Artículo **RevistaAdministracion y Finanzas**
Marzo 2017 Vol.4 No.13 53-66

"Fuga de información" una práctica que se remedia con la Auditoría ISO/IEC 27002

RAMOS, Johanna*†, FACUY, Jussen, PERALTA, Fabiola y ALEJANDRO, María

Recibido Ocutbre 2, 2017; Aceptado Diciembre 8, 2017

Resumen

En la actualidad todas las instituciones sin importar el tipo que esta sean: administrativas, académicas, de negocios etc., poseen datos que al ser procesados se convierten en información, la misma que se la cataloga como el activo más importante de cualquier organización, es así como se manifiesta ***"Quien llegase a tener la información tiene el poder"***, y quien llegará a obtenerla sea esta para manipular, extraer o hurtar puede convertirse perjucial para la empresa, ante lo expresado existen un sin numeros de equipos electrónicos y aparato de segurdades que en muchos de los casos la información se sigue filtrando, fugando y perdiendo, en vista que la seguridad física mediante mecanismo electrónicos no son los suficiente aparece ñas normas ISO/IEC 27002 estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirementse) la versión actual 27002:2013, la misma que se convierte en una herramienta muy importante para las organizaciones sean estas de cualquier escala, porque proporciona recomendaciones para establecer mejores prácticas en la gestión de la seguridad de la información, todo gracias a la caracterización de los principios de administración y al Ciclo de Deming (PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), el presente documento busca esclarecer como la norma puede mantener la confidencialidad, integridad y disponibilidad de información son esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen institucional.

Auditoría informática, ISO 27002, ISO/IEC, información

Abstract

At present, all institutions, regardless of their type: administrative, academic, business, etc., have data that when processed become information, the same that catalogs it as the most important asset of any organization , is how it manifests "Who would get the information has the power", and who will get to be it to manipulate, extract or steal can become prejudicial to the company, before the expressed there are a number of electronic equipment and security apparatus that in many cases the information is still filtered, leaked and lost, since physical security through the electronic mechanism are not enough appears in the standard ISO / IEC 27002 standards for information security (Technology of information - Security techniques - Information security management systems - Requirement) the current version 27002: 2013, the same which becomes a tool is very important for organizations to be of any scale, because it provides recommendations to establish best practices in the management of information security, all thanks to the characterization of the principles of administration and the Deming Cycle PDCA - acronym for Plan, Do, Verify, Act (Plan, Do, Check, Act), this document seeks to clarify how the standard can maintain confidentiality, integrity and availability of information are essential to maintain the levels of competitiveness, profitability, legal compliance and institutional image.

Computer audit, ISO 27002, ISO / IEC, information

Citación: RAMOS, Johanna, FACUY, Jussen, PERALTA, Fabiola y ALEJANDRO, María. "Fuga de información" una práctica que se remedia con la Auditoría ISO/IEC 27002. Revista Administracion y Finanzas. 2017, 4-13: 53-66.

*Correspondencia del Autor: (correo electrónico: jramos@uagraria.edu.ec)
† Researcher contributing first author.

Introducción

El departamento de sistemas del Gobierno Autónomo Descentralizado del Cantón La Troncal viene prestando sus servicios desde hace más de 20 años, desde que se denominaba Municipio de la Troncal, fue un departamento que empezó con pocos colaboradores y con el pasar del tiempo fue incrementando su personal de trabajo.

Este departamento ha tenido varios cambios desde sus inicios, y esto se ha dado con motivo del avance tecnológico que se ha tenido a nivel informático, anteriormente la información no se encontraba en redes, luego de varios cambios se instaló la primera red de trabajo a inicios del año dos mil.

Una vez que se automatizó el Municipio lo primero que se realizó es ingresar el historial de toda la información relacionada a los predios de los habitantes del cantón La Troncal, luego se fueron incluyendo datos catastrales, obras, permisos municipales entre otros servicios que entrega el municipio a la sociedad Troncaleña.

Con el pasar del tiempo y a medida que la información fue incrementando en el GAD, se tomaron medidas para organizar de mejor manera la información, pero no se lo ha realizado de manera documentada, es decir no ha existido una política de establecer manuales y procedimientos lo que ha generado que en diversas ocasiones existan errores en la forma como se manejas y como se guarda la información dentro del departamento.

Después de haber realizado un estudio detallado de la situación actual del departamento de sistemas del Gobierno Autónomo Descentralizado del Cantón La Troncal se pudieron evidenciar algunos aspectos considerados como erróneos en el cuidado de la información que posee la institución.

El departamento carece de algunas políticas y procedimientos para llevar el cuidado de los datos, y en ocasiones existen estos documentos pero no se los ha socializado con los involucrados, lo que genera desconocimiento y por ende el error en el cuidado tanto físico como digital de la información.

Auditoria de la seguridad informática basado en la ISO 27001

Dentro de la base teórica que da inicio al trabajo de investigación. Se describe los aspectos primordiales de la seguridad de la información, así como las plataformas y herramientas de aplicación de la norma NPT-ISO/IEC 17799:2007, y la metodología OSSTMM, para aplicarlos en la elaboración de este proyecto.

ISO

De acuerdo a la Organización Internacional de Normalización (ISO), es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 157 países, uno por cada país. (Calderón, 2011).

La ISO es una organización no gubernamental, establecida en 1947 cuya misión es promover el desarrollo de la estandarización y las actividades relacionadas, con el fin de facilitar el intercambio de servicios y bienes y promover la cooperación en la esfera del Tl intelectual, científico, tecnológico y económico. Todos los trabajos realizados por la ISO resultan en acuerdos internacionales, los cuales son publicados como Estándares Internacionales.

ISSN 2410-342X

Estándar ISO

Un estándar es una publicación que recoge el trabajo en común de los comités de fabricantes, usuario, organizaciones, departamentos de gobierno y consumidores y que contiene las especificaciones técnicas y mejores prácticas en la experiencia profesional, con el objetivo de ser utilizada como regulación, guía o definición para las necesidades demandadas por la sociedad y tecnología. (Peña, 2015).

Los estándares ayudan a aumentar la fiabilidad y efectividad de materiales, productos, procesos o servicios que utilizan todas las partes interesadas (productores, vendedores, compradores, usuarios y reguladores). En principio, son de uso voluntario, aunque la legislación y las reglamentaciones nacionales pueden hacer referencia a ellos.

ISO 27001

Desde 1901 y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como: BS 5750 publicada en 1979, origen de ISO 9001; BS 7750 publicada en 1992, origen de ISO 14001.

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información. (Viveros, 2013).

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En el 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas.

ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

Esta norma, está constituida por 8 cláusulas y Anexos, de los cuales la parte principal del sistema son desde la cláusula 4 a la 8 y el Anexo A. Las cláusulas indican los procedimientos que deben ser implementados, los documentos que deben ser elaborados y los registros que deben ser mantenidos dentro de la organización. El anexo A indica los controles y objetivos de control a implementar con el fin de ser salvaguardas, los mismos que se encuentran distribuidos en dominios que son:

Política de seguridad

Organización de la seguridad de la información,

- Gestión de activos,
- Seguridad de los recursos humanos,
- Seguridad física y ambiental,
- Gestión de las comunicaciones y operaciones,
- Control de acceso,
- Adquisición, desarrollo y mantenimiento de los sistemas de información,

ISSN 2410-342X

- Gestión de incidentes en seguridad de la información,
- Gestión de la continuidad del negocio y
- Cumplimiento.

Por lo tanto, ISO 27001, es un estándar que proporciona un modelo para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en un ciclo de vida PDCA (del inglés Plan-Do-Check-Act, cuyo significado en español es Planear, Hacer, Verificar y Actuar; o ciclo de Deming) de mejora continua, al igual que otros sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.). (Krajewski, Ritzman, & Malhortra, 2012).

Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

Seguridad de la información

Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. (Seguridad, 2014).

La seguridad en todas sus ramas es un componente que no debe faltar porque da la garantía de protección, tranquilidad, defensa, control, paz, estabilidad y confianza, si a falta de la misma nos encontramos en un campo muy abierto de vulnerabilidades teniendo una sociedad en riesgo, (Moran, 2016).

Entendiéndose por confidencialidad a la propiedad que impide la divulgación de información a personas o sistemas no autorizados, es decir asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización; así mismo, cuando nos referimos a integridad, es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, es decir trata de mantener la información tal cual fue generada y al hablar de disponibilidad, nos referimos a la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

El aumento de la interconectividad informática y la popularidad del Internet están ofreciendo a las organizaciones todo tipo de oportunidades sin precedentes para mejorar las operaciones, reduciendo significativamente el uso del papel, a su vez reduciendo los costos al compartir información. Sin embargo, el éxito de muchos de estos esfuerzos depende, en gran parte, de la capacidad de la organización para proteger la integridad, confidencialidad y disponibilidad de los datos y de los sistemas informáticos. (Clarke, 2014).

Aunque la seguridad de la información juega un papel importante en la protección de los datos y de los activos de una organización, a menudo oímos noticias sobre delitos informáticos, como la alteración de sitios web o robo de datos. Las organizaciones tienen que ser plenamente conscientes de la necesidad de dedicar más recursos a la protección de los activos de información y seguridad de la información, la seguridad de la información debe convertirse en una de las principales preocupaciones de una empresa.

ISSN 2410-342X

La seguridad de la información ha sido un área de investigación durante mucho tiempo. Inicialmente los virus y los gusanos se propagaban lentamente a través del intercambio de contenedores magnéticos como los disquetes. Con el desarrollo del internet, los problemas de seguridad se han hecho más frecuentes y han tomado formas muy diferentes, dando lugar al desarrollo de las técnicas nuevas de seguridad. (Rivera & Villardefrancos Álvarez, 2012).

Los principios básicos clásicos de la seguridad de la información, que son, la confidencialidad, integridad y disponibilidad, constituyen la base para su protección de la TI. Los términos tecnología de información y comunicaciones, y tecnología de información y telecomunicaciones se utilizan con frecuencia como sinónimos. Debido a la longitud de estas expresiones, se han establecido abreviaturas y por lo tanto la gente en general, simplemente se refiere a ella como TI.

Debido a los avances de la tecnología, y su naturaleza de las comunicaciones, cada vez es más difícil asegurar la información de tal manera que su integridad está garantizada. En el entorno actual de las TI, las organizaciones son cada vez más dependientes de sus sistemas de información. La información es un activo que, como otros activos comerciales es muy importante y esencial para el negocio, por lo tanto necesita ser protegido adecuadamente. Esto es especialmente importante en el entorno empresarial, donde la información está expuesta a un número cada vez mayor de personas y por tanto a una variedad más amplia de amenazas y vulnerabilidades. Las amenazas, tales como código malicioso, la piratería informática, y ataques de denegación de servicio han vuelto más comunes, y cada vez son más sofisticadas. (Norma ISO 27001, 2005) La seguridad de la información a más de ser un problema de TI, también es un asunto de negocios.

Si una empresa quiere sobrevivir, y mucho más prosperar, es necesario comprender la importancia de la seguridad de la información y poner en práctica medidas y procesos apropiados.

Es vital estar preocupado por la seguridad de la información ya que gran parte del valor de una empresa se concentra en el valor de su información. La información es la base de la ventaja competitiva de las empresas. Tanto en el sector privado como en el sector público, se debería tener mayor conciencia de la probabilidad de robo de identidad y en sí de la información. Sin información, ni las empresas privadas ni públicas podrían funcionar. Por tanto valorar y proteger la información son tareas cruciales para las organizaciones modernas.

La razón básica acerca de los sistemas de seguridad, es que la información confidencial de una empresa debe ser protegida contra la divulgación no autorizada, por motivos ya sea confidencial o competitivo; toda la información que se almacena también debe ser protegida contra la modificación accidental o intencionada y a su vez debe estar disponible de manera oportuna. Además hay que establecer y mantener la autenticidad de los documentos que las organizaciones crean, envían o reciben. (Krajewski, Ritzman, & Malhortra, 2012).

Otro tema de la importancia de la seguridad informática, es el comercio electrónico que se puede ver como parte de la estrategia de desarrollo del mercado. Los consumidores han expresado su preocupación general por la privacidad y la seguridad de sus datos, las empresas con una fuerte seguridad pueden aprovechar su inversión para aumentar el número de compradores y a su vez aumentar su cuota de mercado.

ISSN 2410-342X

Ya no se tiene que mirar a la seguridad informática únicamente como para evitar la pérdida de la información, la seguridad informática hoy se convierte en una ventaja competitiva que puede contribuir de manera directa a las cifras de ingresos y así el progreso de una empresa.

Vunerabilidad

(Chamba Maleza, 2017) manifiesta que la vulnerabilidad hace referencia a una debilidad en un proceso informático permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones, también se considera vulnerabilidad a cualquier debilidad que se pueda presentar en la infraestructura tecnológica que lleve al mal funcionamiento de esta.

Metodología a desarrollar

Por tratarse de una investigación de campo se consideran las siguientes variables a tratar

Variable Independiente:

Gestión de Seguridad de la Información en el Departamento de Sistemas para el GAD Municipal La Troncal

Variable Dependiente:

Auditoria de la Seguridad Basado en la Norma ISO 27001 Tecnicas de Recolección de Datos

Teniendo en cuenta el talento humano que va a realizar el proyecto es la autoría de la investigación en conjunto quienes direccionaron el presente trabajo

Recursos humanos

Estudiante que propone el tema: Srta.: Martha Siguachi Fernández.

Director de trabajo de titulación: Ing. Jussen Facuy Delgado, Msc, otros investigadores considerando los autores de la presente investigación en conjunto con el Personal del GAD Municipal.

Recursos bibliográficos

- Libros.
- Artículos científicos.
- Revistas y tesis.

Recursos tecnológicos

Hardware

- Una computadora. Software
- Sistema Operativo Windows, Microsoft office.

Materiales

Norma Iso / IEC

Para recabar la información necesaria que permitió realizar el estudio de la situación actual del departamento de sistemas del Gobierno Autónomo Descentralizado del Cantón La Troncal se procedió a realizar una encuesta a todos los involucrados.

Como la población fue considerada pequeña se encuestó a las 20 personas que forman parte del proceso, en total los 12 integrantes que forman parte del área informática y 8 personas involucradas directamente con el departamento.

Limite espacial

El área en el cual se desarrolló el presente trabajo de investigación se relaciona con la auditoria informática, pertenece al entorno local, ya que se encuentra posicionada dentro del Cantón La Troncal.

ISSN 2410-342X

Límite Temporal

El tiempo establecido por medio del cual se desarrolló el presente estudio fue de 94 días que se resumen en un total de 3 meses y 4 días.

Resultados

Se procedió a tabular los resultados que se obtuvieron en las encuestas en base a un cuestionario de 42 preguntas, las mismas que se dividieron en siete áreas que se detallan a continuación:

- Seguridad de la información
- Organización para la seguridad de la información en el departamento
- Activos del área de sistemas
- Seguridad para recursos humanos
- Seguridad Física
- Comunicación y Operaciones
- Control de Acceso

Como la población se consideró pequeña, se procedió a encuestar a las 20 personas involucradas directamente el proceso, los resultados que se obtuvieron se detallan a continuación.

Seguridad de la información

Existe preocupación dentro del departamento de Sistemas por la elaboración de un documento sobre políticas de seguridad para controlar los riesgos que tiene la información.

Ítems	*OPCIÓN*	*No.*	*%*
1	SIEMPRE	8	40%
2	CASI SIEMPRE	6	30%
3	A VECES	4	20%
4	CASI NUNCA	2	10%
5	NUNCA	0	0%
	TOTAL	20	100%

Tabla 1 Políticas de Seguridad

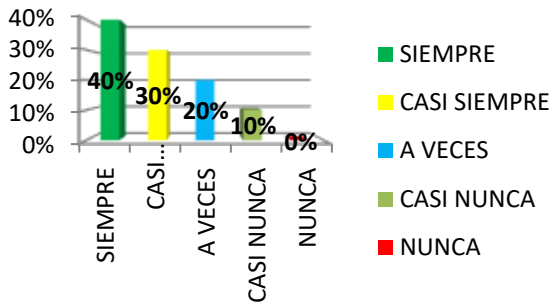

Figura 2 Políticas de Seguridad

Fuente: Técnicas de Investigación

La pregunta número uno consulta a los encuestados acerca de la preocupación del departamento de sistemas acerca de un documento sobre políticas de seguridad, la respuesta entregó como resultado que el 40% expresó que siempre existe la preocupación y otro 30% que casi siempre, lo que evidencia que existe una inquietud acerca de la seguridad de los datos dentro del departamento de sistemas, es evidente que siempre la información corre riesgos que deben ser controlados debido a que lo más importante en la actualidad dentro de las instituciones son los registros que se tiene en la base de datos.

ISSN 2410-342X

Es importante siempre contar con un documento que detalle las políticas de seguridad para el control de la información, además este documento debe ser siempre revisado, ya que a medida que la tecnología avanza existen nuevos riesgos a controlar para la información. Y si no existe un documento para políticas de seguridad se debe crear.

1. Se toman acciones rápidas y correctivas cuando se considera que la información del departamento está en riesgo.

ÍTEMS	*OPCIÓN*	*No.*	*%*
1	SIEMPRE	0	0%
2	CASI SIEMPRE	4	20%
3	A VECES	12	60%
4	CASI NUNCA	3	15%
5	NUNCA	1	5%
	TOTAL	20	100%

Tabla 2 Riesgo de Información

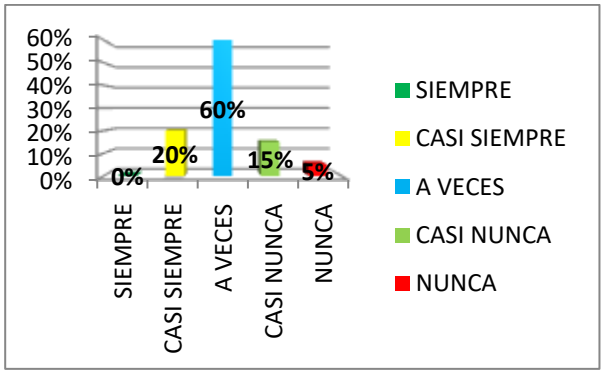

Figura 3 Riesgo de Información

Fuente: Técnicas de Investigación

En esta pregunta se consultó a los encuestados si en la institución se toman acciones rápidas y correctivas cuando la información está en riesgo, el 20% expresó que casi siempre, se considera un porcentaje muy bajo, mientras que el 60% respondió que a veces, este porcentaje es demasiado alto si se toma en consideración que al detectar que la información se encuentra en riesgo se debería tomar acciones inmediatas para tratar de lograr que los datos se pongan a buen recaudo.

No se puede poner en riesgo la información de la institución, ya que está en juego lo más valioso que se tiene en la actualidad. Por lo cual si se detectan falencias en estos casos se debería tomar las acciones correctivas.

Se revisan con frecuencia las medidas y procedimientos para la seguridad de la información.

Ítems	*Opción*	*No.*	*%*
1	Siempre	1	5%
2	Casi siempre	3	15%
3	A veces	13	65%
4	Casi nunca	2	10%
5	Nunca	1	5%
	Total	20	100%

Tabla 3 Seguridad de la Información

ISSN 2410-342X

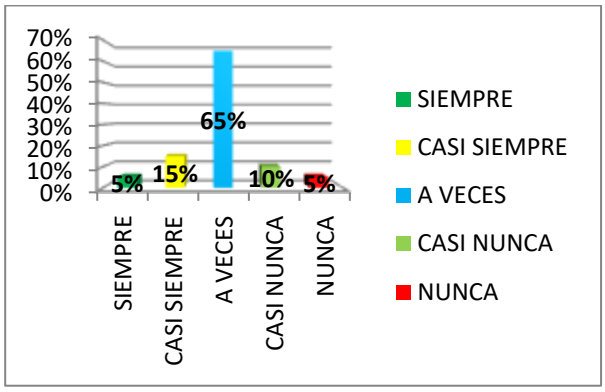

Figura 4 Seguridad de la Información

Fuente: Técnicas de Investigación

Es importante tener la información de una empresa o institución lo más segura posible, la pregunta anterior tiene relación acerca de la revisión periódica de las medidas y procedimiento para el control de la seguridad de la información dentro del departamento, para lo cual los encuestados expresaron en un 5% que siempre se revisan, otro 15% que casi siempre se revisan mientras que la mayoría que representa el 65% expresaron que a veces se tiene revisión de la misma.

Esto evidencia que existe un poco de despreocupación en cuanto a los procedimientos que se deben de tener para que se controle la seguridad de la información, y es un punto a tratar con importancia por medio del departamento.

Organización para la seguridad de la información en el departamento

El departamento de sistemas se preocupa que las personas que laboran en él, tomen conciencia acerca de la importancia de la seguridad de la información y las responsabilidades de cada uno.

Ítems	*Opción*	*No.*	*%*
1	Siempre	1	5%
2	Casi siempre	3	15%
3	A veces	14	70%
4	Casi nunca	2	10%
5	Nunca	0	0%
	Total	20	100%

Tabla 4 Seguridad e importancia de la Información

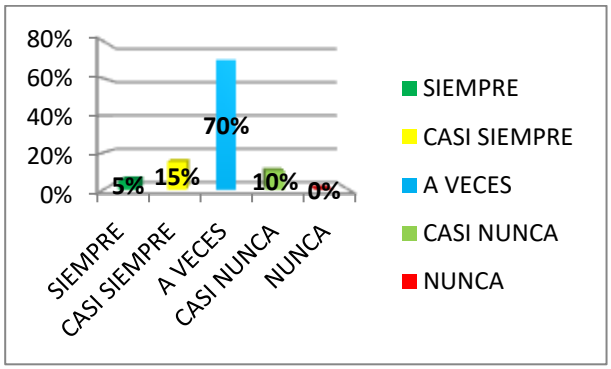

Figura 5 Seguridad e importancia de la Información

Fuente: Técnicas de Investigación

En esta pregunta se consultó a los involucrados si el departamento de sistemas se preocupa por que sus colaboradores tengan conciencia de la importancia de la seguridad de información que se tiene en el departamento y la responsabilidad con la que debe actuar cada uno, el 5% expresó que siempre, un porcentaje muy bajo, el 15% se manifestó que casi siempre y un 70% contestó que a veces.

Estos resultados evidencias que se debería tener una mayor preocupación por parte de los directivos de la institución para que quienes laboran en el departamento de sistemas tomen conciencia absoluta acerca de lo importante que manejan y las responsabilidades que deben asumir cada uno de ellos.

ISSN 2410-342X

Se tienen definidas todas las responsabilidades de cada integrante del departamento en base a la seguridad de la información.

Ítems	*Opción*	*No.*	*%*
1	Siempre	4	20%
2	Casi siempre	14	70%
3	A veces	2	10%
4	Casi nunca	0	0%
5	Nunca	0	0%
	Total	20	100%

Tabla 5 Responsabilidades

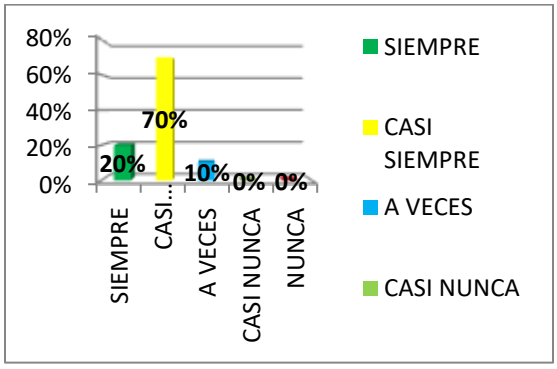

Figura 6 Responsabilidades

Fuente: Técnicas de Investigación

La pregunta anterior se refiere a la definición de responsabilidades que tiene cada trabajador en el departamento de sistemas en base a la seguridad de los datos, el 20% expresó que siempre y el 70% se manifestó que casi siempre, si sumamos los dos resultados se puede demostrar que están bien definidas las responsabilidades que se tiene en el departamento informático. Esto representa una gran ventaja para proteger la información, debido a que si cada integrante tiene bien definida su responsabilidad se tendrá conocimiento de cómo cuidar los datos en beneficio de la institución.

El departamento posee un acuerdo de confidencialidad o no divulgación de la información para los que integran el área.

ÍTEM	*OPCIÓN*	*No.*	*%*
1	SIEMPRE	0	0%
2	CASI SIEMPRE	1	5%
3	A VECES	4	20%
4	CASI NUNCA	14	70%
5	NUNCA	1	5%
	TOTAL	20	100%

Tabla 6 Confidencialidad de la Información

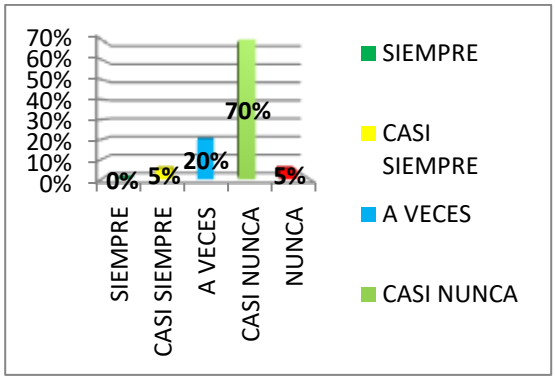

Figura 7 Confidencialidad de la Información

Fuente: Técnicas de Investigación

Es importante definir en general todas las responsabilidades dentro de un departamento de sistemas, no sólo es suficiente con detallar el trabajo que debe hacer cada integrante, además se necesita que cada uno conozca lo importante de la confidencialidad de los datos, esta pregunta se refiere a este aspecto, para lo cual los encuestados expresaron en un 5% que casi siempre el departamento posee un acuerdo de confidencialidad, 20% que a veces, y el 70% que representa la mayoría se manifestó que casi nunca.

ISSN 2410-342X

Esto evidencia que no existe un acuerdo de confidencialidad o no divulgación de la información, por lo tanto la información está en riesgo, ya que los integrantes del departamento deberían tener claro este acuerdo inmediatamente cuando asumen el cargo dentro del área.

Parámetros de Evaluación	**Opción de Respuesta**	**Puntos 1, 2 o 3)**	**Observación**
Número Total de Computadoras	1. Menos de 100 computadoras. 2. Entre 100 y 300 3. Más de 300	1	Ninguna
Número de Servidores	1. Menos de 5 2. Entre 5 y 10 3. Más de 10	1	Suficiente para el departamento y áreas involucradas
Número de Empleados en el Dep. de Sistemas	1. Menos de 10 2. Entre 10 y 20 3. Más de 20	2	Ninguna
Existencia y función del área de sistemas (Tecnología).	1. No hay dep. de Sistemas 2. Área de Sistemas enfocada en resolver problemas de puntos informáticos. 3. Punto anterior más área de sistemas que planea y desarrolla proyectos nuevos.	2	Ninguna
Redes	1. Solo Intranet 2. Solo Internet 3. Intranet e Internet	3	Ninguna
Desarrollo de Software	1. Compras Software 2. Desarrollan Software para uso local. 3. Compran y Desarrollan Software.	1	No existen desarrolladores de software

Tabla 7 valoración de aspectos del departamento de sistemas

Clausula	**Objetivo de Control**	**Control**	**Observación Directa**
Seguridad de la Información	Política de Seguridad de la Información en el departamento	Documento de políticas de seguridad de la información institucional	No existe un documento de política de seguridad para la información de la Institución.
Organización para la seguridad de la información en el departamento	Organización de la información	Documento que maneje los flujogramas de la formas como estás organizada la información	No existe documento con flujos y procedimientos de la seguridad de la información.
Activos del área de sistemas	Inventario de equipos y dispositivos	Documento que evidencie un inventario periódico de los equipos con los que cuenta la institución	Existe documento de inventario, pero no se realiza de manera periódica en determinados ciclos.
Seguridad para recursos humanos	Control de usuarios del departamento de sistemas	Documento que contiene las responsabilidades y sanciones del uso en el manejo de la información por parte del personal	Existe documento con responsabilidades y sanciones, pero no se ha socializado.
Seguridad Física	Control de los equipos e información de la institución	Documento con directrices para el cuidado de los equipos.	No existe manual de procedimientos para el cuidado de equipos ni el cuidado de la información.
Comunicación y operaciones	Control de la información que se tiene por medio de internet e intranet.	Manual de procedimientos con reglas para el cuidado de la información	No existe documento que controle el manejo de información importante, divulgación al exterior o salida de datos por medio de dispositivos.
Control de acceso	Controlar la información con permisos de usuarios.	Documento que controle los permisos de usuarios y acceso que se da a la información.	Existe documento de accesos a información de usuarios, pero no está actualizado.

Tabla 8 observación directa

Agradecimiento

Un Agradecimiento especial a la Ing. Martha Siguachi, Gobierno decentralizado de la Troncal y demás investigadores inmersos en el presente trabajo.

Conclusiones

• No existe un documento de políticas de seguridad de la información, el mismo que se considera muy importante para llevar el control de los datos.

• Los activos del área de sistema y los departamentos involucrados son muy importante, por lo cual se debería de realizar un inventario periódico de los equipos, dispositivos y los programas que se manejan.

• Se pudo evidenciar que existe un documento donde se detallan las funciones, responsabilidades y sanciones en caso de incurrir en una falta dentro del departamento, pero este documento no tiene una firma ni sello de aprobación, además nunca se ha socializado, por lo tal muchos de los usuarios desconocen de estas políticas.

• Se verificó que no existe un documento que detalle políticas de seguridad física de los equipos, dispositivos e información de la institución.

• Se lleva un control a medias de la administración de la red.

• El control de acceso para los usuarios se maneja de manera desordenada, hay un documento con procedimientos pero este no ha sido aprobado por alguna directiva y además no está actualizado.

• No se encuentran definidos los requisitos para la confidencialidad de la información.

• No existen procedimientos para permitir el ingreso sólo al personal autorizado al área de sistemas, además no existe un control de ingreso en un horario determinado para los que laboran en el departamento.

Referencias

Aguilera, L., & Gonzalez, M. (Abril de 2015). LA INFLUENCIA DE LA INNOVACIÓN Y LA INFORMACIÓN FINANCIERA EN LA COMPETITIVIDAD DE LA PEQUEÑA Y MEDIANA EMPRESA MANUFACTURERA. REVISTA INTERNACIONAL ADMINISTRACION & FINANZAS, 119.

Andrés , A., Fernandez, C., & Delgado , B. (2016). Guía práctica de ISO/IEC 20000-1 para servicios TIC. AENOR Ediciones, 176.

ASAMBLEA NACIONAL DEL ECUADOR. (2008). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. Quito, Ecuador.

Bosh, L. (2014). Evaluacion fonologica del habla infantil . Barcelona, España: Manson.

Calderón, J. L. (14 de Diciembre de 2011). ¿De que hablamos ahora? Obtenido de https://ydequehablamosahora.wordpress.com/2011/12/14/trabajo-publicado-de-que-hablamos-ahora-jorge-lopez-calderon/

Chamba Maleza, J. T. (2017). Plan informático 2016-20209 basado en la norma ISO/IEC 27001:2013 para mejorar la seguridad de información, infraestructura tecnológica y procesos informáticos en la Cooperativa de Ahorro y Credito Camara de Comercio de la ciudad de Santo Domingo, 334.

China, N. (2014). La sonoridad y la marcacion en los errores comunes del habla infantil. Revista Argentina de Neuropsicol, 23-37.

Clarke, M. &. (2014). Informe de vigilacia tecnologica. Madrid.

Cuní, D. (30 de Abril de 2012). Como Usar Microsoft Visio. Obtenido de http://empresayeconomia.republica.com/newsletter/como-utilizar-el-programa-microsoft-visio.html

D`Introno, F., & Martinez, V. (2015). Procesos de metatesis en el desarrollo fonologico de niños de 3 a11 años. Madrid: Editorial Catedra.

Enjuto, J. (2012). ISO 20000, camino a la excelencia. Nextel, 3-4.

Fernandez, A. (2013). Sistemas Integrados de Gestión. Sistemas Integrados de Gestión. Asturias, España.

Fernández, J. (S/F). PROACTIVANET. Recuperado el 22 de SEPTIEMBRE de 2016, de PROACTIVANET: https://www.proactivanet.com/blog/proactivanet/la-familia-de-normas-iso-20000/

Forget, T. (2014). Fundamentos de Marketing con unas perspectivas generales. Mexico DF: Pearson Education.

Hurtado, Y. (16 de Septiembre de 2016). ¿QUÉ ES BPMN Y PARA QUÉ SIRVE? Obtenido de http://nextech.pe/que-es-bpmn-y-para-que-sirve/

Jimenez, J., & Rodriguez, J. (2015). Internt y sus aplicacion en el contexto global. Mexico DF: Pearson Education.

Krajewski, L., Ritzman, L., & Malhortra, M. (2012). Administracion de Operaciones (8 ed.). Mexico D.F: Pearson Prentice Hall.

Morán Pedro. (2016). Plan de Seguridad Informática en base a parámetros de la norma ISO/IEC 27002 para mejorar la Seguridad de la Información en el Departamento de Tecnologías de Información y Comunicación del Gobierno Autónomo Descentralizado Provincial De Santo Domingo de l, 96. Retrieved from http://dspace.uniandes.edu.ec/handle/123456789/4222

NACIONES UNIDAS. (2012). Gobernanza de la tecnología de la información y de las comunicaciones en las organizaciones del sistema de las Naciones Unidas. Roma.

Papo. (16 de Mayo de 2015). 10 Ventajas de usar Microsoft Excel. Obtenido de http://top10mejores.com/ventajas-de-usar-microsoft-excel/

Peña, F. (19 de Marzo de 2015). ISOTools Excelence. Obtenido de https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

Phill, C. (2012). Marketing con una vision global en las organizaciones. Mexico DF: Mc Graw Hill.

Presidencia De La República. (1998). Ley De Propiedad Intelectual. Quito, Ecuador.

QAEC. (2016). Norma UNE ISO/IEC 20000. Recuperado el 10 de Septiembre de 2016, de Norma UNE ISO/IEC 20000: http://www.aec.es/web/guest/centro-conocimiento/norma-iso-20000

Rivera, Z., & Villardefrancos Álvarez, M. d. (2012). La auditoria como proceso de control: concepto y tipología. redalyc, 68-69.

ISSN 2410-342X

Saavedra, M., & Tapia, B. (Abril de 2013). El uso de las tecnologías de información y comunicación TIC en las micro, pequeñas y medianas empresas. El uso de las tecnologías de información y comunicación TIC en las micro, pequeñas y medianas empresas. Venezuela.

Seguridad, S. C. (2014). Seguridad de la Informacion. GUATEALA: Consejo Editorial.

Serra, M. (2014). Normas estadisticas de articulacion para la problacion escolar de 3 a 7 años del area metropolitana de Barcelona. Revista Logoped Fonitr Audiol, 232-250.

SIGA. (2015). Manual del Sistema Integrado de Gestión. Colombia.

Storti, P. (2012). Estudio descriptivo sobre los procesos fonologicos de simplificacion en niños de 2 años a 5 años . Buenos Aires: Universidad Nacional del Rosario.

Universidad san nicolas de hidalgo. (2015). Sistema de gestion de calidad. Sistema de gestion de calidad. Michoacana, mexico.

Vázquez, L. (9 de Enero de 2012). Características y usos de Microsoft Project. Obtenido de http://empresayeconomia.republica.com/aplicaciones-para-empresas/caracteristicas-y-usos-de-microsoft-project.html

Viveros, N. L. (2013). Gerencia de compras: La nueva estrategia competitiva (Segunda ed.). Colombia: ECOE EDICIONES.

ISSN 2410-342X