio.
- Eficiencia: lograr los objetivos y metas programadas con los recursos disponibles en un tiempo predeterminado, mejorando la capacidad para cumplir en el lugar, tiempo, calidad y cantidad las metas y objetivos establecidos.
- Eficacia: optimizar el uso racional de los medios con que contamos para alcanzar un objetivo predeterminado; mejorando la capacidad de alcanzar los objetivos y metas programadas con el mínimo de recursos disponibles y tiempo, logrando su optimización.
- Honestidad: siempre pensar, hablar y actuar con simpatía a lo correcto y la verdad.
- Lealtad: cumplir y hacer cumplir nuestra misión, visión y valores institucionales, por encima de nuestros intereses personales.
- Mejora Continua: siempre buscar fortalecer y mejorar nuestro trabajo.
- Servicio: brindar a la ciudadanía servicios que les permita vivir mejor socialmente.
- Solidaridad: hacer nuestras las necesidades de formación e información.

El MTOP, asume dentro de su rol de entidad rectora de la política pública, la planificación y ejecución de planes, programas y proyectos, además de la formulación de políticas y regulaciones, vinculados a las actividades de construcción y conservación de la infraestructura del transporte, así como la gestión de las diferentes modalidades del transporte a nivel nacional. En este sentido, se han definido cuatro tipos de competencias: infraestructura del transporte; transporte terrestre, tránsito y seguridad vial; transporte aéreo y puertos y transporte marítimo y fluvial.

La institución posee trece departamentos, 155 trabajadores, de los cuales 27 son directivos. A continuación, se muestra una tabla que orienta sobre los datos enunciados con anterioridad.

Tabla 1: Distribución de trabajadores en el Ministerio de Transporte y Obras Públicas

TRABAJADORES POR DEPARTAMENTOS		
Departamentos	**Trabajadores**	**Directivos**
Secretaria zonal	3	1
Infraestructura de Transporte	4	1
Departamento de estudio	19	2
Departamento Socioambiental	1	1

Planificación Social	2	2
Asesor Jurídico	2	1
Comunicación Social	1	1
Dirección Distrital	5	1
Infraestructura distribuidora de Transporte	5	1
Departamento de Construcción	6	1
Gestión de Transporte	7	1
Conservación de la Infraestructura	41	10
Administración Financiera	32	4
TOTAL	**128**	**27**

Fuente: Elaboración propia

La Estructura Orgánica de Gestión Organizacional por Procesos del Ministerio de Transporte y Obras Públicas, está conformada por unidades técnicas, jurídicas, administrativas y financieras interrelacionados, alineados con la misión y el desarrollo institucional y define su estructura orgánica sustentada en los objetivos institucionales.

A partir de enero de 2013, se incorpora a la estructura organizacional del MTOP, la Coordinación General de Gestión Estratégica con las siguientes direcciones: Dirección de Administración de Procesos, Dirección de Tecnologías de la Información y Comunicaciones - DTIC, Dirección de Gestión del Cambio de Cultura Organizacional, como unidad de asesoría al Despacho Ministerial. La misma que consta en el estatuto y sus competencias son gestionadas por la unidad de Desarrollo Institucional y por la DTIC. En la actualidad esta Coordinación se encuentra en proceso de implementación.

Mediante el diagnóstico institucional, se identifica la situación actual de la institución, sus capacidades y limitaciones y la forma de operar de la entidad, para conseguir mejorar la gestión administrativa, técnica y política, lo cual optimizará resultados y procesos, tanto a nivel interno como externo.

Resultados

Las reflexiones teóricas y metodológicas en torno a la seguridad informacional, permitieron determinar que los propósitos de esta variable (seguridad informacional), se ajustan al desarrollo de conocimientos, y comportamientos.

Para el procesamiento de estos resultados se tomó como patrón lo establecido por Paúl Torres Fernández, Teresa León Roldan y Silvia Puig Urzueta (febrero, 2004); en el Manual para el

procesamiento de los datos educativos. Así, a partir de la frecuencia de respuestas de cada uno de los factores evaluados se precisó el índice de cada indicador en unidades de índices porcentuales (UIP), y desde estos se determinó el índice de cada dimensión, de los cuales se concretó el índice de la variable, lo cual se presenta en tablas para su mejor análisis.

Variable: Seguridad informacional

Dimensión 1: Cognitiva

Indicadores	Índice de cada indicador obtenido en los diferentes factores evaluados												Índice general del indicador
	Trabajadores						**Directivos**						
	A	%	M	%	B	%	A	%	M	%	B	%	
1.1	119	92.9	6	4.6	3	2.3	26	96,2	1	3.7	-	-	83.3
1.2	120	93.7	6	4.6	2	1.5	26	96.2	1	3.7	-	-	86.1
1.3	112	87.5	4	3.1	12	9.3	27	100	-	-	-	-	83.3
Índice de la dimensión													**84.23**

Fuente: Elaboración propia

Leyenda

Indicadores

1.1 Conceptualización de Seguridad Informacional

1.2 Valoración de las acciones ilegales, malintencionadas o accidentales que pueden dañar los activos de información

1.3 Conocimiento de políticas y programas que tienen la finalidad de conservar la confidencialidad, integridad y disponibilidad de la información

- A: Alto
- M: Medio
- B: Bajo

Indicador 1.1 Conceptualización de Seguridad Informacional: en este indicador los índices obtenidos en los trabajadores y directivos reflejan un alto índice de conocimiento respecto a la conceptualización de la Seguridad Informacional, pues el 92.9% de los trabajadores y el 96.2% de los directivos, obtuvieron altos resultados, al ser capaces de referirse con exactitud a los elementos claves que caracterizan y definen la Seguridad informacional. Solo el 4.6% de los trabajadores y el

3,7% de los directivos respondieron con algunos elementos ambiguos al respecto, logrando ubicarse en el nivel medio, y tres trabajadores que representan el 2,3% de los encuestados, no fueron capaces de definir ni caracterizar este concepto, para inscribirse en el nivel bajo. En el caso de los directivos ninguno alcanzó el nivel bajo.

De este análisis se infiere que existen un gran dominio a nivel de empresa sobre la seguridad informacional, siendo esto una cuestión indispensable para poder trabajar por la protección y resguardo de la información, ya que, para identificarse con algo, o sentir sentido de pertenencia hacia algo primero hay que conocerlo.

Indicador 1.2 Valoración de acciones ilegales, desmedidas, o accidentales que pueden dañar los activos de información: este indicador al igual que el anterior revela el dominio y control que existe sobre las acciones ilegales, malintencionadas o accidentales que pueden dañar los activos de información. Se puede notar que el 93.7% de los trabajadores y el 96.2 de los directivos ofrecen respuestas convincentes que denotan control y organización al respecto. Solamente 2 trabajadores, que representan el 1.5 de los que participan en este estudio, respondieron con criterios alejados de la realidad para ubicarse en el nivel bajo.

Indicador 1.3 Conocimiento de políticas y programas que tienen la finalidad de conservar la confidencialidad, integridad y disponibilidad de la información: en este indicador el 87.5% de los trabajadores lograron ubicarse en el nivel alto, pues sus respuestas demostraron un alto nivel de conocimiento sobre políticas y programas que tienen la finalidad de conservar la confidencialidad, integridad y disponibilidad de la información en la empresa. En el caso de los directivos el 100% alcanzaron el nivel alto. Es de significar que solamente el 9.3% de los trabajadores, representado por 12, se ubicaron en el nivel bajo al ofrecer solamente dos respuestas o ninguna correcta respecto a este indicador.

De este análisis se deduce que existen un gran dominio a nivel de empresa sobre la conceptualización y caracterización de la Seguridad Informacional, y acciones ilegales, desmedidas, o accidentales que pueden dañar los activos de información, siendo esto una cuestión indispensable para poder trabajar por su protección, salvaguarda y conservación. También alertó sobre la importancia de retomar espacios para divulgar y controlar el nivel de conocimiento respecto a las políticas y programas que tienen la finalidad de conservar la confidencialidad, integridad y disponibilidad de la información: Esta situación condujo a prestarle especial atención

a este indicador durante el proceso investigativo. Estos resultados en los indicadores llevan a la dimensión a obtener un índice de 84.23 UIP.

Dimensión 2: Comportamental

Indicadores	Índice de cada indicador obtenido en los diferentes factores evaluados												Índice general del indicador
	Trabajadores						**Directivos**						
	A	%	M	%	B	%	A	%	M	%	B	%	
2.1	52	44.5	47	36.7	29	22.6	23	85.1	2	7.4	2	7.4	83.3
2.2	128	100	-	-	-	-	27	100	-	-	-	-	100
2.3	114	89.0	10	7,8	4	3.1	27	100	-	-	-	-	83.3
Índice de la dimensión													**86.66**

Fuente: Elaboración propia

Leyenda

Indicadores

2.1 Participación en actividades de capacitación que impliquen preparación sobre la Seguridad Informacional

2.2 Postura exigente y combativa hacia las personas que manifiestan un comportamiento de conformidad tolerancia ante manifestaciones que deterioran y alteran la Seguridad Informacional

2.3 Realización de acciones dirigidas a implementar, revisar, mantener y mejorar la Seguridad Informacional

- A: Alto
- M: Medio
- B: Bajo

Indicador 2.1 Participación en actividades de capacitación que impliquen preparación sobre la Seguridad Informacional: constituye este el indicador de más bajo índice en la dimensión, el cual no rebasa las 83.3 UIP, donde el 22.6% de los trabajadores representado por 23 trabajadores, el 7.4% de los directivos, es decir (2) coinciden en señalar que no han participado ni han sido convocados a realizar actividades o capacitaciones que impliquen preparación relacionada con la Seguridad Informacional.

Este análisis demuestra que es necesario planificar capacitaciones con la participación de los directivos y trabajadores sobre dicha temática. También se necesita buscar métodos, tomar otras alternativas, hacer diversas actividades que motiven, sensibilicen e impliquen a todos los factores con énfasis en los trabajadores para participar en actividades relacionadas con la seguridad Informacional.

Indicador 2.2 Postura exigente y combativa hacia las personas que manifiestan un comportamiento de conformidad tolerancia ante manifestaciones que deterioran y alteran la Seguridad Informacional: Existe un consenso generalizado de todos los factores, es decir trabajadores y directivos en que mantienen una actitud exigente y combativa hacia las personas que manifiesten un comportamiento de conformidad, tolerancia ante manifestaciones que deterioran y alteran la Seguridad Informacional. Esta situación pudo constatarse a través de las observaciones realizadas durante el periodo de practica pre-profesional que realizó la estudiante en la empresa. Por tales razones en este indicador el 100% de los que participan en este estudio se ubican en el nivel alto. Así este indicador se presenta con un índice de 100% UIP.

Indicador 2.3 Realización de acciones dirigidas a implementar, revisar, mantener y mejorar la Seguridad Informacional: durante la evaluación de este indicador al decodificar los resultados de las encuestas, nos percatamos que el 89% de los trabajadores, es decir (119), se ubicaron en el nivel alto, al igual que el 100% de los directivos, al demuestran en sus respuestas conocimiento sobre la realización de acciones dirigidas a implementar, revisar, mantener y mejorar la Seguridad Informacional, solo 4 trabajadores, es decir el 7.8% de los que participan en el proceso investigativo, se inscriben en el nivel bajo, al ofrecer respuestas poco elocuentes y convincentes al respecto.

Los resultados obtenidos hasta el momento llevaron a los investigadores a la realización de observaciones al desempeño de trabajadores y directivos un día cotidiano de trabajo. Esto se efectuó en un período, de tres meses. El trabajo realizado condujo a los siguientes resultados:

- Se realizaron un total de 30 observaciones. Los indicadores más afectados que se vieron fueron: Realización de acciones dirigidas a implementar, revisar, mantener y mejorar la Seguridad Informacional Los resultados obtenidos a partir de la aplicación de estos instrumentos ponen en evidencia la situación real del Ministerio de Trasporte y Obras Públicas de Portoviejo, para favorecer la Seguridad Informacional.

Discusión

Este análisis indica la situación actual que presenta la Seguridad Informacional en el Ministerio de Obras Públicas de Portoviejo, lo que conduce a la afirmación que existe gran dominio sobre la conceptualización y caracterización de la Seguridad Informacional, y se muestra un ambiente exigente y de control al respecto. Sin embargo, se hace necesario potenciar capacitaciones para perfeccionar y actualizar el nivel de preparación en este sentido, sobre todo en los trabajadores.

Conclusiones

Los análisis específicos realizados y el recorrido epistemológico seguido se convirtieron en sustento teórico de la investigación; al expresar las potencialidades latentes en el interior del Ministerio de Transporte y Obras Públicas en Portoviejo que dirigidas administrativamente contribuyen a la seguridad informacional en la institución seleccionada para este estudio.

La seguridad informacional hoy día no es sólo un aspecto tecnológico, por el contrario, es una solución integrada que combina recursos organizacionales, procesos y tecnología.

Existen algunas debilidades, en el Ministerio de Transporte y Obras Públicas en Portoviejo, lo que se evidencia fundamentalmente en la escasa capacitación que reciben sobre el tema

Se propone la realización de una estrategia de capacitación que incluya actualización sobre el tema de la seguridad informacional y actualización técnica de equipos en aras de lograr favorecer la seguridad informacional en este plantel.

Referencias

1. Areitio, J. (2008). Seguridad de la información redes, informática y sistemas de información. España: Cengage Learning. Citado por Felipe Emiliano Arevalo-Cordovilla, ett all en Importancia de la seguridad en los Sistemas de Información. Revista FIPCAEC (núm. 20) Vol. 5, Año 5. Edición Especial 2020, pp. 136-144
2. Carmona, D. H., Nieto, E., Angelo, M., & Polo, R. (2009). Modelo de Madurez para la Seguridad de la Información. Revista Generación Digital Vol. 8 No. 1. Edición 15. octubre de 2009

3. Constitución del Ecuador (2008). Recuperado a parir de https://www.acnur.org/fileadmin/Documentos/BDL/2008/6716.pdf
4. Contraloría General del Estado. Normas de Control Interno de la Contraloría General del Estado, Última (2009). Recuperado a partir de http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cgepdf
5. Córdova, González, B. 2017). Acuerdo Ministerial 032 del 2017. Ministerio de Transporte y Obras Públicas, pp.3
6. Fonquernie González, Andrés (2015) La información en las empresas. En PublicaTIC. Deusto. Facultad de ingeniería ingeniaritza Fakultatea,pp.1. Recuperado a partir de https://blogs.deusto.es/master-informatica/la-informacion-en-las-empresas/.
7. Fernández Barcell, Manuel, (2014) Estudio de una estrategia para la implantación de los sistemas de gestión de la seguridad de la información. Universidad de Cádiz
8. Fiallo, Juan Carlos (2017) Importancia de la seguridad de la información. VIII Congreso Iberoamericano de Seguridad Informática y III Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información, 14 de enero, de 2017
9. ISO -International Organization for Standardization. (2011). Familias de las Normas ISO 27000, 19. Recuperado a partir de http://www.iso27000.es/download/doc_iso27000_all.pdf
10. Matalobos Veiga, J. M. (2011). Análisis de riesgos de seguridad de la información. Recuperado a partir de http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf
11. Sánchez, J. (2015) En torno a la información: algunos puntos de vista. Universidad de La Habana, Cuba. Editorial UH
12. Bibliographic references
13. Areitio, J. (2008). Information security networks, computers and information systems. Spain: Cengage Learning. Cited by Felipe Emiliano Arevalo-Cordovilla, ett all in Importance of security in Information Systems. FIPCAEC Magazine (No. 20) Vol. 5, Year 5. Special Edition 2020, pp. 136-144

14. Carmona, D. H., Nieto, E., Angelo, M., & Polo, R. (2009). Maturity Model for Information Security. Generación Digital Magazine Vol. 8 No. 1. Edition 15. October 2009
15. Constitution of Ecuador (2008). Recovered from https://www.acnur.org/fileadmin/Documentos/BDL/2008/6716.pdf
16. Office of the Comptroller General of the State. Internal Control Standards of the Comptroller General of the State, Ultima (2009). Recovered from http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cgepdf
17. Córdova, González, B. 2017). Ministerial Agreement 032 of 2017. Ministry of Transport and Public Works, pp.3
18. Fonquernie González, Andrés (2015) Information in companies. In PublicaTIC. Deusto. Fakultatea Engineering Faculty of Engineering, pp. 1. Recovered from https://blogs.deusto.es/master-informatica/la-informacion-en-las-empresas/
19. Fernández Barcell, Manuel, (2014) Study of a strategy for the implementation of information security management systems. Cadiz University
20. Fiallo, Juan Carlos (2017) Importance of information security. VIII Ibero-American Congress on Computer Security and III Ibero-American Workshop on Teaching and Educational Innovation in Information Security, January 14, 2017
21. ISO -International Organization for Standardization. (2011). Families of the ISO 27000, 19. Standards. Retrieved from http://www.iso27000.es/download/doc_iso27000_all.pdf
22. Matalobos Veiga, J. M. (2011). Information security risk analysis. Recovered from http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf
23. Sánchez, J. (2015) About information: some points of view. University of Havana, Cuba. Editorial UH.