REVISIÓN BIBLIOGRÁFICA DE LA NORMA ISO 27001 Y SUS COMPONENTES.

DAVID GERARDO BENITEZ PINEDA

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERÍA DE SISTEMAS
TUNJA
2016

REVISIÓN BIBLIOGRÁFICA DE LA NORMA ISO 27001 Y SUS COMPONENTES.

DAVID GERARDO BENITEZ PINEDA
Cód. 3091293

ALEX PUERTAS GONZALEZ
TUTOR

UNIVERSIDAD SANTO TOMAS
FACULTAD DE INGENIERÍA DE SISTEMAS
TUNJA
2016

CONTENIDO

LISTA DE ILUSTRACIONES

pág.

LISTA DE TABLAS

pág.

INTRODUCCIÓN

Los estándares, en general, que se manejan dentro de las empresas, se ven reflejados en las políticas de calidad, los controles de seguridad y la adaptabilidad económica respecto a las ganancias. Estos procesos requieren parámetros que permitan evaluarlos, corregirlos y asegurar que se realicen en condiciones óptimas, para lograr que la empresa tenga la seguridad de elaborarlos y que en su desarrollo no se presenten problemas respecto a productos defectuosos o servicios inadecuados.

En la mayoría de las empresas los procesos están en manos de sistemas informáticos, por lo que, de su correcto funcionamiento depende la continuidad de los mismos y por ende la actividad de la empresa. Por lo cual existen métodos de gestión que garantizan un mínimo de seguridad a estos sistemas informáticos, regidos por mecanismos adscritos en un conjunto de normas denominado ISO 27000, lo que hace a este compendio de reglas un eslabón fundamental en la práctica de calidad de las empresas.

Para la realización de este trabajo se hizo una revisión bibliográfica de toda la norma ISO 27000 resaltando su historia, sus familias, sus características generales, como y cuando se aplica. Además de lo anterior, se señalan los pasos para lograr que norma se cumpla eficientemente; esto con el fin tener una guía de aprendizaje que permita la utilización correcta de dicha norma en las empresas que lo requieran.

Además de lo anterior, en este trabajo se describirán las tablas de control y sus respectivos controles para alcanzar las certificaciones en términos de la norma ISO 27001.

2. OBJETIVOS

2.1 GENERAL

Realizar la revisión bibliografía de la norma ISO 27001 teniendo en cuenta su aplicación, componentes e historia.

2.2 ESPECÍFICOS

- Identificar la familia de las normas ISO 27000 para su aplicación, objetivos y estructura

- Evidenciar los diferentes componentes que tienen la norma ISO 27001, en función de su aplicabilidad, conformación y escenarios de uso

- Socializar la revisión bibliográfica de la norma ISO 27001 a través de informes y presentaciones multimedia.

1 TITULO

REVISION BIBLIOGRAFICA DE LA NORMA ISO 27001 Y SUS COMPONENTES.

2 PLANTEAMIENTO DEL PROBLEMA

3.1 DESCRIPCION DEL PROBLEMA

El desconocimiento de las normas ISO, genera en la sociedad una falta de entendimiento en el proceso de mejoramiento y desarrollo, no solo para procedimientos en empresas sino también en la vida cotidiana, en términos de seguridad, calidad y medio ambiente. Es por esto que muchas veces no se logra que los procesos se cumplan efectivamente, dando como consecuencia desconocimiento y falta de oportunidades laborales para las personas.

Un ejemplo práctico es la no aplicabilidad de la norma ISO 27001, la cual enseña procesos de seguridad para actividades empresariales respecto de los sistemas de información y manejo de los datos. Es así que, el uso no adecuado e implementación fallida de los parámetros que expone la ISO puede conllevar a que la empresa sea afectada a por ataques informáticos dada la presencia de vulnerabilidades.

La falta de integración de sistemas de calidad en procesos empresariales y la vida cotidiana genera en las empresas, la no realización de procesos efectivos y la generación de sobrecostos, pérdida de tiempo, falta de efectividad y muchas veces lo más importante, pérdida de clientes, siendo estos el motor clave para cualquier organización.

3.2 PLANTEAMIENTO DEL PROBLEMA

El desconocimiento de la norma ISO 27001 de seguridad de la información para procesos, genera vulnerabilidades en el desarrollo de las actividades de las organizaciones y falta de oportunidad de empleo por falta de certificaciones en la misma.

3.3 SISTEMATIZACION DEL PROBLEMA

- ¿Cuantas sub divisiones existen de la norma ISO 27000?

- ¿Para qué actividades se puede aplicar la norma ISO 27001?

- ¿La socialización de la norma ISO 27001 ayudara al conocimiento de sus características y componentes y aplicabilidad?

3 JUSTIFICACION

Es importante realizar este trabajo porque ayuda en el conocimiento acerca de la norma ISO 27000 y su aplicabilidad en procesos sistémicos y de gestión en documentación informática. Además de esto es importante realizar la revisión bibliográfica de la norma porque brinda las bases necesarias para conseguir la certificación en ISO 27001.

La información es el capital más importante de una organización, puesto que es un bien irrecuperable, a diferencia de otros recursos de la misma. Esta comprende la esencia de la empresa, por lo cual es valioso protegerla y hacerla invulnerable, teniendo en cuenta que actualmente dicha información es ordenada y almacenada en sistemas informáticos, es vital que para estos sistemas existan herramientas actualizadas, que aseguren su integridad, confidencialidad y disponibilidad.

La revisión bibliográfica sirve para conocer la norma ISO 27001 con cada una de sus características y el cómo se le da una aplicabilidad y usabilidad correcta. Además de esto sirve para fundamentar y comprender los compromisos de confidencialidad, integridad de la información y disponibilidad de la misma, para los sistemas a los cuales se les aplica. Esto, sin dejar de lado el hecho de la fundamentación y el diseño de un plan de ruta para que los estudiantes, docentes y administrativos de la universidad Santo Tomas logren una ejecución de la norma ISO 27001, facilitando su conocimiento y la toma de decisiones.

Como carta de presentación ante una empresa, la certificación en ISO 27001, funciona como un plus, ya que, para las empresas del sector ingenieril, el desarrollo de procesos con estándares de calidad y certificaciones crea ante sus competidores grandes diferencias y además de eso, como trabajador se pueden conseguir mejores remuneraciones con su certificación y cumplimiento.

4 ESTADO DEL ARTE

Las normas ISO son algunas de las certificaciones que empresas buscan agregar y tener dentro de sus alcances, la ISO 27000 con cada una de sus familias puede aportar a las empresas y personas mejores prácticas y mejores oportunidades laborales.

La familia de la ISO 27000 es una de las normas que muestra materias para la seguridad de la información y que además de esto están asociadas a normas que ayudan a que esto se desarrolle en total cumplimiento como por ejemplo la norma ISO 9000 y la norma ISO 14000.

La norma ISO 27000 es la norma que reúne normas cada una específica y aplicable a cada uno de los diferentes problemas, que se puedan tener en la empresa o en la vida cotidiana. *"'ISO/IEC 27000 series'. ISO/IEC 27000 is an international standard entitled: Information technology — Security techniques — Information security management systems — Overview and vocabulary".*[1]

Para las empresas es muy importante que su seguridad, su información y todos sus sistemas estén protegidos y con políticas de seguridad con sociedades aplicables al hogar a "la vida cotidiana para que se dar mayor efecto de valor a lo que se realice dentro de la empresa y ser reconocida como una de las mejores del sector".[2]

Las funciones principales de las normas es dar pautas para que los procesos se desarrollen bajo una actividad concienzuda y con y que las evidencias, desarrollos, trabajos, actividades, tareas entre otras se realicen con una efectividad muy alta. "En el análisis de evidencia digital encontramos que la

[1]ISO. (02 de 11 de 2015). *ISO27000*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf
[2]Mellado, D., & Rosado, D. G. (2012). *An Overview of Current Information Systems Security.*Madrid: J.UCS Special Issue .

norma ISO 27000 es una de las normas de seguridad y es la que nos puede ayudar a solucionar este tipo de conflictos".[3]

El estudio de las normas ISO no es garante de empleo puesto que los estudiantes no siempre se familiarizan con un estudio concienzudo de que es en realidad y para que funciona cada uno de los parámetros que dicta la norma, además de esto la utilización de normas como la ISO no está bien parametrizadas al momento de realizar por ejemplo un trabajo de grado.

No solo las empresas viven atemorizadas por el robo de información "*In thismodernworld of computerization, lots of data isstored in ComputerSystem&hencerequirementtosavethis data increasedaybyday*."[4], y se sabe que lo más preciado es la información y lo que generaría si esta se llegara a perder o simplemente sus competidores tuvieran acceso a esta, por esta razón es que se viven pensando en los ataques, los hackers el robo de información entre otras.

Dentro de los sistemas de información se tiene en la vida cotidiana la necesidad de hablar de la computación en la nube o cloud computing, pero además de esto saber que todo está en la nube puede generar un gran riesgo de seguridad y además de eso presentar deficiencia en procesos, es cuando se debe empezar a pensar en cómo asegurar la información y como prevenir que se llegue a perder, dañar o simplemente llegue a manos que por ningún motivo debiera llegar. "*The quality of the results produced when performing these steps has a*

[3]Veber, J., &Klíma, T. (2014). Influence of standards ISO 27000 family on digital evidence analysis. Paper presented at the IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks, 103-111. Retrieved from www.scopus.com

[4]Shrivastava, A., Kumar, A., Rai, A., Payal, N., & Tiwari, A. (2013). ISO 27001 compliance via Artificial Neutral Network. *in computal intelligence and communication Network(CICN)*, (págs. 339-342).

crucial influence on the subsequent steps such as identifying loss, vulnerabilities, possible attacks and defining countermeasures" [5]

Existe manuales que no buscan suplir a la norma ISO 27001, si no que tratan de explicarla para despejar dudas en cuanto a redacción, para evitar que se tomen mal los conceptos de la norma y se ejecuten de manera errónea las indicaciones que en esta se plasman, uno de estos es la guía AUDISEC, que nos brinda una clara explicación de la norma basado en la percepción de profesionales con bastante experimentados en la guarda de información, y en los sistemas de gestión para la seguridad informática.

A su vez, existen programas informáticos que brindan instrucciones personalizadas a cada organización para la aplicación y manutención de un SGSI, como el que ofrece AUDISEC (GLOBALSGSI).

[5]Beckers, K., Schmidt, H., Küster, J. -.,&Faßbender, S. (2011). Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. Paper presented at the Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011, 327-333. doi:10.1109/ARES.2011.55

5 MARCO TEORICO

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

A la norma ISO 27000 les corresponden una serie de normas o familia de normas sobre seguridad informática.

Tabla 1: Familia norma ISO 27000

NORMA	CARACTERÍSTICA
ISO 27001	Esta es la especificación de un sistema de gestión de seguridad de la información (SGSI), que sustituyó a la antigua norma BS7799-2
ISO 27002	Esta es la norma numero 27000 serie de lo que originalmente era la norma ISO 177999 (que en si era conocido antes como BS7799-1)
ISO 27003	Este será el número oficial de una nueva norma pretende ofrecer una guía para la implementación de un sgsi(Sistema de Gestión de IS).
ISO 27004	Esta norma cubre la medición de información del sistema de seguridad y gestión de métricas, incluyendo controles de ISO27002.

ISO 27005	Este es el estándar ISO independiente metodología para la gestión de riesgos de seguridad de la información.
ISO 27006	Esta norma proporciona directrices para la acreditación de organizaciones que ofrecen la certificación del SGSI.
ISO 27007	Directrices para la seguridad de la información de auditoría de sistemas de gestión (centrados en el sistema de gestión)
ISO 27008 TR	Orientación para los auditores sobre los controles del SGSI (centrado en los controles de seguridad de la información)
ISO 27010	Información de gestión de la seguridad para las comunicaciones intersectoriales e inter-organizacionales
ISO 27011	Directrices de gestión de seguridad de información para las organizaciones de telecomunicaciones basados en la norma ISO / IEC 27002
ISO 27013	Directriz sobre la aplicación integrada de la norma ISO / IEC 27001 e ISO / IEC 20000-1
ISO 27014	Gobernabilidad seguridad de la información
ISO 27015	Directrices de gestión de seguridad de la información para los

TR	servicios financieros
ISO 27018	Código de prácticas para la protección de la información de identificación personal (PII) en nubes públicas
ISO 27031	Directrices para la información y la tecnología de comunicación de preparación para la continuidad del negocio
ISO 27032	Guía para la ciberseguridad
ISO 27034-1	Seguridad de las aplicaciones
ISO 27035	Información de gestión de incidentes de seguridad
ISO 27036-3	Seguridad de la información para las relaciones proveedor
ISO 27037	Directrices para la identificación, recolección, consolidación y preservación de evidencia digital

FUENTE: Autor

5.1 APLICACIÓN DE LA NORMA ISO 27001

Esta norma se aplica a todo prototipo de organizaciones como empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro, y

puede aplicarse a cualquier tipo de estas, sin importar su tamaño, tipo o naturaleza. (ICONTEC, 2006)

Según la GUÍA DE IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UNE – ISO/IEC 27001:2007 CON LA HERRAMIENTA GLOBALSGSI de AUDISEC “para la implantación de un SGSI se van a utilizar dos normas, la UNE ISO/IEC 27001:2007 que describe, como se ha indicado anteriormente, el ciclo PDCA de gestión del sistema; y la norma ISO/IEC 27002:2005 que es un guía de implantación de controles de seguridad”. (AudiSec, 2010)

AUDISEC también afirma que “esta norma tiene 11 dominios diferentes de controles que cubren todos los ámbitos de una entidad donde debe existir seguridad de la información. Estos dominios están divididos en 39 objetivos de control que a su vez comprenden 133 controles de seguridad”. (AudiSec, 2010)

Ilustración 1: dominios de controles de una entidad

FUENTE: AudiSec. (1 de febrero de 2010). *GUÍA DE IMPLANTACIÓN DE UN SISITEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.* Obtenido de audisec: www.audisec.es

6.2 BENEFICIOS DE UN SGSI

Un SGSI nos permite adquirir ciertos beneficios en su aplicación que probablemente ayudaran a la organización en su correcto funcionamiento.

Ilustración 2: beneficios de un SGSI

FUENTE: AudiSec. (1 de febrero de 2010). *GUÍA DE IMPLANTACIÓN DE UN SISITEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.* Obtenido de audisec: www.audisec.es

Como se observa los beneficios que se obtienen de aplicar un SGSI en nuestra organización se basan en la prevención de incidencias que pudieren ocurrir si no se toman estas medidas y en la seguridad que se reflejan en nuevos y antiguos clientes o beneficiarios de la organización, lo que conlleva a un crecimiento o evolución de la misma.

Ahora bien, aplicar un SGSI sin tener en cuenta los requisitos que proclama la norma ISO 27001, sin seguir estrictamente sus recomendaciones provee riesgos

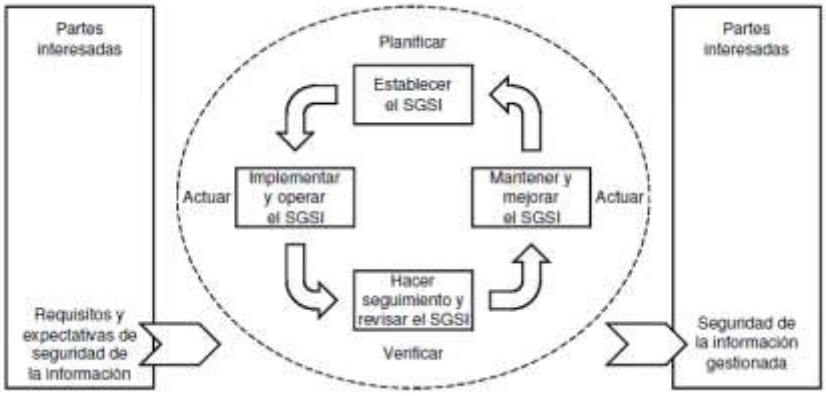
a los sistemas informáticos por lo que se deben seguir al pie de la letra los lineamientos que se especifican es esta norma, y en caso de no aplicar alguno de estos requisitos en nuestro SGSI, es importante justificar claramente los motivos o el motivo por el cual no se aplicó dicho requisito.

Según la norma NTC-ISO/IEC27001 “Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño y naturaleza”. (ICONTEC, 2006).

6.3 REQUISITOS GENERALES QUE DEBE CONTENER UN SGSI

Los requisitos que debe cumplir todo SGSI implementado en una organización según la norma ISO 27001 son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado

Ilustración 3: Modelo PHVA aplicado a los procesos de SGSI



Fuente: ICONTEC. (2006). *NORMA TÉCNICA NTC-ISO/IEC.* Bogotá, D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

El diagrama que observamos en la ilustración 2, es una representación gráfica del proceso del modelo PHVA que aplica los requisitos necesarios en un SGSI.

Las siglas PHVA significan:

Ilustración 4: modelo PHVA

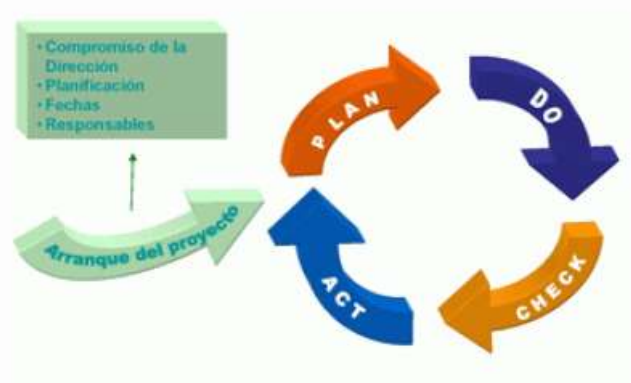
Planificar (establecer el SGSI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (hacer seguimiento y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y 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 con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Fuente: ICONTEC. (2006). *NORMA TÉCNICA NTC-ISO/IEC.* Bogotá, D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

6.4 ADAPTACIÓN DEL SGSI A LA ORGANIZACIÓN.

Para implementar un SGSI a una organización es necesario seguir un procedimiento que permitirá realizar esta adaptación de una manera satisfactoria.

Ilustración 5: Arranque del proyecto.



Fuente: ISO. (02 de 11 de 2013). *ISO27000.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf. pp 12

Para el arranque del proyecto (SGSI) es indispensable que la dirección o administración de la organización se comprometa, además de la planeación de ejecución, la asignación de fechas y de las personas responsables de la ejecución del proyecto.

Ilustración 6: planificación

Fuente: ISO. (02 de 11 de 2013). *ISO27000.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf. pp 13.

Al planificar la implementación de un SGSI, es importante definir los alcances que tendrá el SGSI, en función de las características de la organización, como el tamaño la tecnología, el tipo de información, la norma ISO 27001 recomienda que inicialmente el alcance del SGSI debe ser limitado, para a largo o mediano plazo cubrir totalmente la organización.

Seguidamente se concreta la política de seguridad teniendo en cuenta todos los recursos legales y de contrato con que cuenta la organización, todo en rasgos generales, y sin especificar procedimientos.

Según lo indica ISO 27001 hay que "definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable" el riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo." (ISO, ISO27000, 2013)

Además hay que elaborar un inventario de activos donde se ubican todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.[6]

Identificar amenazas y vulnerabilidades que afectan a los activos del inventario.

Encontrar los impactos que podrían suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

[6]ISO. (02 de 11 de 2013). *ISO27000*. Obtenido de http://www.iso27000.es. pp 14.

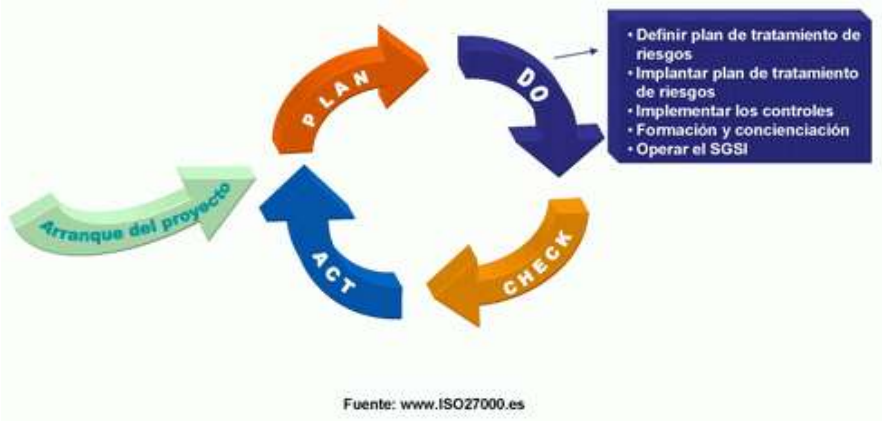
Evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

Seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 y otros controles adicionales si se consideran necesarios.

Hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

La llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

Ilustración 7: Implementación del SGSI



Fuente: ISO. (02 de 11 de 2013). *ISO27000.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf. pp 14.

Determinar el plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

Implantar plan de tratamiento de riesgos con la meta de alcanzar los objetivos de control identificados[7].

Realizar los controles todos los que se seleccionaron en la fase anterior.

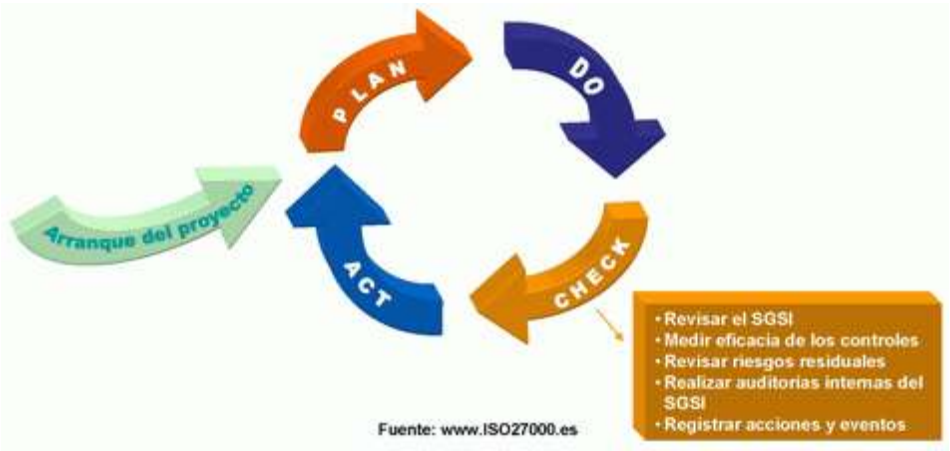
Formación y concienciación de todo el personal en lo relativo a la seguridad de la información.

Búsqueda y aplicación de normas, manuales, procedimientos e instrucciones.

Gestionar las operaciones del SGSI y todos los recursos que se le asignen.

Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

Ilustración 8: seguimiento.



[7]ISO. (02 de 11 de 2013). *ISO27000*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf. pp 15.

Fuente: ISO. (02 de 11 de 2013). *ISO27000.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf. pp 15.

Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.[8]

Revisar regularmente la eficacia del SGSI en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.

Medir la eficacia de los controles para verificar que se cumple con los requisitos de seguridad.

Revisar regularmente la evaluación de riesgos los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

Realizar regularmente auditorías internas para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

[8]ISO. (02 de 11 de 2013). *ISO27000*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf. pp 15.

Revisar regularmente el SGSI por parte de la Dirección para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

Actualizar planes de seguridad teniendo en cuenta los resultados de la monitorización y las revisiones.

Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI sirve como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

Ilustración 9: mejora continua

Fuente: ISO. (02 de 11 de 2013). *ISO27000.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf. pp 16.

Poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.

Entablar acciones correctivas para solucionar inconformidades detectadas.

Prevenir potenciales inconformidades.

Comunicar las acciones y mejoras a todos los interesados y con el nivel adecuado de detalle.

La eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

6 MARCO CONCEPTUAL

Cada uno de los términos que se utiliza en la ingeniería de sistemas debe ser aclarado y especificado correctamente, puesto que para cada persona las palabras puede llegar a significar diferente según el contexto y como se pueda llegar a leer dentro de una oración o párrafo.

6.1 ISO

Se denomina ISO a la Organización Internacional para la Estandarización, la cual se trata de una federación cuyo alcance es de carácter mundial, ya que está integrada por cuerpos de estandarización de 162 países. Esta organización se estableció en 1947, como un organismo no gubernamental, cuya misión es promover a nivel mundial el desarrollo de las actividades de estandarización.

6.2 EIC

The International Electrotechnical Commission (IEC) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

Close to 20 000 experts from industry, commerce, government, test and research labs, academia and consumer groups participate in IEC Standardization work.

6.3 ISO/EIC 27000

Mediante el uso de la familia de normas UNIT-ISO/IEC 27000, las organizaciones pueden desarrollar e implantar un marco para la gestión de la seguridad de sus activos de información, incluyendo información financiera, propiedad intelectual y detalles de sus empleados, o información confiada a la organización por sus clientes o terceras partes. Estas normas también pueden

ser utilizadas para prepararse para una evaluación independiente de sus SGSI aplicada a la protección de la información.

La gestión eficaz de la seguridad de la información es un aspecto primordial para salvaguardar a las organizaciones de los riesgos que pueden dañar de forma importante sus sistemas de información.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) han desarrollado una serie de normas internacionales de amplísima difusión a nivel mundial al respecto de esta problemática.

6.4 ISO/EIC 27001

Information security management, family of standards helps organizations keep information assets secure. Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system

6.5 SEGURIDAD INFORMATICA

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

6.6 SISTEMAS

Resulta de la interacción entre los componentes físicos que se denominan hardware y los lógicos que se denominan software. A estos hay que agregarles el recurso humano, parte fundamental para un sistema informático.[9]

6.7 REDES

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, "*la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo*".[10]

7.8 BASE DE DATOS

Una base de datos es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico. (MASADELANTE, 2014)

7.9 USABILIDAD

Se refiere básicamente a la facilidad de uso de una aplicación o producto interactivo[11].

[9] INFORMÁTICAHOY. (11 de 11 de 2015). *informatica hoy*. Obtenido de http://www.informatica-hoy.com.ar

[10] REDUSERS. (17 de 2 de 2009). Obtenido de http://www.redusers.com

[11] MONTERO, H., & SANTAMARIA, O. (2009). *Informe APEI Sobre Usabilidad.* Gijon: Asociación Profesional de Especialistas en Información.

Es un atributo de calidad cuya definición formal es el resultado de la enumeración de los diferentes componentes o variantes a través de los cuales puede ser medida. (MONTERO & SANTAMARIA, 2009)

7.10 ESCALABILIDAD

Propiedad de un sistema, de una red o de un proceso que le permite incrementar la cantidad de operaciones (concurrentes) a la vez que se mantiene un nivel de servicio aceptable, aun cuando la demanda aumenta.[12]

7.11 HACKING

Llamamos hacking a un conjunto de técnicas para acceder a un sistema informático sin autorización. Existe autorización cuando se dispone de un control de acceso mediante uso de identificadores de usuario y passwords. Es un término tradicionalmente ligado a la libertad de información de internet. En sus códigos está el respetar la vida privada, pero eso después de aprender cómo funcionan los sistemas y donde están los datos.[13]

[12]administrator, w. (15 de 9 de 2009). *club de investigación tecnológica*. Obtenido de http://clubdeinvestigacion.com

[13]GIMENEZ, v. (2013). *Hacking y Ciberdelito.* Valencia: UNIVERSIDAD POLITECNICA DE VALENCIA.

7 METODOLOGIA

7.1 TIPO DE INVESTIGACIÓN

Se realiza un estudio descriptivo con el fin de estudiar la norma ISO 27001 para tratar de responder a las preguntas ¿Por qué no se cuenta con una certificación ISO?, ¿Por qué se tienen otras certificaciones en la empresa?, y así determinar para determinar Quiénes pueden ser los usuarios potenciales y personas que fácilmente pueden aplicar a estas certificación.

7.2 MÉTODO DE INVESTIGACIÓN

Esta investigación requiere del método deductivo, puesto va de lo general a lo particular, y es necesario por el tipo de información que se solicita, adquiriendo en primer lugar una noción de la ISO para llegar posteriormente al análisis estratégico de las fortalezas y debilidades con que se cuenta, así como las amenazas y oportunidades para realizar el análisis y recopilación bibliográfico de la norma ISO 270001.

7.3 VARIABLES

- Utilidad
- Componentes
- Escalabilidad

7.4 POBLACIÓN

Por ser un trabajo descriptivo no tendremos una población específica sobre la cual hacer un trabajo o realizar algún tipo de ejercicio

8.5 INSTRUMENTOS PARA RECOPILAR INFORMACIÓN

Revisión bibliográfica de los diferentes autores

8.6 INSTRUMENTOS PARA RECOPILAR INFORMACIÓN

Las normas de la ISO se encuentras relacionadas en tesis, libros, artículos y estos son los que utilizaremos como guía y como fuente para recopilar la información necesaria en el desarrollo del trabajo; sin dejar de lado fuentes de internet como la página de la ISO

8.7 METODOLOGÍA DE LA INVESTIGACIÓN

Identificar la norma ISO 27000 con cada una de las familias que componen su estructura y sus objetivos, recolectando información de cada una de sus funcionalidades, y utilidad. Usando como estándar de seguridad cada uno de los diferentes modelos de las normas ISO y otras normas que puedan ayudar a la comprensión de esta.

Analizar cada uno de los componentes que puede tener la conformación de escenarios en el uso de la norma ISO con respecto a cómo funciona al momento de realizar su aplicación en empresas, usando como estrategia la utilización dada por sectores de seguridad informática y seguridad de datos.

Presentar una socialización a los interesados en conocer más acerca de la norma ISO buscando que se genere proyectos para su adaptación, cambio y uso en diferentes espacios de la vida cotidiana en empresas, además de esto realizar una convocatoria para mostrar la viabilidad de las certificaciones y así lograr que no solo los proyectos avancen sino que también la universidad genere procesos de mayor calidad.

8 IDENTIFICACION DE LA NORMA ISO 27001

La norma ISO 27000 siendo un compendio de estándares sobre seguridad informática para cualquier tipo de organización, debe evolucionar a la par con los riesgos que pudieren vulnerar la información. Y teniendo en cuenta que actualmente existen muchas personas con el conocimiento para poner en peligro la información de la organización, y que con el avance de la tecnología es necesario disponer de toda la información en sistemas informáticos que corren el riesgo de ser atacados.

La norma ISO 27001 da rasgos generales que pueden ser aplicados a cualquier organización, pero esta debe proveer las herramientas indicadas al SGSI de la organización con el fin de que este no se vuelva obsoleto con el avance de la tecnología y los medios informáticos. Básicamente la mayor desventaja que tiene la norma ISO 27001 está en su adaptación o implementación dentro de la organización, y esta específicamente en la planeación, pues al brindar requisitos tan generales, como una guía, las características de cada empresa podrían alterar la efectividad de la norma. Y existirá un estado de vulnerabilidad hasta que la implementación del SGSI esté completa.

El SGSI que provee la norma ISO 27001 no es infalible, puesto que la mayor responsabilidad de su ejecución y de su eficacia recae sobre el capital humano de la organización, por lo que es necesario que este SGSI sea elaborado, administrado y ejecutado por personal calificado, certificado, con el compromiso y disposición suficiente para que los procesos involucrados en la implementación del SGSI se lleven a cabo eficazmente.

Los estándares ISO se revisan y evalúan cada 4 o 5 años, así se actualiza la norma ISO 27001, con esto se garantiza que cuando pasa este periodo se inspeccionaran los riesgos y vulnerabilidades nuevas que hayan surgido o

evolucionado durante este lapso de tiempo, el problema latente es la velocidad con que avanza la tecnología y con ello nuevos tipos de fraudes y peligros que pueden atentar contra la información de nuestra organización; dejando la duda si esta revisión se hace con la frecuencia requerida.

Uno de los beneficios más importantes que posee el SGSI que provee la ISO 27001, y en lo que la mayoría de autores coinciden es el manejo que se le da a la información, puesto que es un requisito de la ISO 27001, que esta se ordene de tal forma que se fácil de consultar, de guardar y por ende de proteger, dándole a la organización el plus de la facilidad y agilidad con que podríamos examinarla y analizarla, lo que en tiempos y movimientos representa ganancias a la organización y por ende a los clientes o beneficiarios.

La asignación de los recursos para el SGSI debe ser acorde con el tamaño y prioridades en la información a guardar, se deben disponer de los recursos necesarios, para que la ejecución sea óptima.

Diferentes autores como el Ing. Manuel Collazos Balaguer afirman que en la norma ISO 27001 del 2013, los requisitos son más difíciles de interpretar que otras ediciones de la norma como la del 2005, debido a que se utilizan nuevos conceptos, este podría representar un problema en la aplicación, por lo que es necesario que estos conceptos sean aclarados. Lo bueno de esta edición es que se removieron inconsistencias de las ediciones anteriores[14]

[14]Balaguer, I. M. (2014). *la nueva version ISO 27001:2013: un cambio en la integracion de los sistemas de gestion.* lima: colegio de ingenieros del Peru.

9.1 OBJETIVOS DE CONTROL Y CONTROLES

La norma ISO nos da los parámetros y lineamientos generales para realizar los controles y además de esto cada una de las posibles acciones que podemos desarrollar y lograr el cumplimiento de la misma.

La información relacionada a continuación es tomada de la norma[15] y ajustada para una fácil comprensión por parte del autor y además de eso de los que lean el libro.

ISO 27001 TABLA DE CONTROLES		
POLÍTICA DE SEGURIDAD	Política de seguridad de la información	Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Organización Interna Partes externas	Objetivo: Gestionar la seguridad de la información dentro de la organización
GESTIÓN DE ACTIVOS	Responsabilidad por los activos Clasificación de la información	Objetivo: lograr y mantener la protección adecuada de los activos organizacionales, asegurando que la información recibe el nivel de protección adecuado
SEGURIDAD DE LOS RECURSOS HUMANOS	Antes de la contratación laboral Durante la vigencia de la contratación laboral Terminación o cambio del contratación laboral	Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las

[15] 2006, *Sistemas de gestión de la seguridad de la información,* Bogotá D.C., Colombia, ICONTEC

		instalaciones, reduciendo el riesgo de error humano
SEGURIDAD FÍSICA Y DEL ENTORNO	Áreas seguras Seguridad de los equipos	Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones, perdida de la información de la organización.
GESTIÓN DE COMUNICACIONES Y OPERACIONES	Procedimientos operacionales y responsabilidades Gestión de la prestación del servicio por terceras partes Planificación y aceptación del sistema Protección contra códigos maliciosos y móviles Respaldo Gestión de la seguridad de las redes Manejo de los medios Intercambio de Información Servicios de comercio electrónico Monitoreo	Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información.
CONTROL DE ACCESO	Requisito del negocio para el control de acceso Gestión del acceso de usuarios Responsabilidades de los usuarios	Objetivo: controlar el acceso a la información.

	Control de acceso a las redes Control de acceso a las aplicaciones y a la información Computación móvil y trabajo remoto	
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	Requisitos de seguridad de los sistemas de información Controles criptográficos Seguridad de los archivos del sistema Seguridad en los procesos de desarrollo y soporte Seguridad de los archivos del sistema Seguridad en los procesos de desarrollo y soporte Gestión de la vulnerabilidad técnica	Objetivo: garantizar que la seguridad es parte integral de los sistemas de información.
GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN	Reporte sobre los eventos y las debilidades de la seguridad de la información Gestión de los incidentes y las mejoras en la seguridad de la información	Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.
GESTIÓN DE LA CONTINUIDAD	Aspectos de seguridad de la información, de la	Objetivo: contrarrestar las interrupciones en las

DEL NEGOCIO	gestión de la continuidad del negocio	actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.
CUMPLIMIENTO	Cumplimiento de los requisitos legales Cumplimiento de las políticas y las normas de seguridad y cumplimiento Consideraciones de la auditoría de los sistemas de información	Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

A.5 POLÍTICA DE SEGURIDAD

A.5.1 Política de seguridad de la información

Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

A.5.1.1 A.5.1.2	Documento de la política de seguridad de la información. Revisión de la política de seguridad de la información.	Control La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.
		Control La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A.6.1 Organización Interna

Objetivo: gestionar la seguridad de la información dentro de la organización.

A.6.1.1	Compromiso de la dirección con la seguridad de la información.	La dirección debe apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información.	Control Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes.
A.6.1.3	Asignación de responsabilidades para la seguridad de la información.	Control Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información.
A.6.1.4	Proceso de autorización para los servicios de procesamiento de información.	Control Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información.
A.6.1.5	Acuerdos sobre confidencialidad	Control Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con las autoridades	Control Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.1.7	Contacto con grupos de interés especiales	Control Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.

A.6.1.8	Revisión independiente de la seguridad de la información	controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

A.6.2 Partes externas

Objetivo: mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

A.6.2.1	Identificación de los riesgos relacionados con las partes externar	Control Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	Control Todos los requisitos de seguridad identificados se deben considerar antes de dar acceso a los clientes a los activos o la información de la organización
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	Control Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o
		gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad

A.7 GESTIÓN DE ACTIVOS

A.7.1 Responsabilidad por los activos

Objetivo: lograr y mantener la protección adecuada de los activos organizacionales.

A.7.1.1	Inventario de activos	Control Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad" de una parte designada de la organización
A 7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información

A.7.2 Clasificación de la información

Objetivo: asegurar que la información recibe el nivel de protección adecuado.

A.7.2.1	Directrices de clasificación	La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.
A.7.2.2	Etiquetado y manejo de información	Control Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.

A.8 SEGURIDAD DE LOS RECURSOS HUMANOS

A.8.1 Antes de la contratación laboral

Objetivo: asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.

A.8.1.1	Roles y	Control

	responsabilidades	Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización
A.8.1.2	Selección	Control Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos
S.8.1.3	Términos y condiciones laborales.	Control Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

A.8.2 Durante la vigencia de la contratación laboral

Objetivo: asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano

A.8.2.1	Responsabilidades de la dirección	Control La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la

		organización.
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Control Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.
A.8.3 Terminación o cambio del contratación laboral Objetivo: asegurar que los empleados, contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.		
A.8.3.1	Responsabilidades en la terminación	Control Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.
A.8.3.3	Retiro de los derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del

		cambio.

A.9 SEGURIDAD FÍSICA Y DEL ENTORNO

A.9.1 Áreas seguras

Objetivo: evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.

A.9.1.1	Perímetro de seguridad física	Control Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información
A.9.1.2	Controles de acceso físico.	Control Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
A.9.1.3	Seguridad de oficinas, recintos e instalaciones.	Control Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
A.9.1.4	Protección contra amena zas externas y ambien-tales.	Control Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.
A.9.1.5	Trabajo en áreas seguras	Control Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.
A.9.1.6	Áreas de carga, despacho y acceso público	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y, si es posible,

		aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.
A.9.2 Seguridad de los equipos Objetivo: evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.		
A.9.2.1	Ubicación y protección de los equipos.	Control Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado
A.9.2.2	Servicios de suministro	Control Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.
A.9.2.3	Seguridad del cableado.	Control El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños.
A.9.2.4	Mantenimiento de los equipos.	Control Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.
A.9.2.5	Seguridad de los equipos fuera de las instalaciones.	Control Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos.	Control Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para

		asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.
A.9.2.7	Retiro de activos	Control Ningún equipo, información ni software se deben retirar sin autorización previa.

A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

A.10.1 Procedimientos operacionales y responsabilidades

Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información.

A.10.1.1	Documentación de los procedimientos de operación.	Control Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.
A.10.1.2	Gestión del cambio.	Control Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.
A.10.1.3	Distribución de funciones.	Control Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación.	Control Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no

		autorizados en el sistema operativo
A.10.2Gestión de la prestación del servicio por terceras partes Objetivo: implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes.		
A.10.2.1	Prestación del servicio	Control Se deben garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes.
A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	Control Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares
A.10.2.3	Gestión de los cambios en los servicios por terceras partes	Control Los cambios en la prestación de los servicios incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.
A.10.3 Planificación y aceptación del sistema Objetivo minimizar el riesgo de fallas de los sistemas.		
A.10.3.1	Gestión de la capacidad.	Control Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.

A.10.3.2	Aceptación del sistema.	Control Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.
A.10.4 Protección contra códigos maliciosos y móviles Objetivo: proteger la integridad del software y de la información.		
A.10.4.1	Controles contra códigos maliciosos.	Control Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios
A. 10.4.2	Controles contra códigos móviles	Control Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados.
A.10.5 Respaldo Objetivo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.		
A.10.5.1	Respaldo de la información.	Control Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
A.10.6 Gestión de la seguridad de las redes Objetivo: asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de las redes.	Control Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los

		sistemas y aplicaciones que usan la red, incluyendo la información en tránsito
A.10.6.2	Seguridad de los servicios de la red.	Control En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente
A.10.7 Manejo de los medios Objetivo: evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.		
A.10.7.1	Gestión de los medios removibles.	Control Se deben establecer procedimientos para la gestión de los medios removibles.
A.10.7.2	Eliminación de los medios.	Control Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales
A.10.7.3	Procedimientos para el manejo de la información.	Control Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado
A.10.7.4	Seguridad de la documentación del sistema.	Control La documentación del sistema debe estar protegida contra el acceso no autorizado
A.10.8 Intercambio de Información Objetivo: mantener la segundad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.		
A.10.8.1	Políticas y	Control

	procedimientos para el intercambio de información.	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.
A.10.8.2	Acuerdos para el intercambio	Control Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización
A. 10.8.4	Mensajería electrónica.	Control La información contenida en la mensajería electrónica adecuada debe tener la protección
A.10.8.5	Sistemas de información del negocio.	Control Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.
A.10.9 Servicios de comercio electrónico Objetivo: garantizar la seguridad de los servicios de comercio electrónico, y utilización segura.		
A.10.9.1	Comercio electrónico	Control La información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.

A.10.9	Transacciones en línea	Control La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración , divulgación duplicación o repetición no autorizada del mensaje
A.10.9	Información disponible al público	Control La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada
A.10.10 Monitoreo		
Objetivo: detectar actividades de procesamiento de la información no autorizadas.		
A.10.10.1	Registro de auditorías	Control Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el finde facilitar las investigaciones futuras y el monitoreo del control de acceso.
A.10.10.2	Monitoreo del uso del sistema.	Control Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad.

A.10.10.3	Protección de la información del registro.	Control Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados.
A.10.10.4	Registros del administrador y del operador.	Control Se deben registrar las actividades tanto del operador como del administrador del sistema
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.
A.10.1.6	Sincronización de relojes	Control Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.

A.11 CONTROL DE ACCESO

A.11 Requisito del negocio para el control de acceso

Objetivo: controlar el acceso a la información.

A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso

A.11.2 Gestión del acceso de usuarios

Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

A.11.2.1	Registro de usuarios.	Control Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información
A.11.2.2	Gestión de privilegios.	Control Se debe restringir y controlar la asignación y uso de privilegios.
A.11.2.3	Gestión de contraseñas para usuarios.	Control La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.
A.11.2.4	Revisión de los derechos de acceso de los usuarios	Control La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios
A.11.3 Responsabilidades de los usuarios Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.		
A.11.3.1	Uso de contraseñas.	Control Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección v el uso de las contraseñas
A.11.3.2	Equipo de usuario desatendido.	Control Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A.11.3.3	Política de escritorio despejado y de pantalla	Control Se debe adoptar una política de escritorio despejado para reportes y medios de

	despejada.	almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.
A.11.4 Control de acceso a las redes Objetivo: evitar el acceso no autorizado a servicios en red.		
A.11.4.1	Política de uso de los servicios de red.	Control Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.
A.11.4.2	Autenticación de usuarios para conexiones externas	Control Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos
A.11.4.3	Identificación de los equipos en las redes.	Control La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto.	Control El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado
A.11.4.5	Separación en las redes.	Control En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.

A.11.4.6	Control de conexión a las redes.	Control Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio (véase el numeral 11.1).
A.11.4.7	Control de enrutamiento en la red.	Control Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.
A.11.5.1	Procedimientos de ingreso seguros	Control El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro.
A.11.5.2	Identificación y autenticación de usuarios	Control Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.
A.11.5.3	Sistema de gestión de contraseñas.	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.

A.11.5.4	Uso de las utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.
A.11.5.5	Tiempo de inactividad de la sesión	Control Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.
A.11.5.6	Limitación del tiempo de conexión.	Control Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.
A.11.6 Control de acceso a las aplicaciones y a la información Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de información.		
A.11.6.1	Restricción de acceso a la información.	Control Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.
A.11.6.2	Aislamiento de sistemas sensibles.	Control Los sistemas sensibles deben tener un entorno informático dedicado (aislados).
A.11.7 Computación móvil y trabajo remoto Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móvil y de trabajo remoto.		
A.11.7.1	Computación y comunicaciones móviles.	Control Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

A.11.7.2	Trabajo remoto.	Control Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

A.12.1 Requisitos de seguridad de los sistemas de información

Objetivo: garantizar que la seguridad es parte integral de los sistemas de información.

A.12.1.1	Análisis y especificación de los requisitos de seguridad	Control Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.

A.12.2 Procesamiento correcto en las aplicaciones

Objetivo: evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

A.12.2.1	Validación de los datos de entrada.	Control Se deben validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.
A.12.2.2	Control de procesamiento interno.	Control Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje.	Control Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.

A.12.2.4	Validación de los datos de salida.	Control Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias
A.12.3 Controles criptográficos Objetivo: proteger la confidencialidad autenticidad o integridad de la información,		
A.12.3.1	Política sobre el uso de controles criptográficos.	**Control** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión de llaves.	Control Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.
A.12.4 Seguridad de los archivos del sistema Objetivo: Garantizar la seguridad de los archivos del sistema.		
A.12.4.1	Control del software operativo.	Control Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.1 2.4.2	Protección de los datos de prueba del sistema.	Control Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse
A.12.4.3	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.

A.12.5 Seguridad en los procesos de desarrollo y soporte

Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.

	Procedimientos de control de cambios.	Control Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.
	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	Control Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

A.12.4 Seguridad de los archivos del sistema

Objetivo: Garantizar la seguridad de los archivos del sistema.

A.12.4.1	Control del software operativo.	Control Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.1 2.4.2	Protección de los datos de prueba del sistema.	Control Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse
A.12.4.3	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.

A.12.5 Seguridad en los procesos de desarrollo y soporte

Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.

	Procedimientos de control de cambios.	Control Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.
	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	Control Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.
A.12.5.3	Restricciones en los cambios a los paquetes de software.	Control Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.12.5.4	Fuga de información	Control Se deben evitar las oportunidades para que se produzca fuga de información.
A.12.5.5	Desarrollo de software contratado externamente	Control La organización debe supervisar y monitorear el desarrollo de software contratado externamente.
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

A.13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información

Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

A.13.1.1	Reporte sobre los eventos de seguridad de la infornación	Control Los eventos de seguridad de la Información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
A.13.1.2	Reporte sobre las debilidades de la seguridad	Control Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información

Objetivo: asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información
A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Control Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de

		seguridad de la información
A.13.2.3	Recolección de evidencia	Control Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio

Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Control Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
A.14.1.2	Continuidad del negocio y evaluación de riesgos	Control Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la	Control Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y

	seguridad de la información	asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio
A.14.1.4	Estructura para la planificación de la continuidad del negocio	Control Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes. y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Control Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

A.15 CUMPLIMIENTO

A.15.1 Cumplimiento de los requisitos legales

Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

A.15.1.1	Identificación de la legislación aplicable.	Control Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización
A.15.1.2	Derechos de propiedad intelectual (DPI).	Control Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con

		respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados
A.15.1.3	Protección de los registros de la organización.	Control Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.
A.15.1.4	Protección de los datos y privacidad de la información personal	Control Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	Control Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados
A.15.1.6	Reglamentación de los controles criptográficos	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes
A.15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento Objetivo: asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.		
A.15.2.1	Cumplimiento con las políticas y normas de seguridad.	Control Los directores deben garantizar que todos (os procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.
A.15.2.2	Verificación del cumplimiento técnico.	Control Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.
A.15.3 Consideraciones de la auditoría de los sistemas de información		

Objetivo: maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.

A.15.3.1	Controles de auditoría de los sistemas de información.	Control Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Control Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

9 CRONOGRAMA

Tabla 2: cronograma de actividades.

n°	nombre de tarea	duración (dias)	Julio	Agost	Sept	Oct	Nov	Dic
1	Revisión bibliográfica de la norma ISO 27001	115						
2	Presentación de anteproyecto	40						
3	Elaboración del proyecto	70						
4	Recopilación de información	8						
5	Selección de información	8						
6	Análisis de información	8						
7	Sustentación	1						

FUENTE: Autor.

10 CONCLUSIONES

Se realizó la revisión bibliografía de la norma ISO 27001 teniendo en cuenta su aplicación, componentes e historia, obteniéndose autores en su mayoría corporativos.

Se identificó la familia de las normas ISO 27000 para su aplicación, objetivos y estructura, siendo ésta un importante eslabón a tener en cuenta para asegurar el recurso más valioso de una organización, que es la información, teniendo en cuenta que es el único capital que si se pierde no se puede recuperar.

Se observaron los diferentes componentes que tienen la norma ISO 27001, en función de su aplicabilidad, conformación y escenarios de uso, siendo esta muy versátil y aplicable a todos los tipos de organizaciones.

La implementación de un sistema de la seguridad de la información es la forma más eficaz de proteger los sistemas informáticos y por ende la información de una organización.

El compromiso por parte de todos los involucrados en el proceso de implementación o renovación se un sistema de gestión de la seguridad de la información, debe ser grande, ya que estos representan un papel trascendental en la eficacia del sistema.

El conocimiento y análisis de los riesgos que cada día se generan para la información de la organización permita que el SGSI se mantenga a la altura para prever y afrontar cualquier inconveniente.

Las falencias más notorias de la norma ISO 27001 están en que dependen en gran medida del recurso humano, por lo que la hace propensa a errores, por lo que los procedimientos de implementación deben ser meticulosos; y que las

frecuencias de revisión por la ISO de la norma y los tiempos de actualización de las entidades que la promueven pueden ser muy amplios para la velocidad con que los riesgos evolucionan o se crean.

Para la implementación de un SGSI además de la norma ISO 27001 se requiere de la norma ISO 17002 puesto que esta ultima contiene los dominios, objetivos de control que son 133 controles.

11 BIBLIOGRAFIA

administrator, w. (15 de 9 de 2009). *club de investigación tecnológica*. Obtenido de http://clubdeinvestigacion.com

APA. (s.f.). *normas APA*. Obtenido de http://normasapa.com/formato-apa-presentacion-trabajos-escritos/

AudiSec. (1 de febrero de 2010). *GUÍA DE IMPLANTACIÓN DE UN SISITEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.* Obtenido de audisec: www.audisec.es

Balaguer, I. M. (2014). *la nueva version ISO 27001:2013: un cambio en la integracion de los sistemas de gestion.* lima: colegio de ingenieros del Peru.

FUNDACIÓN ACPO. (s.f.). Obtenido de http://fundacionacpo.org/

GIMENEZ, v. (2013). *Hacking y Ciberdelito.* Valencia: UNIVERSIDAD POLITECNICA DE VALENCIA.

ICONTEC. (2006). *NORMA TÉCNICA NTC-ISO/IEC.* Bogotá, D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

IEC. (5 de 11 de 2015). *International Electrotechnical Commission*. Obtenido de http://www.iec.ch/about/?ref=menu

INFORMÁTICAHOY. (11 de 11 de 2015). *informatica hoy*. Obtenido de http://www.informatica-hoy.com.ar

ISO. (02 de 11 de 2013). *ISO27000.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO. (4 de 11 de 2015). *implementaciónSIG.* Obtenido de http://www.implementacionsig.com/index.php/23-noticiac/29-que-es-iso

ISO. (2 de 11 de 2015). *ISO*. Obtenido de https://iso.statuspage.io/

KHARLAMOVA, L. (s.f.). *shutterstock.com.* Obtenido de www.shutterstock.com

MASADELANTE. (23 de 9 de 2014). *masadelante*. Obtenido de http://www.masadelante.com

MELLADO, D., & Rosado, D. G. (2012). *An Overview of Current Information Systems Security.*Madrid: J.UCS Special Issue.

MONTERO, H., & SANTAMARIA, O. (2009). *Informe APEI Sobre Usabilidad.* Gijon: Asociación Profesional de Especialistas en Información.

REDUSERS. (17 de 2 de 2009). Obtenido de http://www.redusers.com

SHRIVASTAVA, A., Kumar, A., Rai, A., Payal, N., & Tiwari, A. (2013). ISO 27001 compliance via Artificial Neutral Network. *in computal intelligence and communication Network(CICN)*, (págs. 339-342).

STANDARDIZATION, I. O. (2005). *Information Technology. Security Techniques. Information Security Management Systems. Requirements.* Geneva.

UNIT. (7 de 11 de 2015). *Instituto Uruguayo de Normas Tecnicas*. Obtenido de http://www.unit.org.uy/normalizacion/sistema/27000/

VEBER, J., & KLÍMA, T. (2014). Influence of standards ISO 27000 family on digital evidence analysis. Paper presented at the IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks, 103-111. Retrieved from www.scopus.com

BECKERS, K., SCHMIDT, H., KÜSTER, J. -.,& FAßBENDER, S. (2011). Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. Paper presented at the Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011, 327-333. doi:10.1109/ARES.2011.55

12 ANEXOS

13.1 PRINCIPIOS DE LA OCDE Y EL MODEL PHVA

Principio OCDE	Proceso de SGSI correspondiente y fase de PHVA
Toma de conciencia Los participantes deben estar conscientes de la necesidad de seguridad de los sistemas y redes de la información y de lo que pueden hacer para mejorar la seguridad.	Esta actividad es parte de la fase Hacer (véanse los numerales 4.2.2 y 5.2.2)
Responsabilidad Todos los participantes son responsables por la seguridad de los sistemas y redes de información.	Esta actividad es parte de la fase Hacer (véanse los numerales 4.2.2 y 5.1)
Respuesta Los participantes deberían actuar de una manera oportuna y en cooperación para evitar, detectar y responder ante incidentes de seguridad.	Ésta es en parte una actividad de seguimiento de la fase Verificar (véanse los numerales 4.2.3 y 6 a 7.3 y una actividad de respuesta de la fase Actuar (véanse los numerales 4.2.4 y 8.1 a 8.3). Esto también se puede cubrir por algunos aspectos de las fases Planificar y Verificar.
Valoración de riesgos Los participantes deberían realizar valoraciones de los riesgos.	Esta actividad es parte de la fase Planificar (véase el numeral 4.2.1) y la reevaluación del riesgo es parte de la fase Verificar (véanse los numerales 4.2.3 y 6 a 7.3).
Diseño e implementación de la seguridad Los participantes deberían incorporar la seguridad como un elemento esencial de los sistemas y redes de información.	Una vez que se ha realizado la evaluación de los riesgos, se seleccionan controles para el tratamiento de los riesgos como parte de la fase Planificar (véase el numeral 4.2.1). La fase Hacer (véanse los numerales 4.2.2 y 5.2) cubre la implementación y el uso operacional de estos controles.

Gestión de la seguridad Los participantes deberían adoptar un enfoque amplio hacia la gestión de la seguridad.	La gestión de riesgos es un proceso que incluye la prevención, detección y respuesta a incidentes, mantenimiento, auditorías y revisión continuos. Todos estos aspectos están cobijados en las fases de Planificar, Hacer, Verificar y Actuar.
Reevaluación Los participantes deberían revisar y reevaluar la seguridad de los sistemas y redes de información, y hacer las modificaciones apropiadas a las políticas, prácticas, medidas y procedimientos de seguridad.	La reevaluación de la seguridad de la información es una parte de la fase Verificar (véanse los numerales 4.2.3 y 6 a 7.3), en donde se deberían realizar revisiones regulares para verificar la eficacia del sistema de gestión de la seguridad de la información; y la mejora de la seguridad es parte de la fase Actuar (véanse los numerales 4.2.4 y 8.1 a 8.3).

3.2 CORRESPONDENCIA ENTRE LA NTC-ISO 9001:2000 LA NTC-ISO 14001:2004 Y LA PRESENTE NORMA

Esta norma	NTC-ISO 9001:2000	NTC-ISO 14001:2004
0.Introducción 0.1 Generalidades 0.2 Enfoque basado en procesos 0.3 Compatibilidad con otros sistemas de gestión	0. Introducción 0.1 Generalidades 0.2 Enfoque basado en procesos 0.3 Relación con la norma ISO 9004 0.4 Compatibilidad con otros sistemas de gestión	Introducción
1 Objeto 1.1 Generalidades 1.2 Aplicación	1. Objeto y campo de aplicación 1.1 Generalidades 1.2 Aplicación	1. Objeto y campo de aplicación
2 Referencia normativa	2. Referencias normativas	2. Referencias normativas
3 Términos y definiciones.	3. Términos y definiciones	3. Términos y definiciones
4. Sistema de gestión de la	4. Sistema de gestión de	4. Requisitos del

seguridad de la información 4.1 Requisitos generales	la calidad 4.1 Requisitos generales	sistema de gestión ambiental 4.1 Requisitos generales
4.2 Establecimiento y gestión del SGSI 4.2.1 Establecimiento del SGSI 4.2.2 Implementación y operación del SGS 4.2.3 Seguimiento y revisión del SGSI	8.2.3 Seguimiento y medición de los procesos 8.2.4 Seguimiento y medición del producto	4.4 Implementación y operación 4.5.1 Seguimiento y medición
4.2.4 Mantenimiento y mejora del SGSI		
4.3 Requisitos de documentación 4.3.1 Generalidades 4.3.2 Control de documentos 4.3.3 Control de registros	4.2 Requisitos de la documentación 4.2.1 Generalidades 4.2.2 Manual de la calidad 4.2.3 Control de los documentos 4.2.4 Control de los registros	4.4.5 Control de documentos 4.5.4 Control de los registros
5. Responsabilidad de la Dirección	5. Responsabilidad de la dirección	
5.1 Compromiso de la dirección	5.1 Compromiso de la dirección 5.2 Enfoque al cliente 5.3 Política de la calidad 5.4 Planificación 5.5 Responsabilidad, autoridad y comunicación	4.2 Política ambiental 4.3 Planificación
5.2 Gestión de recursos 5.2.1 Provisión de recursos 5.2.2 Formación, toma de conciencia y competencia	6. Gestión de los recursos 6.1 Provisión de recursos 6.2 Recursos humanos 6.2.2 Competencia, toma de conciencia y formación 6.3 Infraestructura 6.4 Ambiente de trabajo	4.4.2 Competencia, formación y toma de conciencia

6. Auditorías internas del SGSI	8.2.2 Auditoría interna	4.5.5 Auditoría interna
7. Revisión del SGSI por la dirección 7.1 Generalidades 7.2 Información para la revisión 7.3 Resultados de la revisión	5.6 Revisión por la dirección 5.6.1 Generalidades 5.6.2 Información para la revisión 5.6.3 Resultados de la revisión	4.6 Revisión por la dirección
8. Mejora del SGSI 8.1 Mejora continua	8.5 Mejora 8.5.1 Mejora continua	
8.2 Acción correctiva	8.5.2 Acciones correctivas	4.5.3 No conformidad, acción correctiva y acción preventiva
8.3 Acción preventiva	8.5.3 Acciones preventivas	
Anexo A Objetivos de control y controles Anexo B Principios de la OCDE y de esta norma Anexo C Correspondencia entre la NTC-ISO 9001:2000, la NTC-ISO 14001:2004 y la presente norma	Anexo A Correspondencia entre las normas ISO 9001:2000 y la ISO 14001:1996	Anexo A Orientación para el uso de esta norma internacional Anexo B Correspondencia entre la ISO 14001:2004 y la ISO 9001:2000