Importancia de la gestión de la información en un Centro de Diagnostico Automotriz (CDA), para asegurar la confidencialidad, integridad y disponibilidad de la información.

Camilo Andres Rey Bernal
Katrina Lucia Bonilla Daza
Nancy Constanza Mahecha

RESUMEN

Los Centros de Diagnóstico Automotriz (CDA), hacen parte de los organismos de inspección (OIN) cuyo servicio consiste en examinar productos en este caso vehículos de transporte terrestre, en el cual se realizan las actividades de Revisión Tecno-mecánica y de emisiones contaminantes (RTM y EC) para lo cual se requiere contar con la acreditación del Organismo Nacional de Acreditación (ONAC), bajo los requisitos de la NTC-ISO/ 17020 de 2012 y la ley 1581de 2012 para el tratamiento de datos personales. No se reconoce el valor de la información y los factores de riesgo que vulneran el manejo de la información, por parte de los CDA dado que sus esfuerzos están encaminados a cumplir con los requisitos de acreditación que no los obliga a considerar estos riesgos para la implementación de controles que garanticen su eliminación o mitigación. La presente investigación reflexiona cómo desde la aplicación del SGSI, se permite a los CDA asegurar la confidencialidad, integridad y disponibilidad de la información, controlar los factores de riesgo que vulneran su manejo, asegurar el cumplimiento de sus procesos y requisitos de la NTC-ISO/IEC 17020 de 2012 y Ley 1581 de 2012 para el tratamiento de datos personales. Para ello se realizó una revisión bibliográfica, desde el punto de vista de varios autores, normatividad técnica y distintas diciplinas; que fueron base para el tema de discusión, factores de riesgo y beneficios de implementar un SGSI en un CDA. Se concluyo los factores de riesgo son trazables a los CDA y los beneficios en la implementación de un SGSI aseguran la confidencialidad, integridad y disponibilidad de la información.

INTRODUCCIÓN

El gobierno nacional es su intento de generar una industria competitiva en un mercado globalizado construye una infraestructura de la calidad, reglamentada en el decreto 1595 de 2015, dio origen a Subsistema Nacional de la Calidad (Sical), del cual hace parte los Organismo de Evaluación de la Conformidad (OEC).

> Los OEC son los encargados de la determinación o evaluación del producto, proceso, sistema, persona u organismo, para establecer si cumple con las condiciones establecidas en un reglamento técnico, una norma técnica o cualquier otro documento normativo, mediante actividades de inspección o realización de ensayos que soporten las certificaciones. (Giraldo, 2020, p.54)

Dentro de los Organismos de Evaluación de la Conformidad (OEC) existen una serie de organizaciones que se diferencian por el esquema de acreditación; laboratorios de ensayo, Organismo de Inspección (OIN), organismo validadores y verificadores, organismo de certificación, organismo de certificación de productos, organismos de certificación de personas y organismo de certificación de sistemas de gestión; los Centros de Diagnóstico Automotriz (CDA) hacen parte de los OIN, según Giraldo (2020) "la labor de los OIN consiste en examinar materiales, productos, instalaciones, plantas, procesos, procedimientos de trabajo o servicios, y determinan la conformidad de estos con los requisitos exigidos, sobre la base de un juicio profesional". (p.58). La presente investigación tiene como objetivo presentar los factores de riesgo en el aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de información y los beneficios que podría traer a este tipo de organizaciones la adopción de un Sistema de Gestión de la Información (SGSI).

El servicio de inspección que realiza los CDA consiste en examinar productos (vehículos de transporte terrestre), sobre los cuales llevan a cabo una serie de actividades que en conjunto se conoce como Revisión Técnico-mecánica y de Emisiones Contaminantes (RTM y EC), alineadas a una serie de normatividad técnica y legal aplicable. Para el desempeño de estas actividades los organismos deben cumplir con los requisitos de la NTC-ISO/IEC 17020 de 2012 y contar con la acreditación correspondiente por parte de Organismo Nacional de Acreditación de Colombia (ONAC). Dentro de un Sistema de Gestión (SG) que responde al cumplimiento de los requisitos de acreditación en un CDA, la información representa un valor importante e indispensable y se debe garantizar confidencialidad, integridad y disponibilidad, asegurar el tratamiento de datos personales conforme a la ley 1581 de 2012 y fortalecer el cumplimiento de los requisitos de acreditación.

La investigación sustenta como desde la aplicación del Sistema de Gestión de la Seguridad de la Información (SGSI), los CDA aseguran la confidencialidad, integridad y disponibilidad de la información, que por su naturaleza son evidencia del desempeño de los procesos y a su vez soportan la acreditación necesaria para su funcionamiento a través del cumplimiento a los requisitos de la NTC-ISO/IEC 17020 de 2012,

"Se entiende por información hechos sobre cualquier cosa que puede percibirse o concebirse que poseen significado". (ISO, 2015, p.24). En los CDA, como resultado de la prestación del servicio de RTM y EC, se obtienen datos los usuarios y de las pruebas realizadas sobre los vehículos; que poseen significado y dan razón de su estado. Dada la relevancia de esta información que avala la calidad del vehículo y adicionalmente el requisito de la NTC-ISO/IEC 17020 que exige asegurar la confidencialidad, la integridad y seguridad de la información, se constituye relevante la implementación de un SGSI.

Un Sistema de Información (SI) se define como: "aplicaciones, servicios, activos de tecnologías de la información y otro componentes para manejar la información"(Álvarez y Sánchez,(2013),p.23) los CDA no son ajenos a los sistemas de información, hacen uso de estos como medio para la administración de la información que se genera al aplicar sus procedimientos, para los CDA los sistemas de

información pretenden asegurar la integridad, confidencialidad y seguridad de los datos sensibles que se obtienen de los clientes e informes generados de la aplicación de las actividades de RTM y EC. “Se puede decir entonces, que el propósito de los SI es proveer datos e información a quien la necesite dentro de la organización a quien sirve”. (Bustamante, Shonerly, Valles, Ángel y Rodriguez,2020, p,150.).Una de las metodología reconocidas para la gestión de la información en las organizaciones es la NTC ISO/IEC 27001 de 2013, que establece los requisitos para un SGSI.

Acorde a la NTC-ISO/IEC 27000 de 2017; un sistema de gestión se define “Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos”(Incontec,2017,p.5); los OEC se estructuran bajo un sistema de gestión el cual tiene como objetivo, permitir a la organización definir políticas y administrar las interacciones entre sus áreas para lograr el cumplimiento de sus objetivos, para el caso de CDA garantizar la continuidad del negocio para la prestación del servicio y mantener la acreditación otorgada por ONAC, que hace parte de los requisitos legales para obtener su habilitación.

Cuando se habla de SGSI según la NTC-ISO/IEC 27000 de 2017 se define “Conjunto de políticas, procedimientos, directrices y recursos y actividades, asociados, que son gestionados de manera colectiva por una organización con el fin de proteger sus activos de información” (Iconte,2017,p.12); el objetivo de la norma es declarar los requisitos para que las organizaciones gestionen los riesgos de tipo humano, físico y tecnológico, sobre toda forma de información física y digital, usada por la organización.

La información hace parte de la naturaleza y objetivo de una organización, significa el valor y compromiso que llevan los que participan en el desarrollo de las actividades en una empresa, cómo se narran las tareas que a diario se realizan según la operación y los mecanismos para resguardar eso que los clientes, empleados y terceros producen para lograr las metas trazadas, guardando las evidencias, soportes, datos, experiencias y material de resultado. Así como la recolección de datos es importante, también lo es, donde reposa o es resguardada, además de identificar el responsable de su custodia ya sea un sistema de seguridad de la información o algún otro mecanismo propuesto por la organización.

Las organizaciones se preocupan cada vez más por proteger la información que se produce en su interior, por blindar esos datos que sus clientes proporcionan y que es un compromiso administrarlos de acuerdo con las políticas que se han generado. Es por eso por lo que los sistemas de seguridad de la información son importantes, valiosos y generan confianza para los clientes.

El artículo inicia con la presentación de los riesgos en el aseguramiento de la información en entornos empresariales; después explica los beneficios de la implementación de un SGSI y aportes a la competitividad en las organizaciones, y por último, se entregan las conclusiones de la investigación.

METODOLOGÍA

Como punto de partida se realizado una revisión sistemática de literatura con el fin de conocer los factores críticos en el manejo de la información en las organizaciones y los beneficios en la implementación de un sistema de gestión de seguridad de la información, para lo que se usó la ecuación de búsqueda:

"factores riesgo" en "información" y "ISO/IEC 27001"

Con la aplicación de la ecuación de búsqueda se identificaron referentes de autores y documentos de diciplinas como: administración y contabilidad, ingeniería y ciencias de la información; que sus conceptos y definiciones aportaron al tema de discusión y desarrollo del objetivo.

Para complementar la revisión de la literatura se analizó a profundidad la norma NTC-ISO/IEC 27001 Sistema de gestión de seguridad de la información, de la familia NTC-ISO/IEC 27000 la cual contempla los requisitos que debe cumplir las organizaciones para dar cumplimiento para implementar un SGSI, identificándose de este ejercicio las garantías que ofrece la implementación de un SGSI.

A partir de la identificación de los factores riesgo en el manejo de la información y los beneficios de la implementación de un SGSI, se realiza un análisis con la intención de validar si estos son trazables a los CDA e impactan de manera significativa el cumplimiento de los requisitos de acreditación NTC-ISO/IEC 17020 de 2012 y legales Ley 1581 de 2012; que obligan a que este tipo de organizaciones aseguran la confidencialidad, integridad y disponibilidad.

FACTORES DE RIESGO EN EL MANEJO DE LA INFORMACIÓN EN UN CDA

Los CDA como resultado de la prestación de su servicio tienen acceso a información sensible de los usuarios. Con la intención de proteger estos datos, el gobierno nacional por medio de la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”, establece que toda organización de carácter privado o público sea responsable del tratamiento de los datos personales de los titulares y debido a la condición que deben mantener de acreditado bajo el esquema de la NTC-ISO/IEC 17020 de 2012, asegure la confidencialidad, integridad y disponibilidad.

Szczepaniuk, Szczepaniuk, Rokicki y Klepacki (2020) afirman:

> En toda organización, la información se encuentra en diversos formatos, no es estática, sino que se encuentra adosada a procedimientos que van sufriendo cambios, y fluye mediante medios físicos como electrónicos, para ambos medios existe posibilidad de que la información sea violentada en cualquier momento. (p.3)

Para los CDA el manejo de los formatos en medios físicos como eléctricos, se presenta de forma inherente, son resultado de la ejecución de las actividades, fruto de esto son los datos que al momento de tomar valor para la organización se vuelven información, que se almacena y conserva, para asegurar su disponibilidad, confidencialidad e integridad. El garantizar estas variables difiere de cada organización, esto depende de la manera en la que administran sus activos de información.

> Hoy las organizaciones son más dependientes de sus redes informáticas y un problema que las afecte, por pequeño que sea, puede llegar a comprometer la continuidad de las operaciones, situación que inevitablemente se traduce en

pérdida económica, retraso en las operaciones y crisis de confianza por parte de los usuarios. (Beckers, Fassbender, Heisel, & Schmidt, 2012, p.6)

Los CDA como resultado de sus actividades hacen uso de diversos medios para administrar la información, situación generadora de riesgos como fugas de información; pérdida de la confidencialidad, integridad y disponibilidad; la conformidad de los requisitos de la normatividad técnica y legal aplicable, condición donde se evidencia problemas en la continuidad del negocio. Según García, Valles y Rodríguez (2020) los factores que contribuyen a la perdida de la información en la organización son factor humano, presupuesto, conocimiento, desastres naturales y agentes maliciosos; los cuales se presentan en el siguiente grafico:

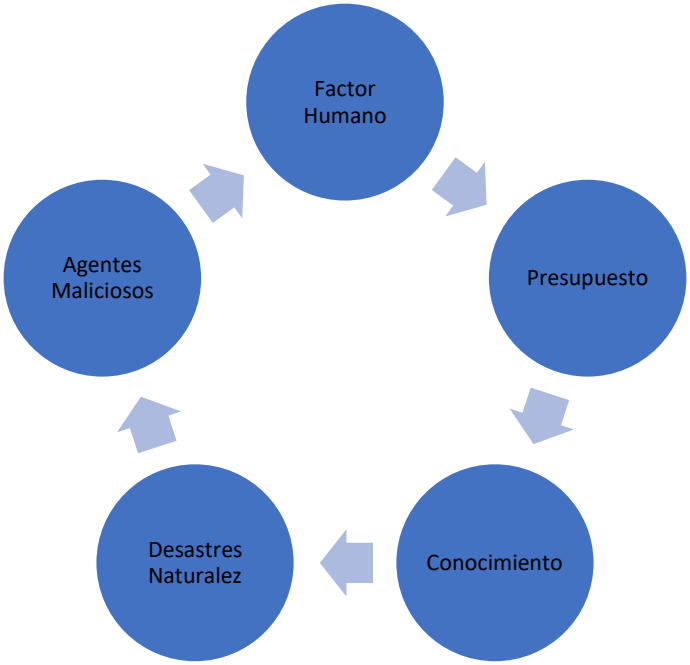


Figura 1. Riesgos que contribuyen a la perdida de la información.

Para los CDA estos factores representan riesgos que impactan la seguridad de los activos de información y son estos organismos los responsables de su tratamiento. ¿Pero de qué manera cada riesgo es trazable a estas organizaciones? y que impacto tiene en la integridad, confidencialidad y disponibilidad de la información.

A continuación, se presentan los factores de riesgo y la manera en que afectan a las organizaciones; se presentan argumentos que dan validez a la trazabilidad de estos factores a los CDA**.**

FACTOR HUMANO

Es imposible pensar que una organización sea cual sea de producción de bienes o servicios, desconozca la necesidad del uso de personas, para el caso de los CDA estas participan de manera activa en el servicio que se presta RTM y EC (Revisión

Técnico-Mecánica y de Emisiones Contaminantes) y en parte estos son responsable de garantizar un manejo adecuado de la información; como resultado de esta interacción. Según Altamirano y Bayona (2020, p.9) “El factor humano tiene un papel trascendental en cuanto al resguardo de información, ya que las personas son consideradas como el eslabón más débil dentro de una organización, pues causan graves pérdidas económicas y el robo de información”.

La pérdida de la confidencialidad, integridad y disponibilidad de la información no solo depende de los colaboradores y el servicio prestado al CDA, tienen acceso a esa información y está disponible para su consulta; la responsabilidad va mucho más allá; dentro de este factor se contempla a los exempleados que cuenten con acceso a la información almacenada y cuyo objetivo sea violentar la seguridad y hacer acciones indebidas que afecten a la continuidad del negocio.

En la prestación del servicio, los CDA son responsables del tratamiento de la información de los usuarios, por tanto, es importante el desarrollo de metodologías de aseguramiento de la información manejada por colaboradores actuales y desvinculados que permitan la confidencialidad, integridad y seguridad de los datos.

La identificación del factor humano como riesgo, predispone a que los CDA diseñen controles para eliminar y/o mitigar el riesgo que representan los empleados y exempleados, frente al cumplimiento del numeral cuatro (4) de la NTC-ISO/IEC 17020 de 2012 y la ley 1581 de 2012; contribuye de tal manera que se generen soluciones que partan desde las personas con las que cuenta o conto el CDA y se asegure el resguardo de la información.

Los controles diseñados son del orden administrativo, que se evidencian en clausulas descritas en documentos como contratos laborales, acuerdos de confidencialidad y reglamentos internos de trabajo que son de conocimiento y sobre los cuales los colaboradores, se comprometen a su cumplimiento; en caso de que se incumpla, el empleador tiene derecho a aplicar sanciones disciplinarias o económicas sobre el colaborador que cometió la falta. Este control es común en las organizaciones y los CDA los consideran para asegurar el la confidencialidad, integridad y disponibilidad de la información.

PRESUPUESTO

Cuando se habla de disponer de recursos en una organización, los CDA, están dirigidos en asegurar la continuidad de la prestación del servicio, del negocio, adecuación de equipos e instalaciones, mantenimiento del SG y formación del personal para garantizar su competencia, no se considera necesario o prioritario destinar recursos en actividades que tengan como propósitos el garantizar la confidencialidad, disponibilidad e integridad de los activos de información.

> Según Zuña, Arce, Romero y Soledispa (2019) indican que uno de los puntos débiles de las organizaciones es el bajo presupuesto que destinan a la seguridad de la información, pues algunas creen que es un gasto innecesario;

> ya que las organizaciones con limitado presupuesto ponen en riesgo la información y tienden a tener considerables pérdidas económicas. (p.489)

El identificar como factor de riesgo el no disponer de los recursos suficientes o no se tenga la intención de asignar un presupuesto, para implementar controles de carácter preventivo, donde permitan a los CDA prevenir y/o reaccionar de manera efectiva a ataques informáticos y tengan como intención violentar la seguridad y/o hacer acciones indebidas, pongan en riesgo la continuidad del negocio, el incumplimiento de los requisitos de acreditación y legales. Esto acarrea pedidas económicas, sanciones, la permanencia del negocio y perdida de la confiabilidad.

De ahí la importancia para los CDA de invertir en sistemas de información soportado y asegurado para que la información de sus usuarios sea almacenada, conservada, confidencial y esté disponible; sin embargo, los equipos tienen como objetivo el almacenar la información, sin desconocer de las posibilidades que ofrecen los sistemas de información y opciones, para la administración de la información, el mantener su integridad, confidencialidad y disponibilidad.

CONOCIMIENTO

El uso de sistemas de información en las organizaciones, como medio para la administración de los activos de información y los CDA hagan uso de estos, facilitan que sus colaboradores tengan disponibilidad de la información; el conocimiento suma como una de los factores de riesgo, resultado de la falta de formación sobre los colaboradores en el manejo de estos sistemas, que resultado del aumento del uso del internet, aumenta la vulnerabilidad y causa la perdida de la confidencialidad, integridad y disponibilidad de la información “El escaso conocimiento por parte del personal en una organización respeto a temas de seguridad, permiten mantener insuficientes controles y mecanismos de protección, para hacer frente a actividades maliciosas de manera efectiva” (Castillejos, Torres y Lagunes, 2016)

Dado que la NTC-ISO/IEC 17020 de 2012 obliga a los CDA, a mantener la confidencialidad de su información, estos organismo no consideran dentro de su esquema de formación, temas relacionados a la protección de los activos de la información y desde el uso de los sistemas de la información, se asegura la confidencialidad, disponibilidad e integridad de los activos de información. La formación del personal en este componente ha de considerarse como un aspecto que fortalece la competencia del organismo en cuanto al cumplimiento de los requisitos de acreditación y la reglamentación legal Ley 1581 de 2012. Arévalo, Bayona y Rico (2015,p.10) “la capacitación se convierte en un medio de sensibilización que conduce a la interiorización y al compromiso de cambio como escenario de competitividad empresarial”.

El sensibilizar al personal en el uso adecuado de los sistemas de información, el generar el conocimiento y habilidad, posibilita que los CDA mitiguen los riesgos resultados de la falta de conocimiento, la implementación de programas de sensibilización, que considere el conocimiento previo que se pueda tener por parte de

los proveedores en seguridad, el uso de internet de manera segura y el brindar formación en la protección online.

DESASTRES NATURALES

Los CDA son vulnerables a causas externas que representan un riesgo para su negocio, en cuanto a la administración de los activos de la información, estos riesgos son trazables a toda organización. Según Agwu, Labib y Hadleigh-Dunn (2019) quien describió la inevitabilidad de los desastres en las organizaciones, lo cual provocan que las instalaciones y los servicios se vieran afectados; por consiguiente, tienen pérdidas económicas y de información, además, señalan que la complejidad de las tecnologías y los procesos bien definidos, han evitado constantemente fallas catastróficas. (p.12)

A pesar del riesgo que representan los desastres naturales, el uso de los sistemas de información a resuelto en gran medida la vulnerabilidad, que representa para las organizaciones la perdida de la información debido a este factor de riesgo, el uso de una de las soluciones tecnológicas más comunes, cloud computing (CC) o computación en la nube, ha ayudado a reducir los costes de potenciar o implementar más ordenadores (Albakri, Zissis; Lekkas,2012).

El uso de estas tecnologías a mitigado y/o eliminado los riesgos que los desastres naturales representan respecto a la perdida de la información, al estar en la nube, los CDA asegurar su almacenamiento y esto es posible resultado de los avances en los medios para la digitalización de los documentos y almacenamiento en la nube.

Riego materializado que se considera en este factor de riesgos y que impactaron a las organizaciones, fue la pandemia por Coronavirus (COVID-19); que obligo a las organizaciones a pensar en el uso de las TIC y medios para administrar sus activos de información, que permitiera el considerar el teletrabajo y el cómo poner a disposición la información a los colaboradores vinculados bajo esta modalidad, es hay cuando los CDA evidenciaron la necesidad de digitalizar los documentos y considera el uso de medios para administrar los medios magnéticos, esto con el fin de dar cumplimiento a sus obligaciones; ejemplo de esto es el desarrollo de Auditorias internas o externas, de manera remota que obligaron el mantener información por medios magnéticos y considerar los riesgos asociados a esta nueva modalidad de administrar la información, respecto a la confidencialidad, integridad y disponibilidad del los activos de información.

AGENTES MALICIOSOS

Como resultado de un mundo más conectado, las perdidas por fallos de seguridad, Según Bander, Maarof y Syed “como virus, gusanos, troyanos y ransomware, que se encargan de acceder a los sistemas de información e interrumpir operaciones, con la intención de modificar su comportamiento original, realizando actividades como robo, alteración o destrucción de la información” (2018,p.11). Lo que hace vulnerable a los CDA y a toda organización es que en la actualidad estas son cada vez mas

dependientes de los sistemas de información, tecnologías de la información y uso excesivo del internet, que brinda metodologías para el almacenamiento de la información.

> Teniendo en cuenta que la información se ha convertido en una fuente de riqueza y de riesgo para las compañías (la protejan activamente o no), los miembros involucrados en la gestión de información necesitan entender la complejidad e importancia de su aseguramiento. (Cárdenas, Martínez y Becerra,2016, p.942)

NTC-ISO/IEC 17020 de 2012 incluye un requisito para que establezca que los CDA, guarden la confidencialidad de la información que obtiene de sus usuarios y comunicar en caso de que la información requiera ser divulgada a cualquier entidad de vigilancia. La confidencialidad afectada por los riesgos mencionados y que no son ajenos a los CDA, para tener en cuenta, ya que representan fuentes de riesgos que afectan el cumplimiento del requisito 4.2 confidencialidad de la NTC/ISO-IEC 17020 y los requisitos establecidos para el cumplimiento a la ley 1581 de 2012.

BENEFICIOS DEL SGSI (SISTEMA DE GESTIÓN DE LA INFORMACIÓN) Y APORTES A LA COMPETITIVIDAD.

La organización que adopte un SGSI, bien sea pyme, mediana o grande empresa, es consciente de los retos que afronta en la actualidad, en lo que respecta a la gestión de los activos de información y su tratamiento. Los CDA, para mantenerse a la vanguardia han implementado tecnologías para la administración de sus activos de información, aprovechando la aplicabilidad y las herramientas que ofrece la seguridad de la información, con el objetivo de mejorar los procesos y garantizar un producto competente. Estos organismos que han sido avalados y autorizados para ejercer y garantizarle a sus clientes un diagnóstico de su vehículo confiable, pertinente y actualizado, también ofrecen la protección de la información a través de políticas, documentos o aplicación del sistema de seguridad de la información.

> La seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de ordenadores y dispositivos de almacenamiento de información, pasando por la seguridad de sistemas y redes de tecnologías de información, a concentrarse en la gestión de alto nivel mediante políticas, procedimientos y controles basados en las personas (Nnolim, 2007,p.15).

Según Di Luca (2009,p.250) “La seguridad de la información aprueba asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización” (p.2). Los activos de información para cualquier organización en este caso para los CDA, sobre los cuales se centra esta investigación; disponen de valiosa información como resultado de las actividades que estos llevan a cabo para garantizar la prestación del servicio a los usuarios. Estas organizaciones se comprometen a validar y conservar la información que suministra el cliente y que mejor manera que utilizando un sistema de seguridad de la información eficaz y acorde a las exigencias del cliente y la organización.

Los beneficios que representa para las organizaciones e implementar un SGSI basado en la NTC 27001 de 2013, aporta al cumplimiento del numeral 4.2. Confidencialidad de

la NTC-ISO/IEC 17020 de 2012 y la reglamentación de tratamiento de datos personales descrita en la ley 1581 de 2012.

Todo SGSI requiere de un compromiso alto por parte de la alta dirección y su equipo, “El uso de políticas basadas en la ISO 27001 mejoran la gestión de la seguridad de la información, pues como argumentan Bustamante, Shonerly y Cuellar (2021,p.70), Ayudan a controlar los procesos de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información”, y es esto lo que hoy en día se exigen las organizaciones para continuar en la participación del mercado que cada vez más resaltan la importancia de desarrollar y mantener un sistema de gestión capaz de ofrecer a sus clientes la mejor disposición, mayor discreción y total control de la información como parte de sus servicios.

Pero de qué manera la gestión de la información, aportan a la competitividad, los CDA; “Los SI (Sistemas de información), se constituyen en una herramienta indispensable para lograr la productividad en las empresas porque ofrecen un control eficaz, permitiendo realizar una adecuada administración de los recursos”. (Cita Corta 1). Estas prácticas son necesarias e indispensables para garantizar los controles y la protección de la información, pero ya no desde lo que ofrece la organización, sino desde el aval de la norma ISO 27001 como soporte y mecanismo para asegurar un proceso de almacenamiento de la información en los CDA que sea confiable, coherente y eficaz. Es así como los centros de Diagnóstico (CDA) generaría diversas opciones basadas en la calidad del servicio, minimizando los riesgos de perdida de información o ataques por acciones maliciosas. La gestión de la información es indispensable y cada vez importante porque va encaminada a aportar a la toma de decisiones en las organizaciones y asegurar el blindaje de la información.

También aportan en el sentido de la aplicación de políticas de seguridad de la información en toda organización, pues es uno de los mecanismos eficaces para preservar la integridad, confidencialidad y disponibilidad, para brindar confianza a las personas que se benefician de los servicios. Parafraseo (Cita Larga 8), la creación y aplicabilidad de políticas para el manejo de la seguridad de la información exige a los CDA rigurosidad y exigencia a la hora de ofrecer el servicio de alta calidad y generar a sus clientes la satisfacción de que la información que han suministrado es valiosa e importante para la organización y que la toman como activo protegido donde se asegura el menor riesgo de que esta se pueda perder o manipular por personas o equipos ajenos a la organización en este caso un CDA.

CONCLUSIONES

Reconocer que existen factores de riesgo que impactan el manejo de la información, permite a los Centros de Diagnóstico Automotriz (CDA), validar si los controles que actualmente implementa para asegurar el cumplimiento del numeral 4.2. de la NTC-ISO/IEC 17020 de 2012 y la Ley 1581 de 2012, están dirigidos a mitigar o eliminar los factores de riesgo que por su generalidad son trazables a estas organizaciones; reflexionar si los controles diseñados e implementados, están alineados a los factores de riesgo humano, presupuesto, conocimiento, desastres naturales y agentes maliciosos.

Considerar la información como activo valioso para los CDA, incentiva a que se preste especial atención, el no desconocer los riesgos que ponen en peligro su manejo,

confidencialidad, integridad y disponibilidad; aporta razones suficientes para agregar valor e importancia a las metodologías de gestión de la información, lo que predispone a los CDA en el marco de asegurar cumplimiento de los requisitos de acreditación NTC-ISO/IEC 17020 de 2012 y Ley 1581 de 2012, evaluar la posibilidad de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), como medio para mitigar o eliminar los riesgos que impactan directamente el manejo de la información y como consecuencia llevar a estos organismos a destacarse por su enfoque basado en riesgos y prevenir situaciones que pongan en peligro la continuidad del negocio.

El masivo uso del internet y tecnologías de la información, a permeado en las organizaciones como elementos que brindan herramientas para dinamizar, flexibilizar y facilitar la disponibilidad de sus activos de información, los CDA no son ajenos a su uso; sin embargo resultado del desconocimiento y omitir el riesgo de usar las herramientas disponibles en estos espacios, aumenta la vulnerabilidad y dificulta que se diseñen o implementen controles que aseguren mantener la confidencialidad, integridad y disponibilidad de la información; es por eso que desde la implementación de un SGSI basado en la NTC-ISO/IEC 27001 de 2013, se establecen los requisitos para cualquier CDA, que brinda los lineamientos que conlleva considerar las condiciones externas e internas que pueden afectar la aplicación de controles reales y efectivos, el brindar evidencias objetivas respecto a su desempeño en el manejo de los activos de información y como garantiza la confidencialidad, integridad y disponibilidad.

REFERENCIAS

SZCZEPANIUK, E., SZCZEPANIUK, H., ROKICKI, T. y KLEPACKI, B., Information security assessment in public administration. Computers and Security [en línea], 2020. vol. 90, pp. 1-11. [Consulta: 17 junio 2020]. ISSN 01674048. DOI 10.1016/j.cose.2019.101709. Disponible en: https://doi.org/10.1016/j.cose.2019.101709.

Bustamante Garcia, Shonerly, Valles Coral, Miguel Angel, & Levano Rodriguez, Dany. (2020). Factores que contribuyen en la pérdida de información en las organizaciones. Revista Cubana de Ciencias Informáticas, 14(3), 148-164. Epub 01 de septiembre de 2020. Recuperado en 26 de noviembre de 2022, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992020000300148&lng=es&tlng=es.

Beckers, K., Fassbender, S., Heisel, M., & Schmidt, H. (2012). Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation. Availability, Reliability and Security (ARES), 2012 Seventh International Conference on , 242 (248), 20-24.

Arévalo Ascanio, José Gregorio, Bayona Trillos, Ramón Armando, & Rico Bautista, Dewar Willmer. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. Tecnura, 19(46), 123-134. https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10

ALTAMIRANO, J. y BAYONA, S., Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao [en línea], 2017. no. 25, pp. 112-134.

[Consulta: 29 mayo 2020]. ISSN 16469895. DOI 10.17013/risti.25.112-134. Disponible en: http://www.scielo.mec.pt/pdf/rist/n25/n25a09.pdf.

Zuña Macancela, E. R., Arce Ramírez, Á., A., Romero Berrones, W. J., & Soledispa Baque, C. J. (2019). Análisis de la seguridad de la información en las Pymes de la ciudad de Milagro. Universidad y Sociedad, 11(4), 487-492. Recuperado de http://rus.ucf.edu.cu/index.php/rus

BENZ, M. y CHATTERJEE, D., Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons [en línea], 2020. vol. 63, no. 4, pp. 1-10. [Consulta: 24 junio 2020]. ISSN 00076813. DOI 10.1016/j.bushor.2020.03.010. Disponible en: https://doi.org/10.1016/j.bushor.2020.03.010.

CASTILLEJOS, B., TORRES, C. y LAGUNES, A., La seguridad en las competencias digitales de los millennials. Apertura [en línea], 2016. vol. 8, no. 2, pp. 54-69. [Consulta: 15 mayo 2020]. Disponible en: http://www.scielo.org.mx/pdf/apertura/v8n2/2007-1094-apertura-8-02-00054.pdf.

AGWU, A., LABIB, A. y HADLEIGH-DUNN, S., Disaster prevention through a harmonized framework for high reliability organisations. Safety Science [en línea], 2019. vol. 111, pp. 1-15. [Consulta: 19 junio 2020]. ISSN 18791042. DOI 10.1016/j.ssci.2018.09.005. Disponible en: https://doi.org/10.1016/j.ssci.2018.09.005.

BANDER, S., MAAROF, M. y SYED, M., Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers and Security [en línea], 2018. vol. 74, pp. 1-48. [Consulta: 22 junio 2020]. ISSN 01674048. DOI 10.1016/j.cose.2018.01.001. Disponible en: https://doi.org/10.1016/j.cose.2018.01.001.

Cárdenas-Solano, L.-J., Martínez-Ardila, H., & Becerra-Ardila, L.-E. (2016). Gestión De Seguridad De La Información: Revisión Bibliográfica. El Profesional de La Información, 25(6), 931–948. https://doi-org.crai-ustadigital.usantotomas.edu.co/10.3145/epi.2016.nov.10

Giraldo, A. (2020). Guía practica para entender el Subsistema Nacional de la Calidad-SICAL. Bogota D.C, Colombia: Legis.

Icontec, (2015). Norma Técnica Colombiana NTC-ISO 9000 de 2015 Sistemas de Gestion de la Calidad-Fundamentos y Vocabulario. Colombia: Icontec.

Icontec, (2013). Norma Técnica Colombiana NTC-ISO/IEC 27000 de 2017 Tecnológica de La Información Técnicas de Seguridad Sistemas de gestión de Seguridad de la información (SGSI) Visión General Y Vocabulario. Colombia: Icontec.

Angulo, N., Zambrano, M., García, G., & Bolaños-Burgos, F. (2018). Propuesta metodológica de seguridad de información para proveedores de servicios de internet en Ecuador. MIKARIMIN. Revista Científica Multidiciplinaria, 4 (4), 165–176. http://45.238.216.13/ojs/index.php/mikarimin/article/view/1197

Altamirano Di Luca, Marlon Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso Avances, vol. 21, núm. 2, 2019 Instituto de Información Científica y Tecnológica, Cuba Disponible en: https://www.redalyc.org/articulo.oa?id=637869113010

Nnolim, Anene (2007). A framework and methodology for information security management. Michigan, United States: Lawrence Technological University, ProQuest

Dissertations & Theses (PQDT) database; 353 pp.
http://gradworks.umi.com/32/96/3296872.html

Castillo, C., Herrera,A.,Rico, L., Salva, S., Sarmiento,J.,Tejerina, M.,&Villarrubia, L.(2013). Sistemas de Información Gerencial en los procesos de negocio de las PyMEs de Jujuy. XV Workshop de investigadores en ciencias de la computación, Paraná, Entre Ríos, 1032-1047.

Montesino, R. (2009). Gestión de la seguridad informática: de la teoría a la práctica. IX Seminario Iberoamericano de Seguridad en las Tecnologías de la Información, La Habana, Cuba.

Alvarez Gonzales, M. A, Sanchez Torrecillas, L.F, Análisis de riesgos de activos de la informacion para área de infraestructura de una compañía de servicios financieros [Tesis de especialización, Universidad Piloto de Colombia]. Repositorio Institucional-Universidad Piloto de Colombia.

Icontec, (2017). Norma Técnica Colombiana NTC-ISO/IEC 27000 de 2017. Tecnología de la información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información (SGSI). Visión general y vocabulario. Colombia: Icontec.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012.D.O.No. 48587.