IMPLEMENTACIÓN DEL SGSI EN EL ÁREA DE REDES DE COMPUSERVER BASADO EN LA NORMA ISO/IEC27001:2013

ÁLVARO CALDERÓN SÁNCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SARAVENA, ARAUCA

2015

IMPLEMENTACIÓN DEL SGSI EN EL ÁREA DE REDES DE COMPUSERVER BASADO EN LA NORMA ISO/IEC27001:2013

ÁLVARO CALDERÓN SÁNCHEZ

Tesis de grado para optar por el título:

Especialista En Seguridad Informática

Director de Proyecto:

Ing. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

SARAVENA, ARAUCA

2015

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Arauca, 19 septiembre 2015

DEDICATORIA

A mis hijos DEIMER FABIAN y JESSICA TATIANA, por ser la inspiración en todo mi camino y darme animo de seguir luchando con el fin de alcanzar las metas propuestas, por regalarme el tiempo que les correspondía a ellos.

A mis padres que desde el Cielo me están acompañando en este momento viendo el legado que en la fase terrenal inculcaron en mí para ser una persona íntegra, responsable y soñadora.

A mis hermanos por el apoyo incondicional que me brindaron durante el lapso de esta carrera, dándome esa fuerza necesaria en los momentos difíciles con el fin de no dejarme caer y poder lograr esta meta que hoy se ve reflejada.

AGRADECIMIENTOS

Agradezco primero a Dios por darme la vida y dotarme de inteligencia para llevar a feliz término mis proyectos. Reconozco el gran aporte de mis maestros quienes siguieron con gran interés este proceso y constantemente me orientaron.

En la vida no solo superamos obstáculos, también vivimos situaciones en las que se siente felicidad y es por ello que agradezco también a todas aquellas personas familia y amigos que a diario me rodean con sus buenas intenciones y afecto desinteresado.

CONTENIDO

Pag.

LISTA DE FIGURAS

Pag.

RESUMEN

Se presenta el diseño del Sistema de Gestión de Seguridad de la Información para para la Red de Datos de la empresa COMPUSERVER aplicándola norma ISO/IEC 27001:2013, con el fin degarantizar conexiones seguras y darle confianza a los clientes que hacen uso de la misma

- Estándar ISO/IEC 27001:2013
- Red de datos
- Puertos de comunicación
- Políticas de seguridad
- Ataques informáticos
- Buenas prácticas en la seguridad informática

INTRODUCCIÓN

Tanto en el ámbito comercial como el domiciliario y los espacios públicos; las redes inalámbricas han tomado gran impulso en los últimos años, conectando diversos equipos móviles, computadoras portátiles, tables, servicios que son ofrecidos en centros comerciales, hoteles, parques, cafés internet y en su propio hogar. Con esta diversidad de conexiones inalámbricas cabe la posibilidad de encontrar conexiones Wi-Fi inseguras a las cuales muchos usuarios al conectarse están expuestos a vulnerabilidades poniendo en riesgo su confidencialidad y disponibilidad de su información personal o corporativa.

El desarrollo de este proyecto comprende un análisis de riesgos de la red de datos de COMPUSERVER que permita identificar las amenazas y vulnerabilidades a la que puede estar expuesta, proporcionará un diseño de controles de seguridad que debería aplicarse en la red de datos que garantice conexiones seguras y la disponibilidad del servicio, también se abordaran buenas prácticas de seguridad de la información para capacitar al personal operativo y en general a la empresa.

1. PLANTEAMIENTO DEL PROBLEMA.

La empresa COMPUSERVER cuenta con una red de datos interconectando varios puntos de forma inalámbrica no superior a los dos (2) kilómetros y de forma cableada no superior a los 100 metros de distancia con el objetivo de distribuir el servicio de internet a los diferentes clientes.

Los equipos que actualmente cuenta son: un computador de escritorio que se usa como escenario para registrar los servicios de internet a los clientes, un modem ADSL que recibe la señal de internet por medio de una línea telefónica interconectado con un Router que está configurado con DHCP.

La empresa no cuenta con una administración adecuada de la red de datos, por lo tanto no tiene las políticas optimas de acuerdo a una norma de seguridad de la información solo provee limitación de acceso con contraseñas utilizando algoritmos de encriptación débiles como es el WEP.

La red está expuesta a cualquier ataque informático por poseer vulnerabilidades de seguridad encontrándose en eminente peligro de ser accedida por terceros conllevando al posible robo de información de la empresa. El diseño de la red lógica se encuentra en un sola (Mascara de subred) por lo cual todos los usuarios conectados tienen expuesta su información entre si violando la confidencialidad de los datos de los clientes que utilicen el servicio de internet de la red de datos de COMPUSEVER.

La administración de la red de COMPUSERVER se encuentra limitada por la carencia de un sistema de un Sistema de Gestión de Seguridad de la Información, ya que en la actualidad no se han establecido parámetros de responsabilidades a los usuarios y empleados que hacen uso de la red informática de datos.

1.1. FORMULACIÓN DEL PROBLEMA

¿Cómo garantizar la disponibilidad, integridad y confidencialidad de la información a los usuarios de la red de datos de COMPUSERVER?

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Implementar un Sistema de gestión de Seguridad de la Información (SGSI) en el área de redes de COMPUSERVER aplicando la norma ISO/IEC 27001:2013

2.2. OBJETIVOS ESPECÍFICOS

- Contextualizar el contenido de la norma ISO/IEC 27001:2013 con el fin de obtener el debido conocimiento para el desarrollo del proyecto.

- Realizar un análisis de riesgos del estado actual de la red de datos de COMPUSERVER considerando la seguridad de la misma y las amenazas a las que está expuesta.

- Diseñar y recomendar los controles de seguridad que se deberían aplicar a la red de datos de COMPUSERVER para garantizar una conexión segura.

- Aplicar la norma ISO/IEC 27001:2013 a cada una de los controles, con el fin de que cumplan las normativas vigentes de seguridad de la información.

- Capacitar al personal operativo de la empresa COMPUSERVER en la utilización y manejo adecuado del SGSI con planes de concientización de seguridad.

3. JUSTIFICACIÓN

El aumento de la tecnología inalámbrica nos hace posible tener dispositivos electrónicos (Computadores, celulares, tablets, etc.) conectados entres si sin tener en cuenta la distancia geográficas y con la gran facilidad de tener equipos de puntos de acceso compactos como los ubiquiti que dan gran ventaja en la instalación física fácil y una gran variedad de configuración lógica. Por este concepto la empresa COMPUSERVER presta el servicio de conectividad a internet a una comunidad en el municipio de Saravena a distancias no mayores a 2 km.

COMPUSERVER les va a brindar a sus usuarios disponibilidad, integridad y confidencialidad de la información que se transmita por medio de la red de datos, convirtiéndose así en una empresa más competitiva y con el objetivo de crecer hasta convertirse en una ISP a nivel departamental.

Para el profesional en seguridad en redes que implemente este SGSI, le brinda una experiencia sobre el manejo de la norma ISO/IEC 27001, aplicándola en el campo real aumentando su nivel profesional conllevándolo al montaje de SGSI más complejos y con mejores resultados en cada proyecto.

Los egresados de la UNAD deben ser muy competitivos en el campo laboral, colocando a esta universidad como una de las mejores a nivel nacional e internacional por el alcance de la educación que brinda utilizando la metodología virtual.

4. MARCO DE REFERENCIAL

4.1. MARCO TEÓRICO

RED INFORMATICA: Desde hace muchos años se utiliza este término para identificar a toda estructura que combine los métodos físicos y técnicos para interconectar equipos informáticos con el propósito de lograr un intercambio efectivo de información en un entorno específico, ya sea laboral, personal o global

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.

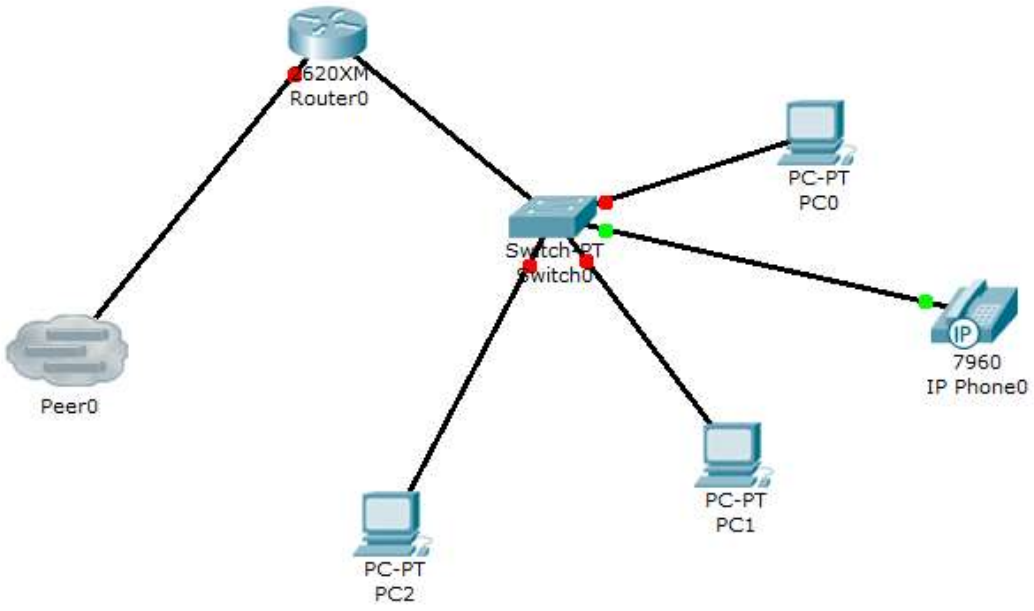
También hay mensajes, que es lo que estos roles intercambian. La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más extendido de todo el modelo TCP/IP, basado en el modelo de referencia o teórico OSI.[1]

Las redes son altamente efectivas para poder compartir todo tipo de información y los recursos que estén disponibles en nuestras computadoras, proveyéndonos de herramientas para centralizar o distribuir, las diferentes necesidades informáticas que podamos tener.

La experiencia que podamos tener como usuarios con una red informática se remite al mero uso de nuestras computadoras para leer noticias, chatear, descargar archivos, imprimir en una impresora compartida, entre otros. Para nosotros un simple par de clics alcanzan para poner en funcionamiento la red según nuestros pedidos y obtener el producto que estábamos buscando. Los procesos para cumplir con nuestras peticiones así como su funcionamiento es totalmente transparenten para el usuario.

[1] Concepto de Red Informática [En línea] <http://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n>[Tomado el 26 de mayo de 2015]

FIG.1DIAGRAMA BÁSICO DE UNA RED DE DATOS



CIBERSEGURIDAD: Cada día se habla más de la ciberseguridad por medios masivos como la televisión, la prensa, redes sociales, artículos en fin se ha masificado, encontrándonos con titulares como "el mayor ataque ciberterrorista es cuestión de tiempo". Todos los especialistas en la materia dan su punto de vista aumentando la ola del tema de la seguridad de la información, pero no es para

menos ya que la masificación de la tecnología, todos estamos inmersos en la transferencia de datos, tocándonos este flagelo de la seguridad de la información que transmitimos por medio de redes de datos, telefónicos, etc.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: El sistema de Gestión de Seguridad de la Información SGSI es en parte la solución del flagelo de la delincuencia informática, para las empresas u organizaciones que implementen un SGSI basándose en la norma ISO/IEC 27000 está colocando a salvo la información que se trasmita por los medio electrónicos y bajando con ello los índices de robos informáticos

Un sistema de gestión de la seguridad de la información (SGSI) (en inglés: information security management system, ISMS) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno[2].

4.2. MARCO CONCEPTUAL

4.2.1. Aspectos Básicos Norma ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

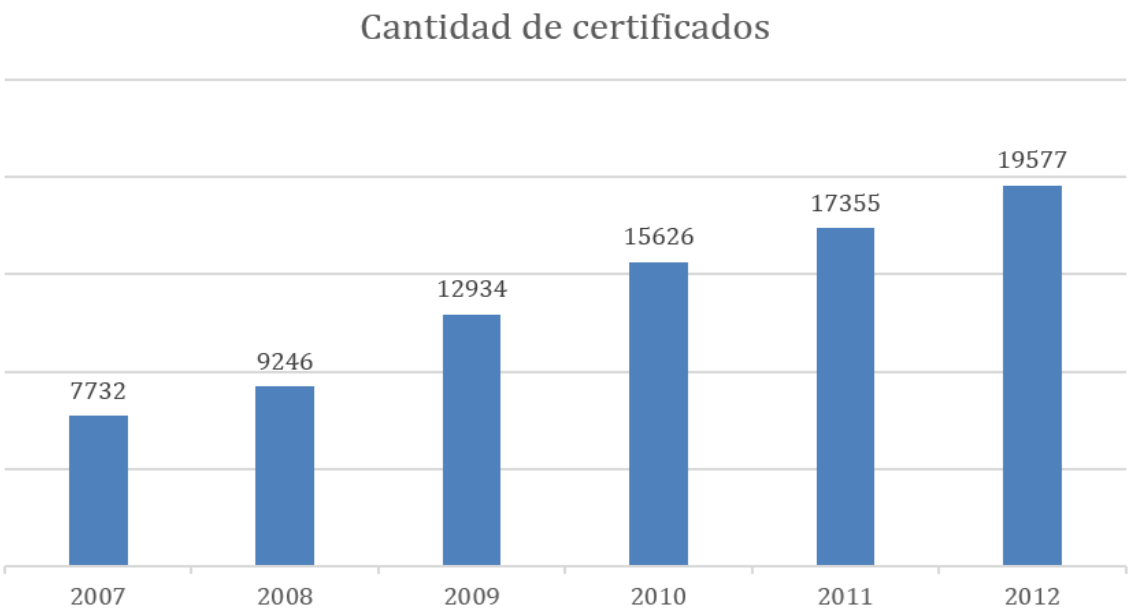
ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad

[2]Sistema de gestión de la seguridad de la información [En línea] <http://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n>[Tomado el 26 de mayo de 2015]

de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años:[3]

FIG 2 ENCUESTA ISO SOBRE CERTIFICACIONES DE LA NORMA PARA SISTEMAS DE GESTIÓN



Fuente: http://www.iso27001standard.com/es/que-es-iso-27001/

4.2.2. Cómo funciona la ISO 27001:2013

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles

[3]Qué es norma ISO 27001 – Conceptos Básicos [En línea] <http://www.iso27001standard.com/es/que-es-iso-27001/> [Tomado el 26 de mayo de 2015]

son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).[4]

Por lo tanto, la filosofía principal de la norma ISO 27001:2013 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

FIG3 ESTRUCTURA DE ISO 27001:2013

Fuente: http://www.iso27001standard.com/es/que-es-iso-27001/

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar

[4] Como Funciona la ISO 27001 – Conceptos Básicos [En línea] <http://www.iso27001standard.com/es/que-es-iso-27001/> [Tomado el 26 de mayo de 2015]

todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.[5]

4.2.3. ¿Por qué ISO 27001 es importante para su empresa?

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

Cumplir con los requerimientos legales – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

Obtener una ventaja comercial – si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

Menores costos – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.[6]

4.2.4. ¿Cómo es realmente ISO 27001:2013?

[5]Qué es norma ISO 27001 Como funciona la ISO 27001 [En línea] <http://www.iso27001standard.com/es/que-es-iso-27001/> [Tomado el 26 de mayo de 2015]

[6]Qué es norma ISO 27001 -Cómo es realmente [En línea] <http://www.iso27001standard.com/es/que-es-iso-27001/> [Tomado el 26 de mayo de 2015]

ISO/IEC 27001:2013 se divide en 14 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – Términos y definiciones – de nuevo, hacen referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Anexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).[7]

4.3. MARCO LEGAL

Una herramienta de la gestión estratégica para la protección de la información es la norma ISO/IEC 27001:2013, que se usa para lograr la certificación de una empresa u organización o ya sea para implementar las buenas prácticas de la seguridad de la información tanto en los aspectos internos como externos de la misma

Cuando se implementa esta norma, consagra un conjunto de dominios con la finalidad de robustecer la seguridad sin que todos estos tengan un impacto jurídico

Por la escasa legislación que existe se toma el enfoque a normas internacionales y nacionales. La norma ISO/IEC 27001:2013 comprende 14 dominios a saber:

- A.5 Políticas de la seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad de los recursos humanos
- A.8 Gestión de activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.15 Relaciones con los proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de la seguridad de la información de la gestión de continuidad del negocio
- A.18 Cumplimiento

[7]Qué es norma ISO 27001<http://www.iso27001standard.com/es/que-es-iso-27001/> [Tomado el 26 de mayo de 2015]

Para la norma ISO 27001 en su comprensión de su finalidad y procedimientos es un requisito fundamental para la contribución desde el derecho al SGSI, desde la cual se puede identificar seis grandes temas desde la perspectiva jurídica a saber:

- Laprotección de datos personales
- La contratación de bienes informáticos y telemáticos
- El derecho laboral y prestación de servicios
- Los servicios de comercio electrónico
- La propiedad intelectual
- El tratamiento de los incidentes informáticos.

Protección de Datos Personales: aunque constitucionalmente, en Latinoamérica, se establece como un derecho fundamental no existe una ley que la regule de forma integral el derecho a la intimidad y al Habeas data. En el dominio A.15.1.4 de la norma ISO/IEC 27001 señala la protección de los datos personales y la privacidad. En consecuencia la organización debe procurar que toda base de datos, tenga connotación comercial o no, cuente con las medidas jurídicas, tecnológicas y físicas que aseguren su protección.

La ausencia de la norma conduce que la gran mayoría de las bases de datos privadas o públicas se exploten de forma ilegal tal vez de forma abusiva, por ignorancia o total desconocimiento de los derechos de los individuos

La ausencia de una norma conduce a que gran parte de las bases de datos en poder de entidades públicas como privadas sean explotadas de manera ilegítima, a partir del abuso, ignorancia o desconocimiento de los derechos que tienen los individuos sobre la información confiada. No se pretende limitar el uso de las bases de datos, sino llamar la atención sobre la posibilidad de explotar la información dentro de unos parámetros legítimos, que atiendan los principios de consentimiento, finalidad, calidad, veracidad, conservación que caracterizan el tratamiento responsable de la información personal.

Contratación de Bienes Informáticos y Servicios Telemáticos: el derecho privado de cada país se fundamenta en la contratación de bienes tangibles los cuales no representan problemas desde la óptica de los servicios informáticos

La norma ISO 27001 en el dominio A.10 y A.12 en cuanto a la gestión de comunicaciones y operaciones, habla de la adquisición, desarrollo y mantenimiento de sistemas de información, ahí las organizaciones tiene el mayor problema porque no se establece todos los aspectos tecnológicos que se requieren para dar cumplimiento al contrato

Políticas Laborales y Prestación de Servicios por Terceros: En el dominio A.8, de la norma ISO/IEC 27001, denominado seguridad de los recursos humanos, que establece los controles antes y después de una contratación laboral. Aquí se advierte a todos los terceros ya sean jurídicos o naturales, como también con todos

sus empleados dotándolos de seguridad con los activos de la seguridad de la organización

Servicios de Comercio Electrónico: en esta norma, el comercio electrónico debe entenderse como la transmisión de información utilizando medio públicos como el internet o redes privadas

El dominio A.10.9 control que garantiza la seguridad del comercio electrónico.

Propiedad Intelectual: como la información es intangible se utiliza la herramienta de protección intelectual para garantizar el desarrollo de esta práctica. El dominio A.15.1.14 de la norma ISO/IEC 27001 establece el cumplimiento de las disposiciones sobre propiedad intelectual en aras de la seguridad de la información

La ley No. 1273 del 05 de enero de 2009 establece: "POR MEDIO DE LA CUAL SE MODIFICA EL CÓDIGO PENAL, SE CREA UN NUEVO BIEN JURÍDICO TUTELADO – DENOMINADO "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS"· Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES".

Esta ley establece dos nuevos capítulos al Código Penal Colombiana: Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y el Capitulo Segundo: De los atentados informáticos y otras infracciones. Es de anotar que esta ley está muy ligada a la norma ISO/IEC 27001 llevando al nuestro país a la vanguardia de la protección de la seguridad de la información y además abriendo más caminos para fortalecer estas buenas practicas

4.4. MARCO CONTEXTUAL

COMPUSERVER es una empresa legalmente constituida con matricula comercial No. 00016916 de la cámara de comercio del piedemonte llanero, con dirección de domicilio en la calle 28 No 16ª-23 del Barrio del Seis de Octubre del municipio de Saravena departamento de Arauca y cuya actividad principal es la comercialización de dispositivos y periféricos computacionales y tecnológico así como la prestación de servicios informáticos y desarrollo e implementación de software.

MISION

Para la organización “COMPUSERSVER” es de vital importancia, poder brindar a los empresarios, comerciantes, estudiantes, familias, maestros, profesionales, técnicos y demás interesadas en estar a la vanguardia de la tecnología, con un servicio eficiente, más un engrandecimiento de alta calidad, proyectando una atención esmerada por parte de nuestros valiosos colaboradores, asesores y empleados, brindando a nuestros clientes respeto, honestidad, y prontitud a lo requerido.

Productos y/o servicios que nos dan la oportunidad de entrar a sus centros de interés, lugares de trabajo u hogares, con calidad, esmero que nuestra empresa posee, distribuye y garantiza, ofreciendo a nuestros clientes el mejor respaldo del mercado con la adecuada asesoría, para alcanzar la satisfacción y calidad total. Nuestra estabilidad es un rendimiento garantizado con el deleite, la confianza de nuestros clientes, el sentido de identidad y responsabilidad de nuestro equipo de trabajo.

VISION

Es el propósito de “COMPUSERVER” ser hacia el año 2020, una empresa de reconocido prestigio nacional, con autonomía administrativa, con excelencia en ventas de computadoras, consumibles, realización de software y soporte, donde se brinde un producto de excelente calidad y en donde el mejoramiento continuo en todas las áreas sean de agrado a nuestros consumidores, de eficiente gestión, competitiva, con alianzas estratégicas en el ámbito nacional e internacional, comprometida con el servicio al cliente, la formación integral de su recurso humano y tecnológico. Y ser un ejemplo para la sociedad a lo que se refiere en buen servicio.

OBJETIVOS DE LA EMPRESA

Desarrollar programas computacionales, con la finalidad y capacidad de resolver situaciones reales a las empresas para su desarrollo, y evolución tecnológico para atender sus necesidades y hacerlas mejores empresas en su campo laboral, financiero, administrativo y económico, además de actualizarlos en el campo computacional.

5. DISEÑO BÁSICO METODOLÓGICO

5.1. TIPO DE ESTUDIO

Por el problema planteado y los objetivos que pretende este proyecto se trata de una puesta en práctica de las bondades que nos ofrece la seguridad informática basados en la norma ISO/IEC 27001:2013 para ser aplicados en la red de datos de COMPUSERVER y convertirla en una red segura para la transmisión de los datos y del servicios de internet.

5.2. POBLACIÓN Y MUESTRA

5.2.1. Población

En el presente proyecto abarca la comunidad de Saravena quien se verá beneficiada con la prestación de un servicio eficiente y seguro dándoles tranquilidad a los usuarios que la utilicen.

5.2.2. Muestra.

Para el estudio de la referencia, no vamos a medir personas sino el proceso o la estructura organizativa de la gestión de los servicios prestados a una comunidad.

5.2.3. Unidad de Observación

Se estructura para el presente trabajo la planeación y la gestión de la seguridad de los datos trasmitidos por la red de datos de COMPUSERVER a los usuarios quien da o aprueban la calidad del servicio que se les preste

Tabla 1 Trabajo de campo

Objetivos Específicos	Actividades

- Realizar diagnóstico de la seguridad actual de la red informática de COMPUSERVER -Hacer un chequeo general de la configuración física y lógica de los puntos de acceso (Ubuiquiti)	Visitas programadas a los actuales clientes para medir la conformidad de la prestación del servicio y la seguridad prestada. Revisar la instalación física de los dispositivos de punto de acceso y estaciones para garantizar las recomendaciones técnicas de cada fabricante.
-Capacitar al personal operativo – Técnico del uso del servidor Zentyal	Programar capacitaciones al personal técnico de la empresa COMPUSERVER

5.2.4. Cronograma de actividades (Gráfico de Gant)

ACTIVIDAD	Mes1				Mes2				Mes3				Mes 4				Mes4			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Apropiarse de la norma ISO/IEC 27001:2013 para estudiarla y aplicarla al problema																				
Hacer estudio del estado real de la red de datos de COMPUSERVER, verificando las vulnerabilidades y amenazas teniendo en cuenta los 14 dominios de la ISO/IEC 27001:2013																				
Aplicar los controles de la norma ISO/IEC 27001:2013 que se van a implementar para la seguridad de la red de datos de COMPUSERVER																				
Diseñar las políticas para la implementación de un Sistema de Seguridad de la Información en la red de datos de COMPUSERVER																				
Capacitación del personal administrativo y Técnico de la empresa de COMPUSERVER para el buen manejo del SGSI																				

6. ACTIVOS DE INFORMACIÓN

6.1. CAPITAL HUMANO

CARGO	*CAN.*	*DESCRIPCION DEL CARGO*
Gerente /Administrador	1	Tiene las funciones de dirigir la empresa y coordinar todos movimientos que en ella se realiza. Se encarga de hacer la contratación y representación legal de la empresa y en la toma de decisiones
secretaria	1	Cuya función es en la atención al público, toma de decisiones funcionales para la empresa. La secretaria se encarga de dar cumplimiento a los contratos de servicios que se halla suscripto por terceros
Técnicos	3	Tienen las funciones de dar soporte técnico a los clientes. Un técnico se encarga del soporte de la red de datos con la cual se presta el servicios de ISP, quien tienen acceso a los puntos de acceso con la limitación de usuarios y contraseñas

6.2. HARDAWARE

CAN	*EQUIPOS*	*CARACTERISITCAS*
1	Computador (Servidor)	Computador Intel Core i5 con disco duro de 1024 GB, memoria de 6 GB, monitor de 21” Samsung LED, unidad de DVD RW, teclado y mouse
1	Impresora Laser	Impresora láser HP 1102W. Impresión a blanco y negro monocromático
1	Impresora a Color	Impresora a color marca Epson L555 con sistema de tinta continua a full Color
3	Computadores (estaciones de Trabajo)	Computador Intel Core i3, con disco duro de 500 GB, memoria de 4 GB, monitor de 18” Samsung LED, unidad de DVD RW, teclado y mouse
1	PicoStation2	Marca Ubiquiti de 1000mW 2.4GHz AP. Incluye una antena omnidireccional de 6dBi. Modos de operacion: Access Point, Access Point WDS, Station, Station WDS.

3	NANOSTATION 5	WIRELESS CPE, OUTDOOR 14DBI DUAL-POL 802.11a. Atheros AR2313 SOC, MIPS 4KC, 180MHz a una frecuencia de 5 GHZ
10	NANOSTATION LOCO 5	NanoStation loco 802.11a 13dbi CPE. WIRELESS CPE, OUTDOOR 13DBI DUAL-POL 802.11a. Memoria: 16MB SDRAM, 4MB Flash

6.3. SOFTWARE

CAN	***LICENCIAS***	***CARACTERISITCAS***
1	SYSPLUS (Licencia Privada)	Software de contabilidad y administrativo con módulos de Contabilidad, Cartera, Nomina, Cuentas por Pagar, Tesorería e inventarios
1	Zentyal (Licencia de Open Source)	Software que se utilizara como Firewall y control de acceso para el servicio de internet

6.4. INFORMACION

CAN	***TIPO***	***CLASIFICACION***	***CARACTERISITCAS***
1	Base De datos de la contabilidad y registro de clientes	privado	Se llevan todos los registros contables y de clientes que es de carácter privado de la empresa de la cual se enviar reportes solo a los entes de control como la DIAN
1	Archivo físico de todos los contratos y pagos de los clientes	privado	Se tiene la relación física de la documentación de clientes y contratos con los mismos
1	Información publicitario	publico	En medios radiales locales, perifoneo, pagina web www.compuserver.com.co, redes sociales como Facebook

7. ANALISIS DE RIESGOS DEL ESTADO ACTUAL DE LA RED DE DATOS DE LA EMPRESA COMPUSERVER

La red de datos de COMPUSERVER está estructurada en una topología física de estrella, donde se encuentra un segmento de red cableada con cable UTP categoría 5C interconectando un Swicth de 8 puertos con dos Routers, uno de ellos conecta la red administrativa de la empresa, tanto alámbrica como inalámbrica, éste a su vez conecta a otro router que da la salida a un punto de acceso inalámbrico de alta cobertura (Máximo dos Kilómetros).

El punto de acceso principal se encuentra en una torre metálica que no cumple en su totalidad con la normativa por no tener la resistencia adecuada para los posibles mantenimientos físicos a los equipos que allí se encuentran. Todos los clientes se les ínstala un equipo receptor de señal (Ubiquiti Nano Loco M5) en forma inalámbrica y desde aquí es donde se presenta vulnerable al no tener una política de seguridad en la trasmisión de los datos estando factible a que un tercero interfiera la comunicación alterando los datos transmitidos

La conexión de los equipos cliente al conectarse inalámbricamente se les deben establecer un sistema de cifrado de los datos de autenticación entre ellos y de igual forma para la información que se transmita entre ellos

Al hacer un análisis de la situación actual de la red de datos de COMPUSERVER aunque no se encuentran estadísticas de vulnerabilidades si es factible tener acceso a la red ya sea por usuarios insiders u ousiders, debido a la falta de políticas de seguridad que no se encuentran establecidas. A los usuarios autenticados como son los empleados y/o clientes que reciben los servicios de internet no están capacitados y restringidos a hacer un buen uso de la información que allí se encuentra

El personal que labora en la empresa no están lo suficientemente capacitados para darle seguridad a la información que tratan, haciéndolos en una vulnerabilidad porque fácilmente la pueden dar a conocer a terceros sin tener la intención de hacerlo

Todo el hardware que cuenta la empresa como computadores, impresoras, escáneres, accesorios inalámbricos para la interconexión de puntos de red y demás herramienta se ve vulnerado al no tener la suficiente política de manejo de activos

Por otra parte por la poca seguridad física y lógica es factible que usuarios externos u outsliders pongan en riesgo la disponibilidad, integridad y confiabilidad de la información que se transmite a través de la red de datos de COMPUSERVER

La red de datos de la empresa COMPUSERVER se basa generalmente en el protocolo TCP/IP para la comunicación entre los diferentes nodos de la misma, por lo tanto está latente a las vulnerabilidades que presenta el modelo OSI en sus diferentes capas. Estas vulnerabilidades se deben a las bajas políticas de seguridad que tiene la red. Los cibernautas u otros usuarios pueden vulnerar la red en los siguientes escenarios:

Desde la capa de aplicación se pueden generar las vulnerabilidades de denegación de servicios DoS, códigos maliciosos entre otros.

- **DNS Spoofing**: falsear una dirección IP y resolverla con el DNS o viceversa
- **Sniffing yEavesdropping:** Como la red de COMPUSERVER, generalmente es inalámbrica, y por falta de seguridad de acceso se puede llevar esta vulnerabilidad si un usuario llega a conectarse a ella y la información que trasmite no está encriptado llegando a tener acceso a la información sensible de la empresa y de los clientes.
- **SMTP Spoofing y Spamming:** El servicio que presta la empresa COMPUSERVER es la prestación de servicio de internet por lo tanto es muy común el uso de envió de correos electrónicos por parte de los clientes y la empresa misma, y aprovechando que el protocolo SMTP (Utilizado para enviar emails) no lleva a cabo ninguna autenticación al hacer conexión TCP al puerto asociado se pueden falsificar e enviar correos falso poniendo en peligro la integridad y confiabilidad de la información
- **DoS (Denegación de Servicio):** En el momento que un usuario tenga acceso a la red se puede presentar este ataque que consiste en saturar el tráfico de la red enviando y recibiendo paquetes entre los diferentes nodos o a uno en particular haciendo colapsar la red. Aun se puede llegar a tener el DDos

  Desde la capa de transporte del modelo OSI las vulnerabilidades se centran en el funcionamiento de los protocolos TCP y UDP, Escaneo de puertos, sobrecarga de conexiones, etc. De los cuales la red puede estar vulnerada por:

- **Fingerprinting:** Como la red de datos de COMPUSERVER se basa en conexiones de equipos con sistemas operativos Windows, tanto el servidor como el de los usuarios y con bajas reglas de seguridad están latentes a tener información detallada de cada máquina y poder ser atacada, especialmente el servidor de control de la empresa de COMPUSERVER
- **Escaneo de Puertos:** El sistema operativo de Windows de forma general se encuentran la mayoría de puertos abierto facilitando el acceso de intrusos. La red de datas de COMPUSERVER no tiene políticas de seguridad de acceso por puertos, dejando puertas abiertas para la vulneración de la red

```
Initiating Parallel DNS resolution of 1 host. at 18:38
Completed Parallel DNS resolution of 1 host. at 18:38, 0.01s elapsed
Initiating SYN Stealth Scan at 18:38
Scanning 4 hosts [65535 ports/host]
Discovered open port 80/tcp on 192.168.10.100
```

- **Connection Flood:** Un atacante puede realizar múltiples conexiones de red falsa o vacías limitar la cantidad necesaria para los clientes que se van a comunicar hasta perder el acceso a la misma o hacer DoS

Desde la capa de red también se pueden hacer vulnerabilidades a una red y en el caso de la red de datos de COMPUSERVER se expondría a:

- **Footprinting**: Mediante esta técnica se puede vulnerar la red debido a la falta de policiacas de seguridad y se pueden revelar datos sensibles para que un atacante tenga acceso y crear sus puertas de entrada
- **Escaneo Basado en el Protocolo ICMP**: Esta red está latente a escaneos como: ICMP Echo, ICMP Broadcast, ICMP Timestamp, ICMP Information, ICMP Address Mask
- IP Spoofing: Se puede falsear direcciones IP para engañar y enviar menajes a traces de máquinas que realmente pertenecen a la red

8. RECOMENDACIÓN DE CONTROLES A APLICAR A LA RED DE DATOS DE COMPUSERVER

Teniendo en cuenta la arquitectura física y lógica de la red de datos de la empresa COMPUSERVER y según el análisis hecho se evidencia que se encuentra en estado vulnerable en un alto porcentaje debido a la falta de políticas de seguridad

Se recomienda implementar un sistema de seguridad de la información SGSI donde se establezcan las política de seguridad básica y las mejoras de acuerdo al presupuesto financiero de la empresa implementando controles de seguridad tanto físicos como lógicos.

9. ANÁLISIS DETALLADO DEL ANEXO A ISO 27001:2013 EN EL NIVEL DE CUMPLIMIENTO DE LA RED DE DATOS DE LA EMPRESA COMPUSERVER

DOMINIO	***OBSERVADO***	***% apli***
A.5 Políticas de la seguridad de la información	Las políticas implementadas son muy mínimas debido al desconocimiento de las posibles vulnerabilidades que existen en las redes informáticas	10
A.6 Organización de la seguridad de la información	No existe una organización ni clasificación de la información de acuerdo algún estándar	5
A.7 Seguridad de los recursos humanos	El personal que labora en la empresa es seleccionada de acuerdo a las funciones que se van a desempeñar, pero falta establecer las responsabilidades de cada uno. Falta establecer la importancia de la seguridad de la información que manejan	30
A.8 Gestión de activos	Los activos están clasificados de acuerdo a la importancia y desempeño de cada uno pero hace falta diseñar mejor las protecciones de cada uno de ellos	40
A.9 Control de acceso	El nivel de acceso se restringe solo a nivel lógico y no cuentan con ningún hardware de protección o firewall, además los controles lógicos son muy básicos. El acceso al tratamiento de la información no está debidamente protegidas	30
A.10 Criptografía	No se cuenta con ningún estándar criptográfico para el envío y recepción de información	3
A.11 Seguridad física y del entorno	Las áreas de procesamiento de información solo están demarcadas pero falta controles para el adecuado procesamiento	15
A.12 Seguridad de las operaciones	Falencia en la seguridad de operaciones por falta estadísticas de eventos y poca capacitación para el manejo de la información	5
A.13 Seguridad de las comunicaciones	No existe algún registro de la transferencia de datos y las conexiones en lapsos de tiempos determinados	

A.14 Adquisición, desarrollo y mantenimiento de sistemas	Se tiene un aceptable plan de mantenimiento tanto preventivo como correctivo de software y hardware. Están estipulados los planes de adquisición según la necedad de hardware teniendo en cuenta el ciclo de vida de cada elemento. No existe algún plan nuevo de desarrollo y actualización	45
A.15 Relaciones con los proveedores	No aplica por que no maneja proveedores	0
A.16 Gestión de incidentes de seguridad de la información	No existe estadística ni registros de incidentes	5
A.17 Aspectos de la seguridad de la información de la gestión de continuidad del negocio	La empresa en su misión y visión prevee los posibles alcances y con el plan de adquisición se denota una continuidad. Falta hacer un mejor plan de mejoramiento de la continuidad	20
A.18 Cumplimiento	Cumple con la normativa como constitución de empresa para prestar el servicio de IPS. Falta documentación acerca de la normativa para el manejo de información por parte de los empleados y personal anexo a la empres	30

10. PLAN DE DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES Y TODOS LOS LINEAMIENTOS DE LA NORMA ISO 27001:2013

DOMINIO	*RECOMENDACIONES*
A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION **A.5.1 Orientación de la dirección para la gestión de la seguridad de la información**	
A.5.1. 1 Políticas para la seguridad de la información	Se debe establecer las políticas de seguridad y ser plasmarlas en el manual de control de la empresa
A.5.1. 2 Revisión de las Políticas para la seguridad información	Establecer una planificación de verificación de las políticas cada seis 6 meses ya que la tecnología avanza continuamente y de esa manera los fraudes
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION **A.6.1 Organización interna**	
A.6.1.1.Roles y responsabilidades para la seguridad de la información	Clasificar los roles de acuerdo a cada actividad o funciones de cada uno de los actores de la empresa y dárselos a conocer en el manual de funciones de los cargos
A.6.1.2 Separación de deberes	Hacer una demarcación de acuerdo a las áreas de trabajo y roles de cada actor dentro o fuera de la empres
A.6.1.3 Contacto con las autoridades	La dirección debe tener un vínculo con las autoridades pertinentes para cada caso. Tener estipulado el contacto inmediato
A.6.1.4 Contacto con grupo de interés social	Incluir un plan para que los trabajadores y administrativos estén vinculados con los grupos de actualización en forma permanente
A.6.1.5 Seguridad de la información en la gestión de proyectos	La gestión de proyecto debe ser por la parte administrativa sin que la parte operativa tenga acceso a esa información. Se debe seguridad para la custodia de los documentos importantes
A.6.2 Dispositivos móviles y teletrabajo	
A.6.2.1 Política para dispositivos móviles	La vinculación de los móviles a la red de datos solo debe gestionarse por parte del encargado de esa área, sin la posibilidad de que vulnere el

	acceso para ello se debe implantar un firewall para la gestión de acceso y registro del mismo
A.6.2.2 Teletrabajo	No aplica para la Empresa ya que no es objetivo de la misma
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS **A.7.1 Antes de asumir el empleo**	
A.7.1.1 Selección	Implementar la política reglamentara para la selección de un empleado haciendo la convocatoria, selección y entrevistas teniendo en cuenta la reglamentación vigente
A.7.1.2 Términos y condiciones del empleo	Los términos de empleo deben estar estipulados en el contrato y sus anexos donde se estipule las responsabilidades dentro y fuera de la empresa con la seguridad de la información
A.7.2 Durante la ejecución del empleo	
A.7.2.1 Responsabilidades de la dirección	En el reglamento interno de la empresa y en las funciones de los cargos, la dirección debe ser la responsable de hacer cumplir los aspectos contractuales de todas las personas que se vinculen a la empres
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	La dirección debe establecer un plan de capacitación y educación en la responsabilidad que cada uno genera al firmar un contrato en cuanto a la seguridad de la información
A.7.2.3 Proceso disciplinario	En el control interno se debe estipular los procesos disciplinarios que se deben llevar a cabo de acuerdo a cada falta.
A.7.3Terminación y cambio de empleo	
A.7.3.1Terminacion o cambio de responsabilidades de empleo	Se deben estipular en el control interno de la empresa, el cual lo debe conocer el trabajador o tercero vinculado en la empres
A.8 GESTION DE ACTIVOS **A.8.1 Responsabilidad por los activos**	
A.8.1.1 Inventario de Activos	Se debe mejorar la clasificación de los inventario en el software que actualmente llevan
A.8.1.2 Propiedad de los activos	Organizar el archivo físico y lógico de los documentos que acreditan la propiedad de los activos de la empresa
A.8.1.3 Uso aceptable de los activos	Los activos instalados en la empresa deben cumplir las condiciones mínimas que la empresa debe estipular y tenerlo documentado

A.8.1.4 Devolución de activos	Los activos son propiedad de la empresa, en el contrato de prestación de servicios de la señal de internet se debe estipular que una vez terminado el contrato se hacen las devoluciones de dispositivos instalados para la prestar el servicio
A.8.2 Clasificación de la información	
A.8.2.1 Clasificación de la información	Diseñar la metodología de registrar la información en el software administrativo contables y con qué prioridad se hace
A.8.2.2 Etiquetado de la información	En el sistema administrativo se debe clasificar la información de acuerdo a la necesidad e implementar más reportes personalizados de acuerdo a la empresa
A.8.2.3 Manejo de activos	Diseñar las planillas de movimientos de los activos y establecer a donde se encuentran, teniendo identificado la función que cumple y el estado actual
A.8.3Manejo de medios	
A.8.3.1 Gestión de medios removibles	Llevar un registro pormenorizado de los medios que se utilicen y aún más cuando son de fácil remoción
A.8.3.2 Disposición de los medios	Diseñar una custodia pertinente de acurdo a la importancia de la información contenida
A.8.3.3Transferencia de medio físicos	El acceso a estos medios solo debe ser de parte administrativa y quienes transportan se debe llevar de forma protegida
A.9CONTROL DE ACCESO **A.9.1 Requisitos del negocio para el control de acceso**	
A.9.1.1 Política de control de acceso	Instalar un firewall como control de acceso a la red de datos
A.9.1.2 Acceso a redes y a servicios de red	El acceso debe ser clasificado de acuerdo al tipo de usuario que la utiliza
A.9.2Gestión de acceso a usuarios	
A.9.2.1 Registro y cancelación del registro de usuarios	Sea gestionado en forma sistematizada
A.9.2.2 Suministro de acceso de usuarios	Sea gestionado en forma sistematizada
A.9.2.3 Gestión de derechos de acceso privilegiado	Sea gestionado en forma sistematizada

A.9.2.4 Gestión de información de autenticación secreta de usuarios	Sea gestionado en forma sistematizada
A.9.2.5 Revisión de los derechos de acceso de usuarios	Sea gestionado en forma sistematizada o por medio de usuarios con derechos de Administrativo
A.9.2.6 Retiro o ajuste de los derechos de acceso	Sea gestionado en forma sistematizada o por medio de usuarios con derechos de Administrativo
A.9.3Responsabilidades de los usuarios	
A.9.3.1 Uso de la información de la autenticación secreta	Diseñar sistemas que lleven el registro de autenticación y la utilización de sistemas de criptográficos
A.9.4Control de acceso a sistemas y aplicaciones	
A.9.4.1 Restricción de acceso a la información	Implementar un firewall lógico con el zentyal que ayuda al acceso
A.9.4.2 Procedimiento de ingreso seguro	Implementar un firewall lógico con el zentyal que ayuda al acceso
A.9.4.3 Sistema de gestión de contraseñas	Implementar un firewall lógico con el zentyal que ayuda a la generación de contraseñas seguras
A.9.4.4 Uso de programas utilitarios privilegiados	No aplica
A.9.4.5 Control de acceso a código fuente de programas	No aplica
A.10CRIPTOGRAFIA **A.10.1 Controles criptográficos**	
A.10.1.1 Políticas sobre uso de controles criptográficos	Encriptar los archivos que se envíen
A.10.1.2 Gestión de llaves	No aplica
A.11 SEGURIDAD FISICA Y DEL ENTORNO **A.11.1 Áreas seguras**	
A.11.1.1 Perímetro de seguridad Física	Mejorar las instalaciones físicas en cuanto a la seguridad de acceso a la empresa
A.11.1.2 Controles de acceso físico	Mejorar las instalaciones físicas en cuanto a la seguridad de acceso a la empresa
A.11.1.3 Seguridad de oficinas, recintos e instalaciones	Mejorar las instalaciones físicas en cuanto a la seguridad de acceso a la empresa. Utilizar medio de seguridad industrial
A.11.1.4 Protección contra amenazas externas y ambientales	Aumentar las medidas de seguridad ambiental y externa

A.11.1.5 Trabajo en áreas seguras	Mejorar la iluminación y seguridad electrónico
A.11.1.6 áreas de despacho y carga	No aplica
A.11.2 Equipos	
A.11.2.1 Ubicación y protección de equipos	Reubicar equipos sensibles a la manipulación no controlada
A.11.2.2 Servicios de suministros	Instalación de un planta eléctrica que se active automáticamente después de una falla eléctrica
A.11.2.3 Seguridad del Cableado	Mejorar el cableado estructurado de la red de datos
A.11.2.4 Mantenimiento de equipos	Diseñar plan de mantenimiento preventivo y correctivo con más prioridad
A.11.2.5 Retiro de activos	Diseñar un control de registros de equipos retirados anexando las causas
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Responsabilizar al cliente del cuidado de los equipos
A.11.2.7 Disposición segura o reposición de equipos	Diseñar el almacenamiento segur de los activos
A.11.2.8 Equipos de usuarios desatendidos	No aplica
A.11.2.9 Política de escritorio limpio y pantalla limpia	Mejorar la metodología del tratamiento de la información
A.12SEGURIDAD DE LAS OPERACIONES **A.12.1 Procedimientos operacionales y responsabilidades**	
A.12.1.1 Procedimientos de operación documentados	Diseñar políticas pertinentes
A.12.1.2 Gestión de cambios	Diseñar plan de choque para los cambio que realice la empresa
A.12.1.3 Gestión de capacidad	Implementar un sistemas lógico de balanceo de cargas para la prestación del servicio
A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	Mejorar el aislamiento de las áreas haciéndoles sus respectivas marcas
A.12.2 Protección contra código malicioso	
A.12.2.1 Controles contra códigos	Implementar software de antivirus y antisapam para el control de acceso de programas peligrosos
A.12.3 Copias de respaldo	

A.12.3.1 Respaldo de la información	Mejorar la cálida de medio para almacenar las copias de seguridad
A.12.4 Registros y seguimientos	
A.12.4.1 Registro de eventos	Diseñar un sistema automatizado para tal fin
A.12.4.2 Protección de la información de registro	Diseñar un sistema automatizado para tal fin
A.12.4.3 Registros del operador y del administrador	Diseñar un sistema automatizado para tal fin
A.12.4.4 Sincronización de relojes	Diseñar un sistema automatizado para tal fin
A.12.5 Control de software operacional	
A.12.5.1 Instalación de software en sistemas operativos	Mejorar la política de instalación de software
A.12.6 Gestión de la vulnerabilidad técnica	
A.12.6.1 Gestión de las vulnerabilidades técnicas	Diseñar una política de registros de vulnerabilidades técnicas y las posibles soluciones debidamente documentada
A.12.6.2 Restricciones sobre las instalaciones de software	Deshabilitar la instalación de software por parte de usuario o programas que lo hagan en segundo plano. La instalación solo debe hacerse por el personal autorizado
A.12.7 Consideraciones sobre las auditorias de sistemas de información	
A.12.7.1 Controles de auditorías de sistemas de información	Diseñar un plan de auditorías periódicas en lapsos de tiempo no mayor a un año
A.13SEGURIDAD DE LAS COMUNICACIONES **A.13.1 Gestión de la seguridad de las redes**	
A.13.1.1 Controles de redes	Diseñar las estrategias para el acceso a la red, la cual se debe monitorizar constantemente tanto automatizado como manualmente para verificar el acceso de usuarios autorizados
A.13.1.2 Seguridad de los servicios de red	Automatizar para el acceso a la red según los derechos y accesos permitidos y control de pagos y vencimientos
A.13.1.3 Separación en las redes	Se recomienda independizar las redes en VLAN de acuerdo al acceso sea internamente o externamente
A.13.2 Transferencia de información	

A.13.2.1 Políticas y procedimientos de transferencia de información	Implementar políticas criptográficas para la comunicación y transporte de datos
A.13.2.2 Acuerdo sobre la transferencia de información	Implementar políticas criptográficas para la comunicación y transporte de datos
A.13.2.3 Mensajería electrónica	Implementar políticas criptográficas para la comunicación y transporte de datos
A.13.2.4 Acuerdos de confidencialidad o de no divulgación	Diseñar las políticas y responsabilidades para la confiablidad de la información
A.14ADQUISION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS **A.14.1 Requisitos de seguridad de los sistemas de información**	
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Diseñar los requerimientos de la empresa para la implementación de cualquier sistema de información
A.14.1.2 Seguridad de servicios de las aplicaciones en redes publicas	Establecer las políticas para la conexión de clientes a quienes se les brinda el servicio
A.14.1.3 Protección de las transacciones de los servicios de las aplicaciones	No aplica
A.14.2 Seguridad en los procesos de desarrollo y soporte	
A.14.2.1 Políticas de desarrollo seguro	No aplica
A.14.2.2 Procedimientos de control de cambios en sistemas	No aplica
A.14.2.3 Revisión técnica de las aplicaciones después de cambio en la plataforma de operación	No aplica
A.14.2.4 Restricciones en los cambios a los paquetes de software	No aplica
A.14.2.5 Principios de la construcción de sistemas seguros	No aplica
A.14.2.6 Ambiente de desarrollo seguro	No aplica

A.14.2.7 Desarrollo contratado externamente	No aplica
A.14.2.8 Pruebas de seguridad de sistemas	No aplica
A.14.2.9 Pruebas de aceptación de sistemas	No aplica
A.14.3 Datos de prueba	
A.14.3.1 Protección de datos de prueba	Diseñar las políticas debidamente documentada para el control de la información utilizada para pruebas.
A.15 RELACIONES CON LOS PROVEEDORES **A.15.1 Seguridad de la información en las relaciones con los proveedores**	
A.15.1.1 Políticas de seguridad de la información para las operaciones con los proveedores	No aplica
A.15.1.2 tratamiento de la seguridad dentro de los acuerdos con los proveedores	No aplica
A.15.1.3 Cadena de suministro de tecnología de información y comunicación	No aplica
A.15.2 Gestión de la prestación de servicios de proveedores	
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	No aplica
A.15.2.2 Gestión de cambios en los servicios de los proveedores	No aplica
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION **A.16.1 Gestión de incidentes y mejoras en la seguridad de la información**	
A.16.1.1.Responsabilidades y procedimientos	Diseñar y documentar los roles de cada área y actores que interviene dándoles a conocer el contenido sobre las responsabilidades de la información
A.16.1.2 Reporte de eventos de seguridad de la información	Llevar un consolidado de registros de los eventos sobre la seguridad de la información. Custodiarla en forma segura para utilizarla posteriormente
A.16.1.3 Reporte de debilidades de seguridad de la información	Diseñar un bitácora de debilidades de la red de datos y registrando las posibles soluciones para prevenirlas posteriormente

A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Tabular los registros de los eventos de la seguridad de la información con respecto al red de datos y priorizar los más débiles
A.16.1.5 Respuesta a incidentes de la seguridad de la información	Si se tiene tabulados los registros de la vulnerabilidades existentes y sus posibles soluciones es más rápido dar respuesta pronta y positiva
A.16.1.6 Aprendizaje obtenido de los incidentes de la seguridad de la información	Registrar las soluciones de las vulnerabilidades existentes para cerrar la brecha a la inseguridad de la información
A.16.1.7 Recolección de evidencias	Tener las evidencias tantos físicas como lógicas de las vulnerabilidades y soluciones
A.17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO **A.17.1 Continuidad de seguridad de la información**	
A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se debe estar actualizando con las mejores prácticas de seguridad
A.17.1.2 implementación de la continuidad de la seguridad de la información	LA implementación del SGSI no es solo implementarla y dejarlo así. Se debe estar actualizando y mejorando los SGSI
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Hacer una evaluación periódica de la continuidad de la seguridad de la información y mejorar donde se esté fallando. Dejarlo totalmente documentado
A.17.2 Redundancias	
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	Implementar plan de contingencia de cada equipo por si alguno falla dándole prioridad a los más importantes
A.18 CUMPLIMIENTO **A.18.1 Cumplimiento de requisitos legales y contractuales**	
A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Tener en la empresa las legislaciones vigentes que regulen el manejo de la información segura
A.18.1.2 Derechos de propiedad intelectual	Hacer énfasis de la propiedad intelectual, adquiriendo las licencias pertinentes
A.18.1.3 Protección de registros	Diseñar la implementación de custodia segura de los registros tanto para el proceso, el traslado y manipulación de los mismos

A.18.1.4 Privacidad y protección de información de datos personales	Diseñar políticas que garanticen a sus clientes y personal de la empresa la privacidad de los datos personales de acuerdo a la ley colombiana
A.18.1.5 Reglamentación de controles criptográficos	Los controles de criptografía se deben reglamentar para cumplir con la normatividad vigente
A.18.2 Revisiones de seguridad de la información	
A.18.2.1 Revisión independiente de la seguridad de la información	Contratar revisiones externas para verificar la seguridad de la información del empresa y clientes
A.18.2.2 Cumplimiento con las políticas y normas de seguridad	Cumplir con la seguridad de montaje y manipulación de activos de la empresa
A.18.2.3 Revisión del cumplimiento técnico	Revisiones periódicas del cumplimiento técnico y dejarlo documentado

11. ESTRATEGIAS DE CAPACITACION AL PERSONAL EN EL SGSI DE LA EMPRESA COMPUSERVER

Para la capacitación del personal de activo de la empresa COMPUSERVER se diseñaron las siguientes estrategias para ser desarrolladas en la implementación del SGSI, con el fin de hacer un seguimiento al desarrollo de la implementación

- Hacer capacitaciones sucesivas en un salón de conferencias que se alquilara para tal fin donde se den a conocer la importancia de la seguridad de la información y la responsabilidad que cada persona tiene al manipular o procesar información.
- Hacer el manual de funciones y responsabilidades y hacerles entrega de una copia impresa a cas actor de la empresa según sus cargos
- Colocar videos en forma constantes y periódica en las instalaciones de la empresa con el fin que el personal se apropie de los objetivos de la implementación del SGSI
- Hacer coevaluaciones y autoevaluaciones del desarrollo del SGSI
- Mantener en lun ligar visible y accesible las políticas mínimas que debe cumplir todos los actores de la empresa

CONCLUSIONES

- La Norma ISO/IEC 27001:2013 nos es de gran importancia para diseñar un buen Sistema de Gestión Seguridad de la información SGSI para cualquier empresa

- Empresas como COMPUSERVER se ven afectado por la vulnerabilidades y amenazas que están expuestas por falta de implementar un SGSI

- Las políticas de seguridad que se implementen en cualquier empresa se deben ajustar al estándar ISO/IEC 27001:2013

- En la implementación del SGSI se debe involucrar al personal de la empresa dándoles las respectiva capacitaciones

BIBLIOGRAFÍA

Conceptos básicos. Internet: (http://www.iso27000.es/sgsi.html)

Norma ISO 27000. Internet (http://www.iso27000.es/download/doc_iso27000_all.pdf)

RAMIREZ Villegas, G & Constain Moreno, G. (2014). Modelos Y Estándares De Seguridad Informática. CEAD PALMIRA. UNAD

Seguridad en redes inalámbricas. Internet (http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml)

ZAVALA, s (2012) Guía a la redacción en el estilo APA, 6ta edición

ANEXOS A

LISTA DE DOMINIOS CON SUS RESPECTIVOS CONTROLES DE LA NORAMA ISO/IEC 27001:2013

A.5 POLITICAS DE LA SEGURIDAD DE LA INFORMACION
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información
A.5.1. 1 Políticas para la seguridad de la información
A.5.1. 2 Revisión de las Políticas para la seguridad información
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION
A.6.1 Organización interna
A.6.1.1.Roles y responsabilidades para la seguridad de la información
A.6.1.2 Separación de deberes
A.6.1.3 Contacto con las autoridades
A.6.1.4 Contacto con grupo de interés social
A.6.1.5 Seguridad de la información en la gestión de proyectos
A.6.2 Dispositivos móviles y teletrabajo
A.6.2.1 Política para dispositivos móviles
A.6.2.2 Teletrabajo
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS
A.7.1 Antes de asumir el empleo
A.7.1.1 Selección
A.7.1.2 Términos y condiciones del empleo
A.7.2 Durante la ejecución del empleo
A.7.2.1 Responsabilidades de la dirección
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información
A.7.2.3 Proceso disciplinario
A.7.3Terminación y cambio de empleo
A.7.3.1Terminacion o cambio de responsabilidades de empleo
A.8 GESTION DE ACTIVOS
A.8.1 Responsabilidad por los activos
A.8.1.1 Inventario de Activos
A.8.1.2 Propiedad de los activos

A.8.1.3 Uso aceptable de los activos
A.8.1.4 Devolución de activos
A.8.2 Clasificación de la información
A.8.2.1 Clasificación de la información
A.8.2.2 Etiquetado de la información
A.8.2.3 Manejo de activos
A.8.3 Manejo de medios
A.8.3.1 Gestión de medios removibles
A.8.3.2 Disposición de los medios
A.8.3.3Transferencia de medio físicos
A.9 CONTROL DE ACCESO
A.9.1 Requisitos del negocio para el control de acceso
A.9.1.1 Política de control de acceso
A.9.1.2 Acceso a redes y a servicios de red
A.9.2 Gestión de acceso a usuarios
A.9.2.1 Registro y cancelación del registro de usuarios
A.9.2.2 Suministro de acceso de usuarios
A.9.2.3 Gestión de derechos de acceso privilegiado
A.9.2.4 Gestión de información de autenticación secreta de usuarios
A.9.2.5 Revisión de los derechos de acceso de usuarios
A.9.2.6 Retiro o ajuste de los derechos de acceso
A.9.3 Responsabilidades de los usuarios
A.9.3.1 Uso de la información de la autenticación secreta
A.9.4 Control de acceso a sistemas y aplicaciones
A.9.4.1 Restricción de acceso a la información
A.9.4.2 Procedimiento de ingreso seguro
A.9.4.3 Sistema de gestión de contraseñas
A.9.4.4 Uso de programas utilitarios privilegiados
A.9.4.5 Control de acceso a código fuente de programas
A.10 CRIPTOGRAFIA
A.10.1 Controles criptográficos
A.10.1.1 Políticas sobre uso de controles criptográficos
A.10.1.2 Gestión de llaves
A.11 SEGURIDAD FISICA Y DEL ENTORNO
A.11.1 Áreas seguras
A.11.1.1 Perímetro de seguridad Física
A.11.1.2 Controles de acceso físico

A.11.1.3 Seguridad de oficinas, recintos e instalaciones
A.11.1.4 Protección contra amenazas externas y ambientales
A.11.1.5 Trabajo en áreas seguras
A.11.1.6 áreas de despacho y carga
A.11.2 Equipos
A.11.2.1 Ubicación y protección de equipos
A.11.2.2 Servicios de suministros
A.11.2.3 Seguridad del Cableado
A.11.2.4 Mantenimiento de equipos
A.11.2.5 Retiro de activos
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones
A.11.2.7 Disposición segura o reposición de equipos
A.11.2.8 Equipos de usuarios desatendidos
A.11.2.9 Política de escritorio limpio y pantalla limpia
A.12 SEGURIDAD DE LAS OPERACIONES
A.12.1 Procedimientos operacionales y responsabilidades
A.12.1.1 Procedimientos de operación documentados
A.12.1.2 Gestión de cambios
A.12.1.3 Gestión de capacidad
A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación
A.12.2 Protección contra código malicioso
A.12.2.1 Controles contra códigos
A.12.3 Copias de respaldo
A.12.3.1 Respaldo de la información
A.12.4 Registros y seguimientos
A.12.4.1 Registro de eventos
A.12.4.2 Protección de la información de registro
A.12.4.3 Registros del operador y del administrador
A.12.4.4 Sincronización de relojes
A.12.5 Control de software operacional
A.12.5.1 Instalación de software en sistemas operativos
A.12.6 Gestión de la vulnerabilidad técnica
A.12.6.1 Gestión de las vulnerabilidades técnicas
A.12.6.2 Restricciones sobre las instalaciones de software
A.12.7 Consideraciones sobre las auditorias de sistemas de información
A.12.7.1 Controles de auditorías de sistemas de información
A.13 SEGURIDAD DE LAS COMUNICACIONES
A.13.1 Gestión de la seguridad de las redes

A.13.1.1 Controles de redes
A.13.1.2 Seguridad de los servicios de red
A.13.1.3 Separación en las redes
A.13.2 Transferencia de información
A.13.2.1 Políticas y procedimientos de transferencia de información
A.13.2.2 Acuerdo sobre la transferencia de información
A.13.2.3 Mensajería electrónica
A.13.2.4 Acuerdos de confidencialidad o de no divulgación
A.14 ADQUISION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
A.14.1 Requisitos de seguridad de los sistemas de información
A.14.1.1 Análisis y especificación de requisitos de seguridad de la información
A.14.1.2 Seguridad de servicios de las aplicaciones en redes publicas
A.14.1.3 Protección de las transacciones de los servicios de las aplicaciones
A.14.2 Seguridad en los procesos de desarrollo y soporte
A.14.2.1 Políticas de desarrollo seguro
A.14.2.2 Procedimientos de control de cambios en sistemas
A.14.2.3 Revisión técnica de las aplicaciones después de cambio en la plataforma de operación
A.14.2.4 Restricciones en los cambios a los paquetes de software
A.14.2.5 Principios de la construcción de sistemas seguros
A.14.2.6 Ambiente de desarrollo seguro
A.14.2.7 Desarrollo contratado externamente
A.14.2.8 Pruebas de seguridad de sistemas
A.14.2.9 Pruebas de aceptación de sistemas
A.14.3 Datos de prueba
A.14.3.1 Protección de datos de prueba
A.15 RELACIONES CON LOS PROVEEDORES
A.15.1 Seguridad de la información en las relaciones con los proveedores
A.15.1.1 Políticas de seguridad de la información para las operaciones con los proveedores
A.15.1.2 tratamiento de la seguridad dentro de los acuerdos con los proveedores
A.15.1.3 Cadena de suministro de tecnología de información y comunicación
A.15.2 Gestión de la prestación de servicios de proveedores
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores
A.15.2.2 Gestión de cambios en los servicios de los proveedores
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información

A.16.1.1.Responsabilidades y procedimientos
A.16.1.2 Reporte de eventos de seguridad de la información
A.16.1.3 Reporte de debilidades de seguridad de la información
A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos
A.16.1.5 Respuesta a incidentes de la seguridad de la información
A.16.1.6 Aprendizaje obtenido de los incidentes de la seguridad de la información
A.16.1.7 Recolección de evidencias
A.17 ASPECTOS DE LA SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DEL NEGOCIO
A.17.1 Continuidad de seguridad de la información
A.17.1.1 Planificación de la continuidad de la seguridad de la información
A.17.1.2 implementación de la continuidad de la seguridad de la información
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
A.17.2 Redundancias
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información
A.18 CUMPLIMIENTO
A.18.1 Cumplimiento de requisitos legales y contractuales
A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
A.18.1.2 Derechos de propiedad intelectual
A.18.1.3 Protección de registros
A.18.1.4 Privacidad y protección de información de datos personales
A.18.1.5 Reglamentación de controles criptográficos
A.18.2 Revisiones de seguridad de la información
A.18.2.1 Revisión independiente de la seguridad de la información
A.18.2.2 Cumplimiento con las políticas y normas de seguridad
A.18.2.3 Revisión del cumplimiento técnico