CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

DOI 10.35381/cm.v8i4.898

La seguridad informática para la toma de decisiones en el distrito de educación 12d03. Mocache-Ecuador

Information security for decision making in education district 12d03. Mocache-Ecuador

Nadia Carminia Coloma-Baños
pg.nadiaccb93@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0002-9916-4130

Fredy Pablo Cañizares-Galarza
da.fredypcg62@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0003-4854-6996

Ariel José Romero-Fernández
ua.arielromero@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0002-1464-2587

Marco Vinicio Quintana-Cifuentes
pg.docentemvqc@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0003-3068-1540

Recibido: 01 de mayo 2022
Revisado: 25 de junio 2022
Aprobado: 01 de agosto 2022
Publicado: 15 de agosto 2022

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

RESUMEN

El objetivo de la presente investigación es diseñar un plan de seguridad informática para la toma de decisiones en el distrito de educación 12D03 Mocache-Quevedo basado en las directrices de la Norma ISO/IEC 27001 con el afán de asignar mejores prácticas en la gestión de la seguridad de la información. La implementación del Plan de seguridad informática contribuyó permitiendo elevar en un grado muy significativo la seguridad en los 11 dominios de la norma ISO 27002, para lo cual es esencial que el equipo de trabajo y la alta gerencia se comprometa con la implementación de las políticas, ya que son el cimiento para obtener un avance significativo en la integridad, confidencialidad y disponibilidad de la información y los servicios otorgados a la comunidad distrital y estén con el continuo cambio si las normativas de la entidad lo requieren.

Descriptores: Datos abiertos; acceso a la información; protección de datos. (Tesauro UNESCO).

ABSTRACT

The objective of this research is to design an information security plan for decision making in the education district 12D03 Mocache-Quevedo based on the guidelines of ISO/IEC 27001 with the aim of assigning best practices in information security management. The implementation of the Information Security Plan helped to significantly increase security in the 11 domains of ISO 27002, for which it is essential that the work team and senior management commit to the implementation of the policies, as they are the foundation for significant progress in the integrity, confidentiality and availability of information and services provided to the district community and are with the continuous change if the entity's regulations require it.

Descriptors: Open data; access to information; data protection. (UNESCO Thesaurus).

INTRODUCCIÓN

La información, como un elemento más al interior de una organización, se considera un activo valioso, ya que de ahí se toman decisiones importantes para el desarrollo de los objetivos corporativos y, a su vez, se le brindan al usuario elementos de juicio para su permanencia como cliente; de ahí, la necesidad de ser protegida. (Candelario-Samper & Rodríguez-Bolaño, 2014)**.**

La seguridad informática actualmente forma parte de los grandes negocios en materia de tecnología y seguridad en las empresas. Debido a que hoy en día se reflejan distintos tipos de ataques y amenazas al acceso de la información de las organizaciones, es necesario crear medidas y procesos que contrarresten estos peligros que afectan los recursos funcionales de las entidades. Por eso, se requiere la disposición de diferentes mecanismos de seguridad que van relacionados con varios tipos de recursos tanto humanos como tecnológicos que ayudan a garantizar una muy buena seguridad en las empresas. La seguridad de la información es un tema de nunca acabar y que por tal motivo la actualización de los distintos recursos y procesos que se identifiquen día a día es sumamente importante para minimizar los riesgos en el ámbito de seguridad de las organizaciones (Suárez & Ávila, 2017)

Según (Acissi, 2015), la seguridad Informática en los sistemas de información, representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y de recursos (físicos, lógicos y humanos) que permiten almacenar y que circule la información que contiene. También representa la red de actores que intervienen sobre él, que intervienen datos, acceden a ellos y los usan.

Así como la tecnología ha ido evolucionando, los fraudes y delitos informáticos han ido a la par, a tal punto que en la actualidad un delincuente informático puede sustraer recursos económicos de una organización desde la comodidad de su hogar, sin dejar rastro alguno, o estructurar grandes delitos desde el interior de la organización; esta situación sumados a los grandes desfalcos financieros ocurridos a nivel mundial,

incluyendo delitos informáticos, han obligado al auditor un cambio de enfoque y la necesidad de que el auditor cuente con nuevas habilidades y conocimientos, sobre todo el área de tecnología (Espinoza-Zallas & Rodríguez-Pérez, 2017).

La seguridad de la información tiene por objeto proteger a los sistemas informáticos de las amenazas a los que están expuestos. Debido a lo anterior, la aplicación de medidas de seguridad debe realizarse de manera planificada y racional, para evitar dirigir esfuerzos e invertir recursos en áreas que no lo requieren. Para que las medidas y mecanismos de protección resulten eficaces, deben integrarse dentro de un sistema más amplio de gestión de la seguridad de la información (Gil-Vera & Gil-Vera, 2017).

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta (Urbina, 2016), se basa, por lo tanto, en proteger la información y resguardarse de los riesgos potenciales, eso se logra aplicando un proceso de gestión de seguridad para todos los entornos de software y hardware presentes en la empresa y poder disfrutar de las últimas mejoras en materia de seguridad (Jean, 2016)**.**

Según (Carpentier, 2016), la gestión de la seguridad de la información, su objetivo consiste en alinear la seguridad de la información con la actividad de negocio y de asegurar que esa seguridad se gestiona eficazmente en todos los departamentos y sus actividades de gestión. La auditoría informática es aquella que tiene como objetivos evaluar los controles de la función informática, analizar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente (Guerrero-Fernández, 2015).

El objetivo de la presente investigación es diseñar un plan de seguridad informática para la toma de decisiones en el distrito de educación 12D03 Mocache-Quevedo basado en las directrices de la Norma ISO/IEC 27001 con el afán de asignar mejores prácticas en la gestión de la seguridad de la información.

PROPUESTA DE TRABAJO

Los funcionarios de la entidad no tienen conocimiento de la existencia de un manual de políticas de seguridad o de un plan de seguridad de informática por parte del departamento distrital de las Tecnologías de la Información, para lo cual sugieren que deben poner en práctica las normativas de este documento o elaborar uno si no existiere para guiar en los inconvenientes presentados a los servidores públicos con la integridad, confidencialidad y la disponibilidad de la información de los servicios informáticos.

Falta de procedimientos en caso de ocurrir problemas con sus equipos de cómputo, en cuanto a respaldos de la información y la regularidad que deberían realizarse para salvaguardar la información de los diferentes departamentos de la entidad.

Se encontró la novedad que los funcionarios entregan sus credenciales de acceso a sus plataformas institucionales de los servicios utilizados a otros funcionarios por diversos motivos, además no existen ningún procedimiento que haga referencia a su uso, modificación y un 60% de ellos lo realizan por iniciativa propia.

No existe ninguna medida de seguridad en cuanto al control de la conexión de las unidades extraíbles de sus equipos de cómputo, acceso a las carpetas compartidas por departamento.

Después de realizar un diagnóstico de los resultados obtenidos de la investigación se propone el desarrollo de un plan de seguridad informática para la toma de decisiones en el Distrito de Educación 12D03 Mocache-Quevedo que contribuya al mejoramiento de la gestión de la integridad, confidencialidad y alta disponibilidad en referencia al Acuerdo Ministerial No. 166, publicado en el Registro Oficial No. 88 del 25 de septiembre de 2013 de la Secretaría Nacional de la Administración Pública en el Artículo 1 menciona “Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las normas Técnicas ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de la Seguridad de la Información, el cual ha desarrollado un esquema gubernamental de Seguridad de la Información(EGSI), en el cual se establece 126 hitos o controles, basadas en la

norma técnica ecuatoriana INEN ISO/IEC 27002 “Código de Práctica para la Gestión de la Seguridad de la Información”.

Se recomienda que previo a la implementación del EGSI se proceda a dar cumplimiento al Art. 7 del Acuerdo 166: “Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 “Gestión del Riesgo en la Seguridad de la Información”; considerando que los activos críticos institucionales identificados en el estudio de gestión de Riesgos, permitirán determinar los controles necesarios a ser implementados. El aporte de este trabajo de investigación está considerado en los siguientes puntos de la propuesta:

Se propone el desarrollo de un plan de seguridad informática para mejorar la gestión de la confidencialidad, integridad y disponibilidad de la información para la toma de decisiones en el distrito de Educación 12D03 Mocache-Quevedo, se utilizará la metodología PDCA (Planificar, Hacer, Verificar y Actuar), ya que este permitió diseñar un plan que se ajuste a las necesidades de la entidad , que contemple las directrices para proteger la información con el uso de las normativas ISO/IEC 27000.

ISO/IEC 27001 adopta el modelo PDCA(o de Demming),”PDCA son las siglas de Plan-Do-Check-Act” y el modelo se aplica para estructurar todos los procesos del SGSI, así como en muchos otros entornos y marcos generales de buenas prácticas como ITIL (Castro Gil , Díaz Orueta, Alzórriz Armendariz , & San Cristóbal Ruiz, 2014)

Las actividades principales Tabla2, asociadas al modelo PDCA aplicadas a SGSI son:

Tabla 1.
Modelo PDCA aplicadas a SGSI.

Planificar (Establecer el SGSI)	Establecer: políticas, objetivos, procesos y procedimientos de seguridad destacados para gestionar el riesgo y mejorar la seguridad informática, con la finalidad de entregar resultados acordes con las políticas y objetivos de la organización.
Hacer (Implementar y operar el SGSI)	Implementación de los controles seleccionados y la correcta aplicación de los mismos (política, controles, procesos y procedimientos)
Verificar (Revisar y dar seguimiento al SGSI)	Medir el rendimiento de los procesos contra los controles del SGSI(la política, los objetivos de seguridad y la experiencia práctica) y reportar los resultados a la dirección, para su revisión.
Actuar (Mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI.

Elaboración: Los autores.

Es la parte más importante de la propuesta, ya que hacen uso de las normas ISO/IEC 27000, la cual es un conjunto de estándares desarrollados -o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. (ISO, 2012). Estas normas permiten a las organizaciones conocer los riesgos con el trato de seguridad hacia la información pudiendo minimizar los riesgos y gestionando de la mejor manera para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con los requisitos de calidad del cliente y con los objetivos previstos.

ISO hace mucho énfasis a la seguridad tanto que existen normas para las diferentes etapas de la gestión de la seguridad de la información. A continuación, se detalla las normas ISO más importantes sobre la gestión de la seguridad de la información de este proyecto:

ISO/IEC 27000: Es un vocabulario estándar para el SGSI; ISO/IEC 27001: Es la certificación para las organizaciones. Especifica los requisitos para la implantación del SGSI detallada en la Figura1. La más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos; ISO/IEC 27002: Es un código de buenas prácticas para la gestión de seguridad de la información; ISO/IEC 27003: Son directrices para la implementación de un SGSI; ISO/IEC 27004: Son métricas para la gestión de seguridad de la información; ISO/IEC 27005: Trata la gestión de riesgos en seguridad de la información. (ISO, 2012)

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año VIII. Vol. VIII. Nro. 4. Edición Especial 4. 2022
Hecho el depósito de ley: FA2021000002
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK). Santa Ana de Coro. Venezuela

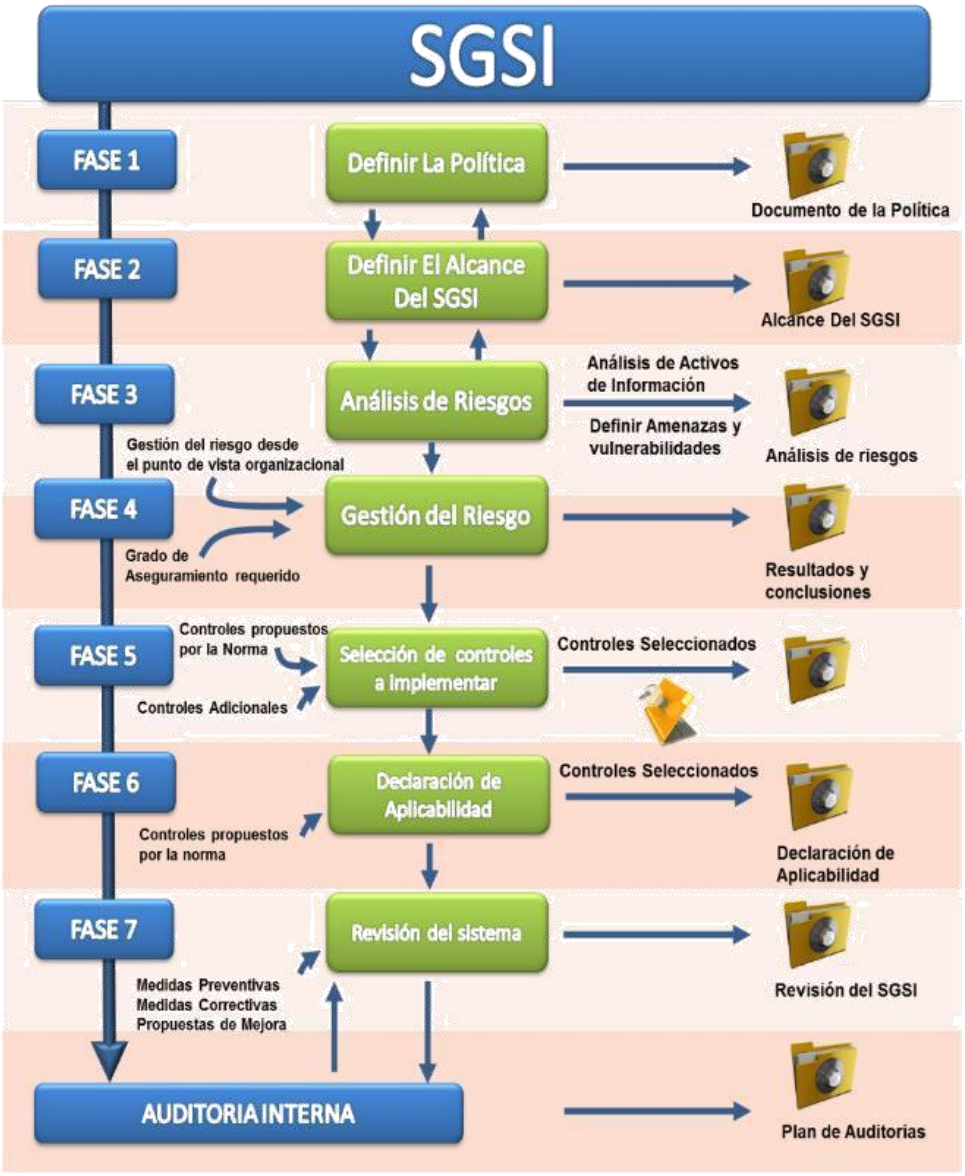

Figura 1. Sistema de Gestión de la Seguridad Informática.
Fuente: https://www.normas-iso.com/iso-27001/

Definir las Políticas

La seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de ordenadores a concentrarse en políticas, procedimientos y controles basados en las personas. Para dar ejecución a esta fase necesario realizar un estudio de las políticas de seguridad que actualmente se encuentran utilizando y enfocándonos en el departamento de tecnologías de la información para realizar esto se procedió a realizar las respectivas entrevistas y encuestas a la directora distrital, analistas y al personal del área de TIC.

Alcance del plan de seguridad informática

Plan de seguridad informática es el documento básico en el que se describe los principios organizativos de una entidad y recoge claramente las políticas, medidas y los procedimientos de seguridad de la información, es decir, los controles del SGSI para alcanzar los objetivos de la organización y las responsabilidades de cada uno de los participantes en el proceso informático.

El plan de seguridad informático debe garantizar:

La Disponibilidad, la trazabilidad y la recuperación de los sistemas de información

La Autenticidad, integridad, confidencialidad, el acceso y la conservación de la información.

El presente Plan de Seguridad Informática es aplicable en su totalidad en los departamentos del distrito de Educación que se encuentra ubicado en la Parroquia San Camilo, calle Honduras y Uruguay. Las políticas citadas en este plan son de obligatorio cumplimiento para todo el personal de la entidad, incluyendo las 157 instituciones educativas fiscales que se encuentran a su cargo.

Análisis de Riesgo.

La norma ISO/IEC 27005 proporciona una guía para realizar el análisis de riesgos de la seguridad de la información contiene diferentes recomendaciones y directrices en la cual específica los parámetros que se deben cumplir en las diferentes fases del proceso (identificación de los activos, identificación de requerimientos legales y comerciales, valoración de Activos, identificación de amenazas, vulnerabilidades y probabilidad de ocurrencia y análisis de riesgo y su evaluación).

Activo para lo cual se identifican los activos de la entidad detallados en la Tabla 2.

Tabla 2.
Identificación de los activos.

EQUIPOS	CANTIDAD
SWICH	9
FIBRA OPTICA	1
ROUTERS	4
ARMARIO RACKEABLE	1
ORGANIZADORES DE CABLE	1
CABLEADO ESTRUCTURADO	1
SERVIDOR	1
PORTATIL	30
EQUIPOS DE ESCRITORIO	38
INSTALACION ELECTRICA	1

CENTRAL DE AIRE	1
DISCOS DUROS EXTERNOS	4
DISCOS DUROS DE SERVIDORES	4
UPS	15
IMPRESORAS	20

Elaboración: Los autores.

El término Amenaza puede entenderse como algún hecho que puede producir algún daño provocado por algún evento natural o antrópico, es decir originado por alguna actividad humana. Viéndolo desde un entorno informático, se puede considerar como cualquier elemento que comprometa al sistema.

Las vulnerabilidades son los fallos del sistema de seguridad o en los propios en que el usuario utiliza para desarrollar las actividades que permitirían que una amenaza tuviese éxito a la hora de generar un problema. (Romero Castro, y otros, 2018)

De acuerdo con una de las clasificaciones, los tipos de vulnerabilidades que pueden presentarse a nivel informático son: Vulnerabilidad física, Vulnerabilidad natural, Vulnerabilidades del hardware, Vulnerabilidades del software, Vulnerabilidad de medios o dispositivos, Vulnerabilidad de las comunicaciones, Vulnerabilidad Humana.

Gestión de Riesgo

El proceso de gestión de riesgos identifica y prioriza los peligros inherentes al desarrollo de un producto, sistema u organización. La gestión del riesgo es una parte importante de la gestión de la seguridad y se define como el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de

establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado.

Selección de los Controles para implementar

Se realizó una auditoría informática, en la fase de su ejecución se seleccionó los controles a través de un checklist in-situ en compañía del analista distrital de tecnologías, además de la entrevista al personal de las diferentes áreas.

A continuación, se detalla en la tabla 3 la valoración de los dominios y la tabla 4 sobre el Cumplimiento por dominios de la norma ISO/IEC 27002.

Tabla 3
Valoración de controles ISO 27002.

Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual.
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.
			Se puede seguir la evolución de los

L4	95%	Gestionado y medible	procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia.
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.
L6	N/A	No aplica	

Fuente: Elaboración propia

Tabla 4.
Cumplimiento por dominios de la norma ISO/IEC 27002.

Dominios	% de Efectividad	Número Control Mayores	Número Control Menores	Control OK
5.- Política de Seguridad	0%	2	0	**0**
6.- Aspectos Organizativos de la SI	31%	7	4	**0**
7.- Gestión de activos	23%	4	0	**1**
8.- Seguridad ligada a Recursos Humanos	89%	0	3	**4**
9.- Seguridad física y del entorno	68%	3	5	**4**

10.- Comunicación y Operaciones	65%	8	9	**13**
11.- Control de Acceso	31%	20	2	**3**
12.-Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	50%	7	4	**3**
13.- Gestión de Incidentes de Seguridad de la Información	92%	0	5	**0**
14.- Continuidad Del negocio	10%	5	0	**0**
15.- Cumplimiento	20%	6	4	0

Elaboración: Los autores.

Preparación de la declaración de aplicabilidad

La declaración de aplicabilidad es el documento central que define cómo implementará una gran parte de la seguridad de su información debe incluir los objetivos de control y controles que serán aplicados y los que serán excluidos. Es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación del sistema de seguridad de la información. El objetivo de este documento es definir cuáles de los 133 controles (medidas de seguridad) sugeridos en la norma ISO 27001 que se implementará y, para los controles que correspondan, cómo se realizará su implementación.

Revisión del Sistema

El control interno está orientado a cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información, y la adopción de medidas oportunas para corregir las deficiencias de control.

Síntesis de la propuesta

Los resultados obtenidos en la evaluación del análisis de Seguridad de la Información y Seguridad Informática, aportarán en la implementación de buenas prácticas que mermarán las vulnerabilidades y amenazas que han sido halladas.

Dentro de los resultados generales más importantes de la aplicación de la metodología de análisis y evaluación de amenazas, vulnerabilidades, riesgos, y los instrumentos diseñados están: Algunos de los problemas de seguridad en las organización evaluada están relacionada esencialmente con: el desconocimiento sobre aplicación y uso de las normas de seguridad de la información y las limitaciones en la administración de seguridad informática y de la información que comprometen seriamente la imagen Institucional.

Las probables causas que originan las falencias encontradas son: poco conocimiento en el tema de seguridad de información, la falta de organización en el área de TICS , no existencia o falta de cumplimiento de controles (políticas, procedimientos y procesos)para la seguridad de la información, no se ha establecido criterio sobre esta revisión ya que cuando sucede un requerimiento relacionado con la seguridad es informado al analista distrital de tecnologías para recién realizar las modificaciones del evento, existe responsabilidades no cumplidas al 100% sobre la seguridad de la información, la información debería ser clasificada según su valor, en general el limitado personal imperante administrativo para proteger los activos informáticos y de información frente a las amenazas y riesgos a que se ven enfrentadas**.**

Los resultados del diagnóstico se basaron en un análisis de los dominios aplicados en la norma ISO/IEC 27001 en porcentaje (%) de cumplimiento al aplicar el check

diseñado. Los porcentajes resultantes en los dominios están asociados a la escala de madurez e interpretados de acuerdo con el porcentaje de cumplimiento. El resultado muestra que es imperativo el apoyo y compromiso real de la alta gerencia o administración para el proceso de diseño, implementación e implantación de un SGSI de acuerdo a los resultados de la auditoria; además se deben concretar los controles(procesos y procedimientos) que así lo requieran y documentarlos, por lo cual se deben definir los procesos y procedimientos faltantes; también se deben establecer mecanismos de control de seguridad informática que permitan la medición permanente orientadas hacia la mejora de la seguridad de la información y al diseño, implementación e implantación de un SGSI en cada una de las organizaciones de acuerdo a sus necesidades.

CONCLUSIONES

En la actualidad existen varios sucesos de ataques a empresa; los riesgos y vulnerabilidades de seguridad de la información representan una amenaza considerable para las organizaciones debido a la posibilidad de pérdida o daño de activos tales como; financieros, de servicios esenciales de red, o de la reputación y confianza de los clientes. Con el fin de preservar la información se ha demostrado que con la implantación de controles y procedimientos de seguridad realizados bajo las normativas ISO 27000 toda la información esencial se puede proteger.

Del proceso diagnóstico llevado a cabo, se puede concluir que no existe una cultura de seguridad de la información dentro de entidad pública, tampoco existe sistemas de control de seguridad informática y de información, y mucho menos, procesos y procedimientos documentados para protección de la información.

La implementación del Plan de seguridad informática contribuyó permitiendo elevar en un grado muy significativo la seguridad en los 11 dominios de la norma ISO 27002, para lo cual es esencial que el equipo de trabajo y la alta gerencia se comprometa con la implementación de las políticas, ya que son el cimiento para obtener un avance significativo en la integridad, confidencialidad y disponibilidad de la información y los

servicios otorgados a la comunidad distrital y estén con el continuo cambio si las normativas de la entidad lo requieren.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Regional Autónoma de los Andes; por motivar el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Acissi. (2015). *Seguridad Informática Hacking ÉTICO [Computer Security ETHICAL Hacking*]. Barcelona: ENI.

Candelario-Samper, J. J., & Rodríguez-Bolaño, M. (2015). Seguridad informática en el siglo xx: una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales [Computer security in the 20th century: a technological legal perspective with a focus on national and global organizations]. *Publicaciones E Investigación*, *9*, 153–162. https://doi.org/10.22490/25394088.1441

Carpentier, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas* [IT security in SMEs: Current status and best practices]. Barcelona: ENI.

Espinoza Zallas, E. A., & Rodríguez Pérez, R. (junio de 2017). Seguridad informática una problemática de las organizaciones en el sur de sonora. Revista de InvestigaciónAcadémica sin Frontera, 10(25). Obtenido de http://revistainvestigacionacademicasinfrontera.com

Espinoza-Zallas, E. A., & Rodríguez-Pérez, R. (2017). Seguridad informática una problemática de las organizaciones en el sur de sonora [IT security a problem for organizations in southern Sonora]. *Revista de InvestigaciónAcadémica sin Frontera,* *10*(25). Obtenido de http://revistainvestigacionacademicasinfrontera.com

Gil-Vera, V. D., & Gil-Vera, J. C. (2017). Seguridad informática organizacional [Organizational IT security]. *Scientia Et Technica, 22*, 193-197. Obtenido de http://www.redalyc.org/pdf/849/84953103011.pdf

Guerrero-Fernández, M. J. (2015). Sistemas de almacenamiento [Storage systems]. (5 ed.). España: Elearning.

Jean, C. (2016). La Seguridad Informática en la Pyme [Information Security in SMEs]. Barcelona: Edición ENI.

Suárez, D., & Ávila, A. (2017). Una forma de interpretar la seguridad informática [A way of interpreting computer security]. *Journal of Engineering and Technology, 4*(2). http://revistas.unilasallista.edu.co/index.php/jet/article/view/1015

Urbina, G. B. (2016). Introducción a la seguridad informática [Introduction to computer security]. México: Grupo Editorial Patria.