ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Sistemas de Información Gerencial

"SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA CERTIFICABLE ISO 27001:2005 PARA UNA EMPRESA PROVEEDORA DE SERVICIOS DE TELECOMUNICACIONES E INTERNET"

TESIS DE GRADO

Previo a la obtención del Título de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Presentada por:

JOFFRE RAMIRO PESÁNTEZ VERDEZOTO

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

A los Ingenieros Lenin Freire y Albert Espinal por contar con su motivación y conocimientos que han sido de gran apoyo en la realización de este trabajo y por su invaluable ayuda.

DEDICATORIA

A Dios por guiar mi camino. A mis padres Sra. Ofelita Verdezoto de Pesántez y Sr. Marco Pesántez por su apoyo incondicional y sus enseñanzas. A mi hermano Lenin Pesántez por su soporte invaluable. A mi esposa Adriana Collaguazo de Pesántez por ser una excelente compañera de vida y siempre brindarme su ayuda.

TRIBUNAL DE GRADUACIÓN

_____

Ing. Lenin Freire C.

DIRECTOR DE TESIS

_____

Ing. Albert Espinal S.

VOCAL PRINCIPAL

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL”

(Reglamento de Graduación de la ESPOL).

_____

Ing. Joffre Ramiro Pesántez Verdezoto

RESUMEN

El presente trabajo tiene como objetivo presentar el desarrollo de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2005 para una empresa proveedora de servicios de Telecomunicaciones e Internet.

En el primer capítulo se muestra la situación actual de este proveedor, su estructura departamental, los productos ofrecidos, infraestructura además de una revisión preliminar de la familia de estándares ISO 27000.

En el segundo capítulo se detalla el levantamiento de los activos de este proveedor, la valoración de los mismos, y el análisis de riesgos con la participación activa de los dueños de los activos.

En el tercer capítulo se presenta la selección y justificación de los controles, y la aceptación y el traspaso del riesgo con la participación de la alta gerencia en el proceso de toma de decisiones.

El cuarto capítulo revisa el proceso de auditoría, se presenta el manual de seguridad y la documentación complementaria del sistema de gestión de seguridad de la información.

ÍNDICE GENERAL

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

AUDITORÍAS INTERNAS, MONITOREO, MEJORA CONTINUA Y CERTIFICACIÓN

ABREVIATURAS Y SIMBOLOGÍA

ACL	Access Control List
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
CPE	Customer Premise Equipment
CRM	Customer Relationship Management
DDoS	Distributed Denial of Service Attack
DNS	Domain Name Service
E1	Trama de portadora E con una ancho de banda de 2048 kbps
EBGP	External Border Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
GRE	Generic Routing Encapsulation
GAN	Gerencia de Area Nacional
GTN	Gerencia Técnica Nacional
SGTN	Subgerencia Técnica Nacional
GTR	Gerencia Técnica Regional
GG	Gerencia General
INS SEC	Instructivo de Seguridad
IP	Internet Protocol
IPSec	Internet Protocol Security

ISO	International Organization for Standarization
ISP	Internet Service Provider
Kbps	Kilo bits por segundo
LAN	Local Area Network
MPLS	Multi Protocol Label Switching
NAP	Network Access Point
NOC	Network Operation Center
OTDR	Optical Time Domain Reflectometer
PBX	Private Branch Exchange
PDCA	Modelo de gestión: Planear, Desarrollar, Chequear, Actuar
POL SEC	Política de Seguridad
POP3	Post Office Protocol
RIP	Routing Information Protocol
SAN	Storage Area Network
SGSI	Sistema de Gestión de Seguridad de la Información
SLA	Service Level Agreement
SMOP	Service Method of Procedure
SMTP	Simple Mail Tranfer Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACs	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol

TDMoIP	Time Division Multiplexing over Internet Protocol
TGS	Telefonica Global Solutions
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USA	United States of America
VIC	Very Importan Customer
VPN	Virtual Private Network
WAN	Wide Area Network

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

La existencia de múltiples actores en el mercado de transmisión de datos y servicios de Internet motivan a este proveedor de servicios a buscar un mecanismo que lo diferencien de sus competidores y a la vez que permita que su flujo de efectivo, específicamente sus ingresos, tengan una mayor estabilidad, lo que le permitirá a este proveedor tomar decisiones y emprender nuevos proyectos en una escenario interno favorable.

Adicionalmente los constantes cambios en las regulaciones externas respecto a la seguridad de la información manejada por sus clientes corporativos motivan a este proveedor a buscar una herramienta para poder brindar a sus clientes soluciones de conectividad que consideren estos aspectos.

La experiencia previa de este proveedor con la implementación y mantenimiento de un sistema de gestión de la calidad basada en la norma ISO 9001 facilitan a este proveedor adoptar un nuevo sistema de gestión, esta vez enfocado en la seguridad de la información.

El sistema de gestión de seguridad de la información basada en la norma ISO 27001:2005 es seleccionada como la herramienta para alcanzar las metas corporativas arriba indicadas.

A través de una metodología inductiva basada en la información y procesos ya existentes, específicamente aprovisionamiento de software y hardware, control de cambios y mantenimiento, se realiza el levantamiento de los activos, la valoración de los mismos y con la colaboración de los dueños de los activos, se realiza en análisis de riesgos. Con el estándar ISO 27002 se escogen los controles a ser implementados, los cuales están alineados con los procesos a ser certificados y con el giro del negocio de este proveedor.

La creación de un departamento dentro de la organización encargado para liderar la implementación del sistema de gestión y la colaboración de las jefaturas de los otros departamentos se conforman como un elemento catalizador para implementar los controles, la implantación del manual de seguridad, políticas generales y procedimientos específicos.

CAPÍTULO 1

CONSIDERACIONES GENERALES DE LA EMPRESA Y ASPECTOS GENERALES DEL ESTÁNDAR INTERNACIONAL ISO 27001:2005

En este capítulo se presenta la situación actual de la empresa, como está formada a nivel de su recurso humano y de su infraestructura, los servicios que presta y el mercado que atiende. Se presenta de manera general los estándares ISO de la familia 27000, enfocándose principalmente en la norma certificable 27001.

1.1 Antecedentes

Desde 1999 esta empresa ha venido desarrollando sus operaciones inicialmente de acceso a Internet para empresas pequeñas y medianas, y luego de transmisión de datos. Para esto, el proveedor montó infraestructura de red metropolitana en Guayaquil, Quito, Manta, Portoviejo y Cuenca. Actualmente ha replicado esta infraestructura en Santo Domingo, Machala, Quevedo, e Isla Isabela.

1.2 Infraestructura del Proveedor

Cada red metropolitana está conformada de un número N de nodos, los cuales están conectados formando un anillo principal. Los nodos que conforman el anillo principal puede a su vez formar un árbol con ellos como raíz. Estos nodos son switches Ethernet de 48 puertos con interfaces GigabitEthernet para los enlaces troncales que conforman el anillo principal.

Se usa fibra óptica para el cableado de última milla desde el nodo más cercano hasta las instalaciones del cliente, donde el proveedor coloca un router con interfaces Ethernet como CPE. Este CPE es de propiedad y administración del proveedor. Debido a que los puertos tanto del nodo como del CPE son Fast Ethernet eléctricos, es necesario usar convertidores ópticos a eléctricos, llamados media converters, para conectarse al cableado de fibra óptica.

A nivel de direccionamiento IP, todos los equipos que están en las instalaciones del cliente poseen direcciones en su tarjeta WAN y en su tarjeta LAN. Las direcciones WAN son asignadas por el proveedor y tienen como puerta de enlace un clúster de routers que sirve a todos los CPE's de la red metro. Este clúster está formado por dos routers, trabajando en modo activo-activo, de tal manera que la mitad del tráfico de los clientes es servido por el router principal y la otra mitad es servida por el router de respaldo.

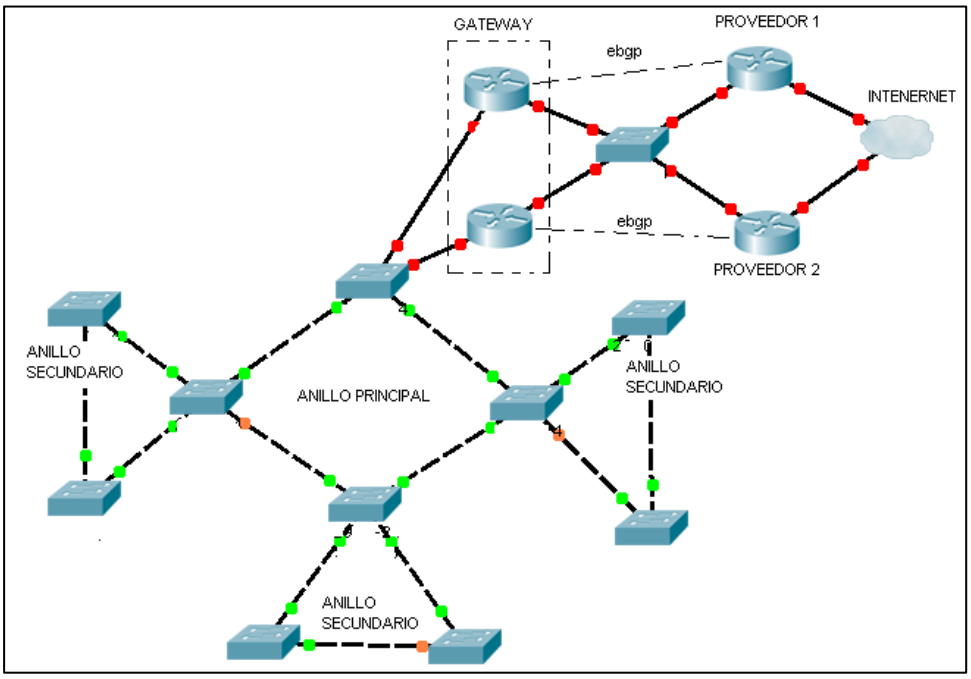


Figura 1.1 Esquema de la Infraestructura del Proveedor

Adicionalmente, el esquema de infraestructura del proveedor muestra la interconexión con los proveedores de Internet internacionales como Sprint, TGS y Telia Sonera. Para esto, se tiene un conjunto de routers de borde, es decir que están fuera del anillo de la red metropolitana, que levantan sesiones del protocolo de enrutamiento EBGP contra los routers de los proveedores internacionales. EBGP es el estándar de facto para el enrutamiento entre proveedores de Internet. Los routers de los proveedores internacionales se encuentran en el NAP de las Américas ubicado

en la ciudad de Miami, USA, por lo que es necesario que este proveedor arriende el transporte de tráfico desde Ecuador hasta USA. Este transporte es provisto por TGS.

1.2.1 Cartera de Servicios

Sobre la infraestructura descrita en la sección anterior, este proveedor ofrece los siguientes servicios:

- Acceso a Internet dedicado 1:1 simétrico
- Transmisión de datos modalidad L3 MPLS, enlace urbano
- Transmisión de datos modalidad L3 MPLS, enlace interurbano
- Transmisión de datos modalidad L3 MPLS, enlace nacional
- Transmisión de datos modalidad TDP sobre IP, enlace urbano
- Transmisión de datos modalidad TDP sobre IP, enlace interurbano
- Transmisión de datos modalidad TDP sobre IP, enlace nacional
- PBX IP administrable
- Virtual Data Center

La mayoría de los ingresos provienen de los servicios de transmisión de datos en todas sus formas, estando en segundo lugar pero no menos importante los ingresos por el servicio de Internet dedicado.

Desglosando un poco los servicios, se observa que este proveedor vende servicio de Internet enfocado al segmento de mercado de ISP’s, medianas empresas y pequeñas empresas, por tal motivo el servicio no tiene ninguna compresión y de forma simétrica, es decir si el cliente compra 1024 Kbps de acceso a Internet, el cliente recibe 1024 kbps de subida y bajada, y la tasa de 1024 kbps es constante, nunca se comparte con otros clientes, a diferencia de proveedores que brindan acceso a Internet a zonas residenciales.

El servicio de transmisión de datos tanto urbano, interurbano como nacional es brindado a la tasa de transferencia que necesite el cliente, gracias a que el medio físico de transmisión es fibra óptica y las interfaces de los routers que se colocan en las instalaciones del cliente son Fast Ethernet,

pudiendo vender enlaces de hasta 100 Mbps aproximadamente. A nivel lógico los mecanismos usados son TDMoIP y L3 MPLS.

Sobre TDMoIP se puede transportar canales de voz E1s canalizados desde la Matriz del cliente hasta sus sucursales en paquetes IP.

Respecto a L3 MPLS, es un mecanismo lógico de transmisión que elimina el overhead de túneles GRE o IPSec, ya que los routers del cliente tienen configuradas sesiones de protocolos de enrutamiento como RIP, EIGRP, BGP, directamente con los routers principales de la infraestructura del proveedor, lo que elimina la necesidad de túneles. Para clientes que necesitan mantener enlaces sincrónicos punto a punto, este proveedor brinda servicios de transmisión de datos urbanos, interurbanos, y nacionales utilizando el mecanismo TDMoIP reenviando las tramas sincrónicas sobre túneles UDP como se indicó anteriormente.

Adicionalmente este proveedor brinda los servicios de PBX IP administrable que libera al cliente de la necesidad de tener una PBX IP dentro de sus instalaciones, sino que a través de un enlace urbano, interurbano ó nacional, se puede conectar a la PBX centralizada de este proveedor, donde se genera una instancia de PBX virtual para el cliente, sobre la cual se pueden crear el plan de marcado telefónico, definir las extensiones y restricciones de llamadas entrantes y salientes.

Finalmente, para empresas pequeñas las cuales como estrategia de reducción de costos prefieren alquilar servicios de procesamiento computacional, este proveedor brinda el servicio de Virtual Data Center, el cual permite al cliente pagar una mensualidad por el uso de una instancia de procesador y memoria dentro de un Blade Server de este servidor, sobre esta instancia, el cliente puede levantar cualquier sistema operativo e implementar su sistema el cual puede ser utilizado por los usuarios del cliente a través de la red del proveedor.

El servicio de Virtual Data Center también está enfocado a aquellas empresas grandes y medianas que necesitan implementar un centro de cómputo alterno para cumplir con requerimientos de continuidad del negocio.

1.2.2 Cartera de clientes

Este proveedor clasifica a sus clientes, de acuerdo a la actividad de los mismos en:

- Clientes Corporativos
- Clientes ISP’s

Adicionalmente este proveedor clasifica a sus clientes de acuerdo a la importancia de los mismos: nivel de facturación, imagen que tienen en el mercado, complejidad en el monitoreo y soporte. Según estos parámetros los clientes son clasificados en:

- Cliente VIC (Very important Customer)
- Cliente C (Customer)

Sin embargo en el contrato de todos los clientes se define el SLA (Service Level Agreement), es decir el Nivel de Servicio Acordado, el cual indica la disponibilidad del servicio que debe garantizar el proveedor. El SLA mensual para los servicios de acceso a Internet Corporativo es de 99.6 %, lo que se traduce en que la duración de una disrupción del servicio no puede superar los 4 horas.

El contrato también define el monto de las penalizaciones en caso de que el proveedor no logre cumplir en la disponibilidad acordada en el contrato.

1.2.3 Organigrama y procesos del Proveedor

El proveedor está organizado por dos Agencias Principales: Guayaquil y Quito, y cada una de estas agencias tiene sus respectivas sucursales.

La agencia Principal Guayaquil tiene jurisdicción sobre las sucursales de Salinas, Machala, Quevedo y Galápagos. La agencia Principal de Quito tiene jurisdicción sobre las sucursales de Santo Domingo, Ambato, Riobamba, y Esmeraldas.

A nivel de administración, este proveedor cuenta con dos tipos de Gerencias: Gerencias de Área Nacional con jurisdicción sobre toda la empresa y Jefaturas Locales con jurisdicción sobre la sucursal respectiva.

Gerencias de Área Nacional.- Se tienen las siguientes:

- Gerencia General
- Gerencia Técnica
- Gerencia Comercial y Ventas
- Gerencia de Procedimientos y Operaciones
- Gerencia de Sistemas de Información y Desarrollo

- Gerencia de Seguridad de Información
- Gerencia de Interconexión de Redes de Datos
- Gerencia de Infraestructura de Fibra óptica
- Gerencia de Infraestructura de Radio Enlaces
- Gerencia de Interconexión de Redes Ópticas
- Gerencia de Telefonía
- Gerencia de Centro de Datos
- Gerencia de Soporte Técnico a Instituciones Financieras y Bancos
- Gerencia de Interconexión Eléctrica
- Gerencia de Contabilidad y Finanzas
- Gerencia de Compras Internacionales

Jefaturas Locales.- Se listan las jefaturas de este proveedor:

- Jefatura Local de Administración
- Jefatura Local de Soporte Técnico Corporativo
- Jefatura Local del Centro de Operaciones de Red (NOC)
- Jefatura Local de Contabilidad y Finanzas
- Jefatura Local de Planificación de Instalaciones y Logística
- Jefatura Local de Recursos Humanos

- Jefatura de Aprovisionamiento de Hardware y Almacenamiento
- Jefatura de Asuntos Legales
- Jefatura de Cobranzas

Departamentos.- En base a las gerencias y jefaturas expuestas, se presenta la organización departamental siguiente:

- Departamento de Soporte Técnico Corporativo
- Departamento de Soporte Técnico a Instituciones Financieras y Bancarias
- Departamento de Operación y Monitoreo de Redes.
- Departamento de Instalaciones, Logística y Comunicación con el cliente.
- Departamento de Sistemas de Información y Desarrollo
- Departamento de Contabilidad y Finanzas
- Departamento Seguridad de Información
- Departamento de Interconexión de Redes
- Departamento de Telefonía
- Departamento de Recursos Humanos

- Departamento de Aprovisionamiento y Almacenamiento de Hardware
- Departamento de Compras Internacionales
- Departamento de Asuntos Legales
- Departamento de Fibra Óptica
- Departamento de Radio Enlaces
- Departamento de Interconexión de Redes Ópticas
- Departamento Comercial y Ventas
- Departamento de Cobranzas

Procesos.- Estos departamentos interactúan entre sí para poder brindar a los clientes el servicio solicitado, entonces se pueden definir los siguientes procesos:

- Planificación
- Comercialización
- Legalización
- Compras
- Almacenamiento de Equipos
- Instalaciones
- Conexión
- Servicio al Cliente

- Facturación
- Cobranzas
- Administración de Red
- Investigación y Desarrollo
- Medición, análisis y mejora

1.3 Estándar ISO 27001:2005

En este apartado se presentarán los objetivos y alcance del estándar para la seguridad de la información ISO 27001:2005. Este estándar puede ser implementado por cualquier tipo de organización sin importar en el ámbito que se desenvuelva: gubernamentales, bienes, y/o servicios, de manera semejante al estándar ISO para la gestión de la calidad.

Cabe señalar que este estándar es parte integrante de la familia de estándares ISO 27000, la cual está integrada por los estándares siguientes:

ISO 27001.- Esta norma es certificable e indica los requerimientos que debe cumplir un sistema de gestión de la seguridad de la información previo a obtener la certificación

ISO 27002. - Define los dominios y controles que corresponden a las mejores prácticas para implementar, operar y mantener un sistema de gestión de la seguridad de la información.

ISO 27003.- Es la guía generalizada de ISO para las empresas que desean implementar un sistema de gestión de la seguridad de la información.

ISO 27004.- Este estándar cubre las métricas y medidas de gestión de un sistema de seguridad de la información, incluyendo los controles sugeridos por el estándar ISO 27002.

ISO 27005.- Es una metodología estándar desde el punto de vista ISO para la gestión de los riesgos de la seguridad de la información.

ISO 27006.- Indica los lineamientos para la acreditación de organizaciones que ofrecen certificar a empresas buscan las certificación de sus Sistemas de Gestión de la Seguridad de la Información.

Tabla 1. Familia de Estándares ISO 27000

27001	27002	27003
REQUERIMIENTOS NORMA CERTIFICABLE	CONTROLES Y MEJORES PRACTICAS	GUIA DE IMPLEMENTACIÓN
27004	**27005**	**27006**
MÉTRICAS	GESTIÓN DE RIESGOS	PARA ENTES CERTIFICADORES

El estándar 27001:2005 establece los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener, y mejorar un Sistema Documentado de Gestión de la Seguridad de la Información dentro del contexto de los riesgos generados por el giro de negocios en que se desenvuelva la organización.

1.3.1 Seguridad de la Información

Las organizaciones generan y consumen información debido al giro mismo de sus operaciones sin importar la clase de actividad a la que estén dedicadas: balances contables, nómina de empleados, rol de pagos, campañas publicitarias, inventarios, movimientos bancarios, etc. Esta información era almacenada en formatos físicos los cuales corrían el riesgo de

ser sustraídos ó destruidos por entidades o personas con intereses contrarios a los de la organización.

Desde hace pocos años atrás, se empezó a usar formatos digitales para el almacenamiento de la información, debido a la baja de los costos de adquisición de dispositivos para ello. El formato físico se sigue usando como respaldo ó por exigencias de las legislaciones locales.

El almacenamiento y transporte de información sobre mecanismos digitales implementados en redes de computadoras las cuales pueden ser utilizadas por integrantes de la organización o por personal externo a la misma, produce de manera lógica la búsqueda de mecanismos para lograr la integridad, confidencialidad y disponibilidad de la información. Según el estándar ISO 27001 se define:

- **Integridad de la Información.-** La propiedad de salvaguardar la exactitud e integridad de los activos

- **Confidencialidad de la Información.-** La propiedad que la información esté disponible y que sea divulgada a personas, entidades o procesos autorizados
- **Disponibilidad de la Información.-** La propiedad de que la información esté disponible y utilizable cuando lo requiera una entidad autorizada.

Entonces según el estándar ISO 27001 se define: “Seguridad de información es la preservación de la confidencialidad, integridad y disponibilidad de la información, además también pueden estar involucradas otras propiedad como la autenticidad, responsabilidad, no repudio y confiabilidad” [1].

1.3.2 Estructura del Estándar

El estándar ISO 27001:2005 está formado de manera general por las siguientes etapas:

- Establecer el SGSI
- Implementar y operar el SGSI
- Monitorear y revisar el SGSI
- Mantener y mejorar el SGSI

El siguiente gráfico nos muestra la interacción entre estos requerimientos, en lo que se llama modelo PDCA (Plane-Hacer-Chequear-Actuar).

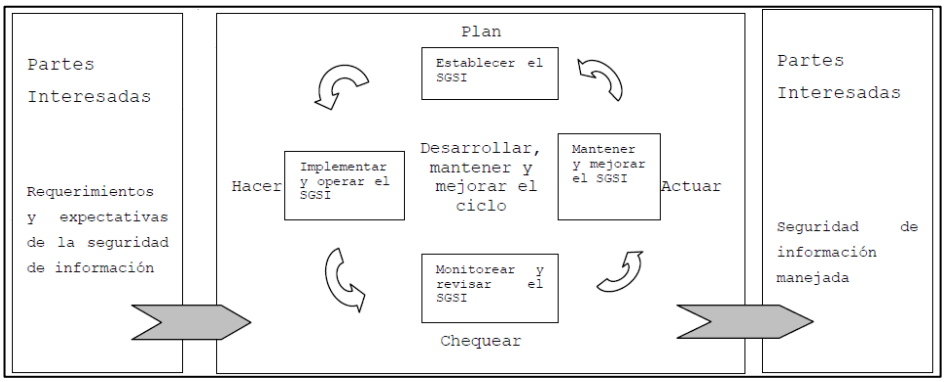


Figura 1.2 Interacción de los requerimientos del SGSI [2]

Adicionalmente debe existir evidencia de todos estos procesos para lo cual los requerimientos de documentación establecidos en el estándar certificable son parte esencial del mismo:

- Requerimientos de Documentación General.
- Requerimientos de Control de Documentos.
- Requerimientos de Control de Registros.

El estándar tiene requerimientos que deben ser cumplidos por la Gerencia:

- Compromiso de la Gerencia
- Gestión de Recursos
- Provisión de Recursos
- Capacitación, Conocimiento y Capacidad

Adicionalmente el estándar busca reglamentar los procesos de monitoreo, revisión y mejora a través de:

- Auditorías Internas
- Revisión Gerencial del SGSI
- General
- Insumo de la revisión
- Resultado de la revisión
- Mejoramiento el SGSI
- Mejoramiento Continuo
- Acción Correctiva
- Acción Preventiva

Este trabajo se enfoca principalmente en los requerimientos generales del estándar. Para poder cumplir estos requerimientos, el estándar cita explícitamente en su Anexo A de los Objetivos de Control y controles, a la norma no certificable ISO 27002:2005 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. Los objetivos de control y controles de derivan directamente de y se alinean con la norma no certificable ISO 27002.

La norma no certificable ISO 27002 establece el lineamiento guía y principios generales para iniciar, implementar, mantener y mejorar la gestión de la Seguridad de la Información dentro de la organización. Esta norma contiene las mejores prácticas de los objetivos de control y los controles en las siguientes áreas de la gestión de la Seguridad de la información:

- Política de Seguridad
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad de Recursos Humanos

- Seguridad Física y Ambiental
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de Incidentes de Seguridad de la Información
- Gestión de la Continuidad Comercial
- Conformidad

Se ha expuesto de manera breve los lineamientos que existen en los dos estándares, pero no hemos ingresado en detalle de mismo. En el capítulo siguiente se analizará la metodología empleada por este proveedor para establecer su sistema de gestión de la seguridad de la información.

CAPÍTULO 2

VALORACIÓN DE ACTIVOS Y ANÁLISIS DE RIESGOS

El objetivo inicial de este proveedor es esencialmente implementar un sistema de gestión de la seguridad de información que se encuentre en armonía con su sistema de gestión de la calidad y que le permita como objetivo económico disminuir las notas de crédito que debe generar a sus clientes por no cumplimiento de los acuerdos de disponibilidad del servicio proporcionado, eso a su vez permitirá tener un flujo de caja estable para poder tomar decisiones corporativas en un ambiente favorable.

En este apartado inicial se establece la metodología o procedimientos empleados para alcanzar los objetivos de este proveedor.

2.1 Metodología

Los lineamientos son dados por el mismo estándar, donde para poder cumplir con el objetivo de establecer el SGSI, se deberán realizar las siguientes actividades:

- Definir el Alcance
- Definir la política de Seguridad
- Definir el enfoque de la evaluación del riesgo
- Identificar los riesgos
- Analizar y evaluar los riesgos
- Identificar y evaluar las opciones para el tratamiento de riesgos
- Seleccionar los objetivos de control y controles para el tratamiento de riesgos
- Obtener la aprobación de la gerencia para los riesgos residuales propuestos
- Obtener la aprobación de la gerencia para implementar y operar el SGSI
- Preparar un enunciado de Aplicabilidad

Las actividades arriba indicadas se realizarán por el Departamento de Seguridad de Información en conjunto con las jefaturas involucradas en los procesos a ser certificados. Cabe indicar que

el Departamento de Seguridad de Información fue creado con la finalidad de liderar la implementación del Sistema de Seguridad de la Información.

De manera práctica apegada a la realidad del giro del negocio del este proveedor, internamente se implementa la siguiente metodología, siguiendo los lineamientos de la norma:

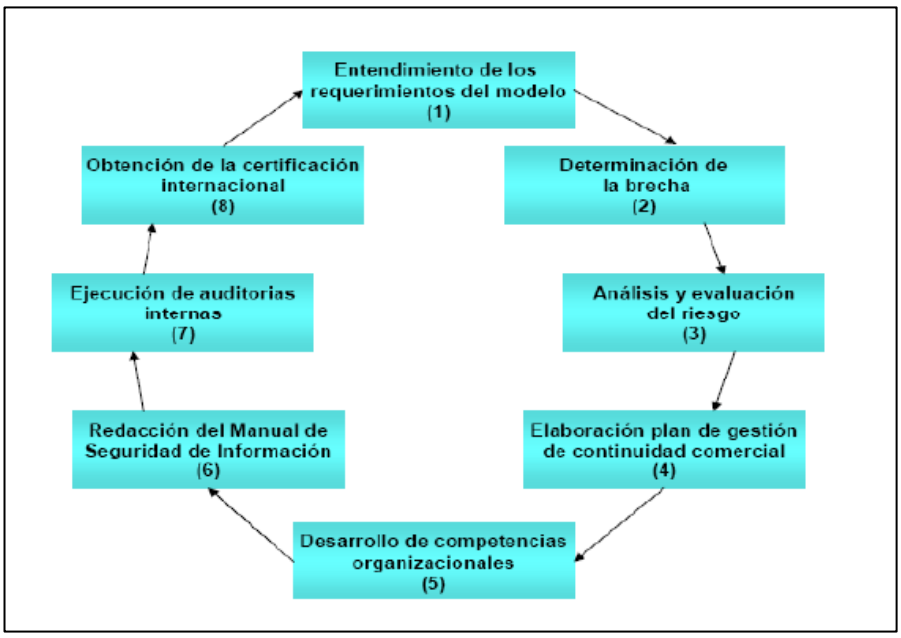


Figura 2.1 Metodología utilizada para implementación del sistema

2.1.1 Alcance del SGSI

El alcance debe ser aprobado por Gerencia. El alcance debe definir los procesos que van a ser objeto de certificación y las

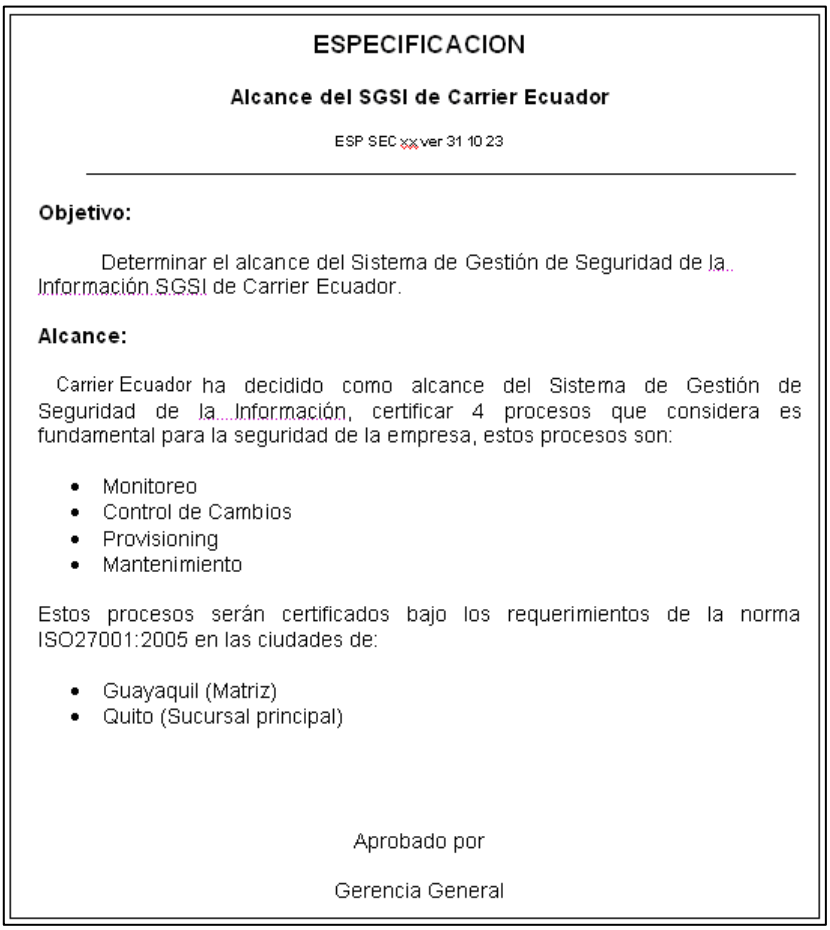
localidades donde se ejecutan estos procesos. Para este proveedor, y de acuerdo a los objetivos de este trabajo, los procesos a ser certificados en las ciudades de Guayaquil (Casa Matriz) y Quito (Sucursal Mayor) son:

- Aprovisionamiento
- Control de Cambios
- Mantenimiento

Aprovisionamiento es el proceso mediante el cual el proveedor obtiene y utiliza los elementos de hardware, software y de personal necesarios para poder brindar sus servicios. Demoras y/o fallas en este proceso ocasiona afectación en la entrega y disponibilidad del servicio.

El control de cambios es un proceso esencial para este proveedor. El proveedor busca implementar una serie de procedimientos para que los cambios ejecutados en la infraestructura tanto a nivel de hardware como software sean coordinados y su efecto sea mínimo sobre la disponibilidad del servicio del cliente.

Debe existir un documento que sea evidencia y donde se especifique el alcance del SGSI y que la Gerencia aprueba. La siguiente figura muestra un ejemplo del documento de definición del alcance de sistema de gestión de la seguridad de la información firmado por el Gerente General.



ESPECIFICACION

Alcance del SGSI de Carrier Ecuador

ESP SEC xx ver 31 10 23

Objetivo:

Determinar el alcance del Sistema de Gestión de Seguridad de la Información SGSI de Carrier Ecuador.

Alcance:

Carrier Ecuador ha decidido como alcance del Sistema de Gestión de Seguridad de la Información, certificar 4 procesos que considera es fundamental para la seguridad de la empresa, estos procesos son:

- Monitoreo
- Control de Cambios
- Provisioning
- Mantenimiento

Estos procesos serán certificados bajo los requerimientos de la norma ISO27001:2005 en las ciudades de:

- Guayaquil (Matriz)
- Quito (Sucursal principal)

Aprobado por

Gerencia General

Figura 2.2 Ejemplo de definición del alcance del SGSI

2.1.2 Política de Seguridad

La política de seguridad establece un sentido de dirección general para la empresa. A través de la misma se logran

establecer los objetivos de la empresa en el ámbito de la seguridad de la información y los mecanismos para alcanzar dichos objetivos.

Una Política de Seguridad debe exponer los puntos que quiere dar a conocer la empresa, su ámbito de acción, sus objetivos, y sus mecanismos para lograrlo. Estos aspectos son la estructura que debe de llevar la carta de presentación ante el cliente, para que tenga una idea muy clara de la empresa a la que está a punto de comprar sus productos o servicios. Desde este punto de vista, este proveedor define su política de seguridad:

“Proveer servicios de Telecomunicaciones disminuyendo el riesgo de incidentes que atenten contra la disponibilidad, integridad y confidencialidad de nuestra infraestructura, utilizando un Sistema de Gestión de la Seguridad de la Información basado en la prevención”

El proveedor define sus propios índices para medir los objetivos de su política de seguridad en base a su giro del negocio y con la meta clara de disminuir las notas de crédito

por fallas en la disponibilidad de los servicios que provee. Estos índices son adicionales a los que exige la norma, pero esta no prohíbe la creación de nuevos índices.

Tabla 2. Objetivos e índices de la política de Seguridad

OBJETIVOS DE SEGURIDAD DE INFORMACIÓN	INDICADORES
▪ Disminuir el porcentaje de notas de crédito, asociadas a la pérdida del SLA de los clientes.	Disponibilidad: El total de pérdida mensual por notas de crédito no puede ser mayor al 2% de la facturación mensual. Frecuencia: mensual

▪ Formar al 80% de los empleados en las áreas de: Buenas prácticas de seguridad de información *y* análisis de causalidad de incidentes de seguridad.	TFOR = % Empleados Formados TFOR = (# Personal Formado x 100)÷(# Total de Empleados) Frecuencia: Anual
▪ Controlar los accidentes laborales suscitados en la empresa a nivel nacional mediante el uso de buenas prácticas de seguridad.	AL = Accidentes Laborales AL = 0 Frecuencia: Anual

2.2 Levantamiento de los activos

Primeramente se define como activo todo aquello que tiene valor para la empresa y que por lo tanto debe ser protegido. En cada proceso están involucrados varios departamentos, y los activos, para lograr el servicio para el cliente final.

2.2.1 Activos en el proceso de aprovisionamiento

El proceso de aprovisionamiento es la actividad que tiene el proveedor, de obtener y utilizar los recursos necesarios para poder brindar el servicio al cliente final. Esto va más allá a un enfoque sólo de hardware y software, el aprovisionamiento también toma en cuenta a los activos humanos de cada departamento y las actividades de los mismos.

Primero se establece la cadena de valor, es decir todas las etapas hasta generar los servicios:

- Planificación
- Gestión de Preventa
- Cierre de Venta
- Instalación
- Legalización
- Servicio Post Venta

En resumen esta es la cadena de valor de este proveedor. Luego usando el método de las elipses se determina como cada departamento de este proveedor interactúa con cada etapa. Se ha utilizado el método de las elipses por ser un mecanismo sencillo para identificar los elementos que actúan entre si durante la operación de la empresa. Este método permite identificar posteriormente los activos de información. La elipse central contiene los procesos principales y la siguiente elipse externa contiene los departamentos que realizan dichos procesos, y las más externas contienen los agentes ajenos a la empresa que también interactúan con los procesos. Finalmente se identifica la interacción entre los procesos y las entidades a través de flechas direccionales o bidireccionales según como sea la interacción. Este trabajo de identificación de la interacción se realiza con la presencia de las jefaturas de cada departamento.

Del gráfico del Anexo 1 se observa que los departamentos que están presentes en todas y casi todas las etapas de la cadena de valor son:

- Gerencia General
- Departamento Financiero

- Departamento de Ventas
- Compras
- Aprovisionamiento de Hardware y Almacenamiento
- Planificación y Logística
- Departamento de Fibra Óptica
- Departamento de Radio Enlaces
- Soporte Técnico Corporativo
- Operación y Monitoreo
- Departamento de Asuntos Legales

Estos han sido ordenados en relación a cada etapa, es decir, las gerencias y el departamento financiero junto con el de ventas planifican objetivos de números de clientes que van a ser servidos, luego para instalarlos es necesario la compra local y algunas veces la importación de dispositivos, luego el departamento de planificación y logística verifica la factibilidad de poder instalar la última milla dependiendo de la ubicación del cliente.

La última milla es instalada a través de la labor de los departamentos de fibra óptica o de radio enlaces dependiendo de las distancias entre la oficina del cliente hasta el nodo de

este proveedor. En el servicio post venta el cliente es atendido en caso de inconvenientes ya sea físicos ó lógicos en su enlace por el Departamento de operaciones y monitoreo, en primera instancia, y en caso de ser necesario, el soporte sobre configuraciones adicionales y cambios de dispositivos a cargo del Departamento de Soporte Técnico Corporativo.

Una vez identificados los departamentos involucrados en el proceso de aprovisionamiento, se procede a levantar los activos de información y humanos utilizados en este proceso:

- Gerencia General
- Formatos de instalaciones
- Sistemas de Facturación
- Base de datos de Clientes
- Tabla de precios
- Análisis de mercados
- Sistemas de gestión de enlaces
- Sistema email
- Servidores de acceso
- Sistemas de Telefonía IP
- PBX

- Proveedores telefonía Fija
- Interconexión de redes y Firewall internos
- Bodega
- Solicitud de compras nacionales e internacionales
- Solicitud de materiales
- Personal operativo
- Personal Administrativo
- Procedimientos de cambios en la Red
- Manuales y formatos internos
- Equipos de cómputo del personal
- Intranet
- Software Utilitario
- Diagramas de Red y clientes
- Sistema CRM
- Sistema de Registro de dominios
- Personal de Ventas
- Contrato con clientes
- Contrato con dueños de Infraestructura
- Contrato de Proveedores de Internet

2.2.2 Activos en el proceso de control de cambios

El control de cambios es quizás uno de los procesos críticos en la operación adecuada de un proveedor de Servicios de Telecomunicaciones. Planificar los cambios, emular los efectos de los cambios en un ambiente de no producción, levantar la documentación, permisos previos y plan de contingencia en caso de falla, por lo general reversando al estado inicial, implementar el cambio en la ventana de trabajo provista, monitorear si los efectos son los esperados y documentación final; todos estas actividades deben estar documentadas en uno ó varios procedimientos que sean los lineamientos para su desarrollo.

Este proveedor haciendo uso de las mejores prácticas internacionales para proveedores de servicios de Internet y datos, tiene implementado desde 2005 un documento llamado SMOP de las siglas en inglés Service Method of Procedure, sin embargo para el envío, revisiones y aprobación de ese documento donde estaban las acciones a realizarse e inclusive las configuraciones a implementarse y acciones de rollback, se utilizaba el correo electrónico.

Como herramienta para la gestión del proceso de cambios, el departamento de Sistemas, desarrollo un portal Web donde las personas asignadas para una tarea ó cambio, pueden cargar el SMOP, este SMOP es revisado por los supervisores o jefes de cada área, y esta tarea es agendada en una ventana de trabajo y asignada un ID para que se pueda dar seguimiento antes, durante y después de ejecutada. En el Anexo 2 se presenta un ejemplo de SMOP.

Las etapas por las cuales transcurre el proceso de control de cambios de este proveedor son:

- Planificación Anual
- Planificación Semanal
- Elaboración de SMOP’s
- Revisión de SMOP’s
- Aprobación de SMOP’s
- Ejecución de SMOP’s
- Post Evaluación de SMOP’s

Utilizando el método de las Elipses, se procede a identificar los departamentos que participan en las etapas de este proceso.

En el Anexo 3 se presenta el gráfico de Elipses para Proceso de Control de Cambios

Los departamentos involucrados en este proceso son:

- Gerencia General
- Gerencia Financiera
- Departamento de asuntos Legales
- Departamento de Administración del Backbone
- Departamento de Fibra óptica
- Departamento de Radio Enlaces
- Departamento de Soporte Técnico Corporativo
- Departamento de Soporte a Bancos
- Departamento de Operaciones y Monitoreo de Redes.
- Departamento de Transmisiones Ópticas

Finalmente se identifican las herramientas o activos que estos departamentos utilizan en el proceso de control de cambios:

- Planificación semanal
- Archivo de Planificación Semanal
- Service Project (Web Access)
- Correo Electrónico
- Servidor Project server (hardware)
- Reporte de trabajos emergentes
- Listado de tareas determinadas
- Simuladores hardware y software
- Personal Técnico
- Notificación de trabajo
- Lista de clientes afectados
- SMOP’s
- Base de Datos de Desarrollo (hardware y software)
- Sistemas de gestión de Red
- Documentos SMOP revisado
- Mail de Aprobación de SMOP’s
- SMOP’s Corregido
- Equipos de backbone
- Sistemas DNS
- Sistema de gestión de clientes
- Repositorios contingencias SAN
- Diagramas de clientes y de Red

- Sistema asignación de claves
- Instructivos
- Sistema intranet
- Sistema de autentificación TACACs
- Fibra óptica backbone
- Enlaces radio backbone
- Sistemas de backup
- Reporte trabajos programados

2.2.3 Activos en el proceso de mantenimiento

El mantenimiento de la infraestructura, el cambio de elementos averiados, obsoletos de mal funcionamiento, ya sea como acción preventiva ó como acción reactiva es un proceso en las operaciones de este proveedor.

Las etapas del proceso de mantenimiento son:

- Planificación del Mantenimiento
- Revisión de la Planificación
- Ejecución del Mantenimiento
- Análisis Post Mantenimiento

Utilizando el método de las elipses, se obtiene el gráfico del Anexo 4 y a partir de este, se identifican los departamentos que actúan en las etapas de este proceso:

- Gerencia Financiera
- Departamento de Fibra Óptica
- Departamento de Radio Enlaces
- Departamento de Soporte y Monitoreo de Redes
- Departamento de Soporte Técnico Corporativo

Ahora se identifican las herramientas ó activos que estos departamentos utilizan en el proceso de mantenimiento.

En el subproceso de planificación:

- Project Server
- Formatos de planificación
- Planificación estratégica

En el subproceso de Revisión de la planificación:

- Solicitud de Permisos y Materiales
- Transporte

En el subproceso de ejecución y post mantenimiento:

- Documentación (Checklist)
- Herramientas: OTDR, fusionadora, medidor de potencia
- Fibra Óptica de nodos
- Aplicativo Repetidoras de Nodos y respaldos eléctricos
- Sistema de llaves
- Personal de Técnico
- Enlaces de radio de backbone, nodos y clientes.
- Enlaces de radio de nodos
- Cargadores de batería de backbone y nodos
- Banco de baterías de backbone y nodos
- Correo electrónico
- Sistema de gestión de clientes
- Instructivos
- Sistema de gestión de la Red e Incidencias
- Teléfonos celulares
- Computadoras portátiles
- Contratos de dueños de infraestructura
- Reporte de trabajos programados
- Listas de escalabilidad
- Caja chica
- SMOP’s
- Repositorio de Contingencias (SAN)

- Aplicativo Bitácora
- Telepuertos y nodos principales

2.3 Valoración de los activos

El valor de los activos no depende de sus valor monetario sino del valor respecto a los aspectos se la seguridad de la información.

La valoración de los activos sirve para determinar el impacto que el deterioro, falla o pérdida de los mismos tiene sobre la confidencialidad, disponibilidad e integridad de los procesos de aprovisionamiento, control de cambios y mantenimiento.

Una vez identificados los activos involucrados en los tres procesos a certificar, para la valoración de los mismos, este proveedor utiliza los criterios de confidencialidad, disponibilidad e integridad, y según el grado de impacto en caso de pérdida, falla, o deterioro, se asigna un valor de 1 al 5, siendo 1 el de menor impacto y 5 el de mayor impacto. Luego se obtiene un promedio, si este promedio está entre 1 ó 2.99, este activo no tiene suficiente valor para ser considerado en el análisis de riesgo.

Se pudiera escoger un rango más pequeño pero el proveedor decide disminuir la cantidad de activos a ser considerados en el análisis de riesgos.

A continuación se presenta un ejemplo del ejercicio de valoración de un activo en la etapa de ejecución en el proceso de mantenimiento.

Tabla 3. Ejemplo de la valoración de activos

	Confidencialidad	Integridad	Disponibilidad	Promedio	Observaciones	Evaluación del riesgo
OTDR	1	5	5	4	Herramientas de Fusión	Si
Fusionadora	1	5	5	4		
Medidor de potencia	*1*	*5*	*5*	*4*		

Las herramientas de fusión de fibra óptica como es el caso de la fusionadora, el medidor de potencia, y el OTDR óptica tienen un impacto mínimo respecto a la confidencialidad del proceso, no así respecto a la disponibilidad e integridad del proceso de mantenimiento. El valor promedio es 4 y por estar encima del límite superior de 2.99, será considerado en el análisis de riesgo.

Este ejercicio se debe realizar para cada uno de los procesos y para cada uno de los activos que participan en los mismos. Este

ejercicio se realizó con los representantes de cada una de las jefaturas de los departamentos involucrados en cada uno de los procesos. Se toma la apreciación subjetiva inicialmente de los representantes para luego hacerla medible a través de pesos. Cabe señalar que la empresa toma la decisión de hacer el análisis de esta manera debido a la experiencia de cada una de las Jefaturas con un promedio de aproximadamente 10 años en sus funciones**.** En los anexos 5, 6 y 7 se presentan la valoración de activos de los procesos de aprovisionamiento, control de cambios y mantenimientos respectivamente.

2.4 Análisis de los riesgos

El estándar ISO 27001 especifica que los controles y acciones a ser implementadas dentro del sistema de gestión de seguridad de la información deben estar basados principalmente en gestión de los riesgos.

Los lineamientos para la gestión de los riesgos en la seguridad de la información son presentados en el estándar ISO 27005 que es parte de los estándares ISO dedicados a la seguridad de la información.

A continuación se presenta una revisión de este estándar el cual será la herramienta usada por este proveedor para la gestión del riesgo

2.4.1 El estándar ISO 27005 y la gestión de los riesgos

Se puede resumir la gestión del riesgo en las siguientes dos actividades: la evaluación y el tratamiento del mismo.

Pero para evaluar el riesgo, se debe definirlo primeramente, según el estándar el riesgo es:

Riesgo = vulnerabilidad + amenaza + probabilidad de ocurrencia de la amenaza

No se trata de una fórmula matemática sino más bien en presentar al riesgo como la convergencia de estos tres elementos: vulnerabilidad, amenaza y probabilidad de ocurrencia de la amenaza. Según el estándar se tiene:

Vulnerabilidad.- Es la debilidad de un activo ó grupo de activos que puede ser explotado por una ó más amenazas.

Una vulnerabilidad que no esté asociada a ninguna amenaza puede no ser considerada al establecer los controles.

Amenazas.- Son circunstancias o eventos que tienen una probabilidad de ocurrencia que tienen el potencial de afectar negativamente los activos de la empresa como información procesos y sistemas y por ende a la empresa misma.

Amenazas accidentales o deliberadas deben ser identificadas y estas deben ser categorizadas (ejemplo acciones no autorizadas, daño físico y averías técnicas)

El estándar indica que la probabilidad de ocurrencia de una amenaza puede ser obtenida de los dueños del activo, del personal humano de la corporación, de especialistas en administración y seguridad de la información, expertos en seguridades físicas, departamentos legales, monitoreo del clima, compañías de seguros, y autoridades gubernamentales. El estándar propone el siguiente modelo iterativo de gestión del riesgo:

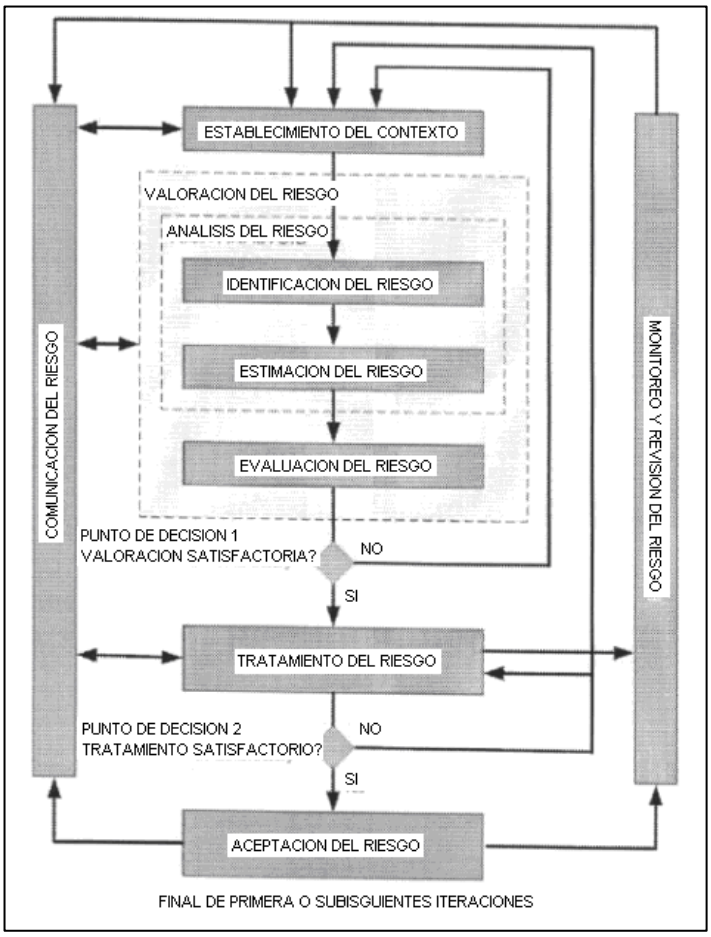


Figura 2.3 Modelo Iterativo de gestión del riesgo [3]

Se observa que la gestión del riesgo empieza en el establecimiento del contexto, esto lo ha realizado el proveedor al definir los procesos que van a ser certificados, y al levantar y valorar a los activos de acuerdo al enfoque de la confidencialidad, integridad y disponibilidad.

Según el gráfico la siguiente etapa es el análisis del riesgo el cual consta de dos procesos identificación del riesgo y estimación de ocurrencia del riesgo, y luego se avanza a la etapa del tratamiento del riesgo.

El estándar coloca los procesos de aceptación del riesgo, comunicación del riesgo, y monitoreo y revisión como procesos bien marcados y definidos. El estándar da mucha importancia a estos tres últimos y en especial al monitoreo el cual es la retroalimentación del sistema de gestión del riesgo que permite en caso de ser necesario empezar nuevamente por el proceso inicial.

Este es el caso cuando las acciones y controles utilizados para minimizar el riesgo no brindan los resultados esperados debido a análisis no adecuados en el momento de su definición o cambios en las circunstancias y escenarios en las que se desenvuelven los procesos a ser certificados.

Este proveedor entonces empieza el análisis de riesgos relacionando los activos considerados con sus respectivos administradores también llamados los dueños de los activos.

2.4.2 Dueños de los activos y el departamento de seguridad lógica

Hasta se ha identificado los activos que son utilizados por los varios departamentos en los procesos a ser certificados. Estos activos son administrados no necesariamente por los departamentos que los utilizan, sino en ciertos casos por departamentos especializados, el departamento de Sistemas ó por alguna Jefatura. Una vez identificados los dueños de los activos, el análisis de los riesgos se facilita ya que son los mismos administradores o responsables de los activos los que empiezan a enlistar las vulnerabilidades y los riesgos a los que están sometidos los activos.

Un elemento importante que este proveedor utiliza tomando en cuenta la sugerencia del estándar ISO 27005, es la creación de un Departamento de Seguridad Lógica, al cual como se ha indicado anteriormente, se le ha dado jurisdicción de coordinar junto con los demás departamentos las actividades necesarias para realizar la gestión del riesgo y la implementación del sistema de gestión de la seguridad de la información.

Este departamento es un ente supervisor, adicionalmente tiene la responsabilidad de administrar equipamiento de seguridad de este proveedor a nivel del backbone y de la red interna del edificio Matriz en Guayaquil. Coordina charlas de concientización respecto a normas básicas de seguridad contra ataques de ingeniería social, auditorías internas, etc.

2.4.3 Metodología utilizada para el análisis de riesgos

Este proveedor realiza el análisis de riesgos en conjunto con los dueños de los activos, tal como se indicó anteriormente. Como se observa en el gráfico de gestión del riesgo, en apartados anteriores ya se identificaron los activos de este proveedor y se valoraron los mismos. Ahora en este apartado las siguientes etapas a revisar son:

- Identificación de las amenazas y vulnerabilidades
- Estimación de ocurrencia
- Evaluación del impacto
- Tratamiento de los riesgos

Identificación de amenazas.- Es importante para el análisis, identificar previamente las amenazas que pudieran afectar los

activos de la organización. Conviene clasificar las amenazas por su naturaleza para facilitar su ubicación, ya que de hacerlo por cada uno de los activos, se presentará información redundante. Se presentan 6 tipos de amenazas:

1.- Amenazas naturales (inundaciones, maremotos, tornados, sismos, tormentas, incendios forestales)

2.- Amenazas a instalaciones (fuego, explosión, perdida de energía, daños de agua, perdida de acceso, fallas mecánicas)

3.- Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, perdida de personal clave)

4.- Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas de red, fallas en líneas telefónicas)

5.- Amenazas operacionales (crisis financiera, pérdida de proveedores, fallas de equipos, aspectos legales y regulatorios, mala publicidad)

6.- Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo)

En este apartado se debe tomar en cuenta de manera conjunta a las amenazas y a las vulnerabilidades. Por este motivo se requiere relacionarlas con la siguiente interrogante:

¿Qué amenaza pudiera explotar cuál de las vulnerabilidades?

Anteriormente se presentó que los riesgos son el resultado de la interacción de las amenazas, vulnerabilidades y la probabilidad de ocurrencia, ahora se presenta la relación existente:

Tabla 4. Relación Vulnerabilidad – Riesgo

CAUSA	PROBABILIDAD	EFECTO
Amenaza →	Vulnerabilidad →	Riesgo → Activo

Lo adicional en este gráfico es mostrar como las vulnerabilidades aumentan la probabilidad de que una amenaza se haga efectiva para consolidarse como un riesgo real para la organización.

Identificación de Vulnerabilidades.- Se procede a identificar las vulnerabilidades por las distintas fuentes que las pueden originar, utilizando como guía algunos de los dominios de la norma ISO 27002:2005, según esto se tiene:

1.- Seguridad de los recursos humanos: Falta de entrenamiento en seguridad, falta de concientización en aspectos de seguridad, ausencia de mecanismos de monitoreo, ausencia de políticas para el correcto uso de las telecomunicaciones, falta de eliminación de accesos de ex colaboradores, falta de procedimientos de entrega de activos al término de contrato, falte de motivación a los empleados

2.- Control de acceso: Distribución inapropiada de redes, ausencia de políticas de de escritorio, protectores de pantalla, y protección de equipos de comunicaciones fijas, móviles, ausencia de políticas de control de acceso: passwords, token pass, etc.

3.- Seguridad física y ambiental: Ausencia de seguridades de control de acceso físico a las instalaciones, oficinas y bodegas, ausencia de procedimientos para tratamiento de

equipos obsoletos y/o averiados, ausencia de controles de variaciones de voltaje

4.- Gestión de operaciones y comunicaciones: Sistemas de información no amigables con los usuarios, control de cambios inadecuado, o totalmente inexistente, gestión inadecuada de la red, ausencia de mecanismos que controlen confirmación de envío y recepción de mensajes electrónicos, ausencia de distribución de tareas de administración, ausencia de control de copiado de documentos, ausencia de protección para conexiones externas y remotas

5.- Mantenimiento, desarrollo y adquisición de sistemas de información: ausencia de manejo de llaves criptográficas, ausencia de políticas para el uso de criptografía, ausencia de validación de datos procesados, falta de ambiente de ensayo antes de puesta a producción de sistemas, documentación de software pobre o inadecuada, mala selección de ensayos de datos

Estimación de ocurrencia.- Como se indicó anteriormente, “el riesgo se define como la probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular” [4].

También se indicó que las vulnerabilidades aumentan la probabilidad de que una amenaza se concrete, es decir genera un riesgo a los activos de la información. Para la estimación de ocurrencia se debe considerar los siguientes aspectos de las amenazas, los cuales también aumentan la probabilidad de que se concreten:

Amenazas deliberadas.- Atracción de los activos genera motivación en los atacantes. El aumento de recursos disponibles para los atacantes: conocimiento, herramientas.

Amenazas accidentales.- Esta probabilidad puede ser obtenida en base a la experiencia de eventos anteriores y estadísticas.

Nuevas tendencias y desarrollo.- Aquí se consideran los informes, novedades y tendencias obtenidas por diferentes medios como Internet y consultorías externas.

Evaluación del impacto.- Primeramente se busca dar prioridad a los riesgos según aquellos cuya probabilidad de que la amenaza se concrete sea mayor, y el valor del activo

involucrado. Este proveedor relaciona estos factores en su análisis usando nuevamente la escala de 5 niveles de Likert:

Tabla 5. Escala de Likert

1	2	3	4	5
Muy Bajo	Bajo	Medio	Alto	Muy Alto

Se implementa entonces la siguiente tabla para realizar el análisis:

Tabla 6. Esquema de medición del riesgo

ACTIVO	AMENAZA	VULNERABILIDAD	VALOR DEL ACTIVO	PROBABILIDAD DE OCURRENCIA	MEDICIÓN DEL RIESGO	PRIORIDAD
A	W	A	5	3	15	1
B	X	B	4	2	8	3
C	Y	C	3	3	9	2
D	Z	D	2	2	4	4

Se observan en las dos primeras columnas enlistados los activos y las amenazas relacionadas a dichos activos. En la

tercera columna se colocan las vulnerabilidades del activo analizado. En la cuarta columna se coloca el valor de los activos. En la quinta columna se coloca la probabilidad de ocurrencia de dicha amenaza, para calcular este valor se considera el promedio entre los pesos de las amenazas y los pesos de las vulnerabilidades, y la multiplicación de los valores de la cuarta y quinta columnas es colocado en la sexta columna de Medición del Riesgo, finalmente dependiendo de los resultados obtenidos en la séptima columna, se otorga la prioridad 1 a las amenazas que obtuvieron un mayor resultado de la multiplicación.

Una vez obtenido el orden de prioridades de los riesgos, se procede a evaluarlos de acuerdo a criterios de significancia para la organización en caso de que el riesgo se materialice. En el caso de este proveedor se escogieron:

- Impacto económico
- Tiempo de recuperación
- Imagen
- Interrupción activa

Son las gerencias en conjunto con la presidencia de la empresa quienes escogen los criterios de evaluación de los riesgos en base al giro del negocio y los objetivos del mismo.

Se puede observar que se busca precautelar los intereses económicos y la imagen de la organización, los demás criterios de tiempo de recuperación e interrupción activa son las causas del impacto económico, es decir mientras más tiempo le tome a la organización recuperarse, y mientras mayor es el tiempo que el ataque o amenaza concretada persista, los efectos económicos serán mucho mayores y la imagen de la organización se ve afectada ante sus clientes y potenciales clientes.

Se usará una escala del 1 al 5, siendo uno el menor valor de importancia del criterio afectado por el riesgo, y 5 el de mayor valor.

Tabla 7. Esquema de evaluación del riesgo

ACTIVO	IMPACTO ECONÓMICO	TIEMPO DE RECUPERACIÓN	IMAGEN	INTERRUPCIÓN DE ACTIVIDAD	TOTAL EVALUACIÓN DEL IMPACTO
A	w	1	3	2	6
B	x	4	2	3	9
C	y	3	3	2	8
D	z	2	2	1	5

Como se puede observar, el valor total del impacto del riesgo es la suma de los pesos asignados a cada uno de los factores.

Finalmente al multiplicar el valor de medición del riesgo obtenido en la tabla anterior, por el valor de evaluación del impacto, se obtiene el valor total de evaluación del riesgo, es decir, el valor total toma en cuenta las amenazas y vulnerabilidades y como estas aumentan el riesgo, además del impacto en caso de materialización de los mismos, obteniéndose un valor total de evaluación del riesgo.

En el Anexo 8, se muestra la evaluación total del riesgo considerando la estimación del riesgo y la evaluación del impacto.

2.5 Definición de las acciones

Una vez que el riesgo se ha calculado, se obtiene un orden de activos en base a los riesgos calculado. ¿Qué hacer con esos activos?. La gerencia debe definir qué acciones tomar sobre esos activos, sin embargo la toma de una decisión respecto a ese activo está influenciada por dos factores:

- El posible impacto si el riesgo se manifiesta
- La frecuencia de ocurrencia del evento

Con estos factores, la gerencia puede proyectar las pérdidas esperadas si el riesgo se concreta en acciones, y si no se toman acciones para mitigar el riesgo estimado.

Sin embargo los valores de frecuencia de ocurrencia y estadísticas necesarias para la toma de la decisión son escasos ó nulos en el área de seguridad de la información lo que hace difícil la tarea para la gerencia.

Por lo que se solicita la colaboración de los dueños de los activos y la experiencia que ellos pueden aportar para ayudar a la gerencia a la toma de una decisión: asumir el riesgo, disminuir el riesgo, o traspasar el riesgo. Esto se verá en detalle en el capítulo siguiente.

CAPÍTULO 3

LOS CONTROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

En los capítulos anteriores se ha presentado la situación de este proveedor, se ha definido el alcance del sistema de gestión de la seguridad de la información, luego se realizó el inventario de activos, el análisis y la evaluación del riesgo. Ahora este proveedor debe decidir cómo va a tratar el riesgo, con que controles va a disminuirlos o eliminarlos de ser posible y que riesgos va a traspasar y cuáles son los motivos para estas decisiones.

3.1 Definición y establecimiento de los controles

El estándar ISO 27001:2005 en su Anexo A define 133 controles para sus sistema de gestión de la seguridad de la información y que

inclusive pueden ser usados para seguridad física, asuntos de recursos humanos y aspectos legales. El Anexo A de la norma define ciertos puntos que agrupan a los controles, los cuales son llamados dominios:

- Política de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad relacionada con el personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de la información.
- Gestión de los incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

Cabe recalcar que solo el estándar ISO 27001 es la norma certificable ya que define los requerimientos que debe cumplir un sistema de gestión de seguridad de información, en cambio el estándar ISO 27002 es la guía de implementación de los controles.

Tabla 8. Dominios de la seguridad de la información

SECCIÓN A	DOMINIOS	OBJETIVOS	CONTROLES
5	Política de Seguridad	1	2
6	Aspectos organizativos para la seguridad	2	11
7	Gestión de los activos	2	5
8	Seguridad de los Recursos Humanos	3	9
9	Seguridad física y del entorno	2	13
10	Gestión de comunicaciones y operaciones	10	32
11	Control de accesos	7	25
12	Adquisición, desarrollo y mantenimiento de sistemas	6	16
13	Gestión de incidentes de seguridad de la información	2	5
14	Gestión de continuidad del negocio	1	5
15	Conformidad	3	10
	TOTALES	39	133

3.1.1 Controles de política de seguridad

Según la norma estos dominios buscan brindar a la gerencia las directrices y soporte para lograr la seguridad de la información (integridad, confidencialidad, disponibilidad) que estén alineados con los requerimientos del giro del negocio y

enmarcados dentro de las regulaciones legales locales. Para esto la norma presenta dos controles: el documento de la política de la seguridad de la información y revisiones periódicas del documento.

Los detalles de los controles se encuentran en el estándar sin embargo, se puede indicar que el documento de la política de la seguridad de la información debe ser realizado en conjunto con la gerencia, aprobado y luego puesto a conocimiento de todos los empleados y terceros que a criterio de la organización deban conocerla.

Respecto a las revisiones del documento, el estándar solicita que sean periódicas o en caso de que algún evento amerite la modificación del documento, por ejemplo, cambios de tecnologías, de giro del negocio, amenazas concretadas, etc.

3.1.2 Controles de organización de la seguridad de la información

En este dominio, la norma solicita establecer aspectos importantes entre ellos: compromiso de la gerencia, roles, responsabilidades, acuerdos de confidencialidad entre otros.

Dedica la mayor parte de los controles al trato con terceros, es decir, solicita hacer un inventario de conexiones de red y flujos de información y exige la revisión de los controles seleccionados.

Este dominio presenta 11 controles, cabe señalar que es la organización la que selecciona si implementa o no todos. Estos controles son:

- Compromiso de la gerencia
- Coordinación de la seguridad de la información
- Asignación de responsabilidades de la seguridad de la información
- Autorización de proceso para facilidades procesadoras de información.
- Acuerdos de confidencialidad
- Contacto con las autoridades
- Contacto con grupos de interés especial
- Revisión independiente de la seguridad de la información.
- Identificación de los riesgos relacionados con los grupos externos.
- Tratamiento de la seguridad con clientes

- Tratamiento de seguridad en acuerdos con terceros

El estándar ISO 27002 presenta los objetivos y los detalles de implementación para cada control.

3.1.3 Controles de gestión de activos

Los controles de este dominio de la norma, solicitan a la organización la elaboración de un inventario de activos de información, donde se definan los administradores ó "dueños" de los activos. Adicionalmente solicita la valoración de los mismos. Este dominio presenta cinco controles:

- Inventario de activos
- Propiedad de los activos
- Uso aceptable de los activos
- Lineamiento de clasificación
- Etiquetado y manejo de la información

3.1.4 Controles de seguridad de recursos humanos

Este dominio de la norma solicita a la organización la reducción de riesgos de robo, mala utilización de medios,

fraude a través de los controles presentados, asegurando que los empleados, contratistas y terceros sean calificados para los roles que fueron solicitados, y estos entiendan sus responsabilidades para con la organización.

Para esto el estándar, de manera lógica, solicita la verificación de antecedentes antes de cualquier contratación y al final de los contratos se solicita un control de los activos utilizados por los contratados. Adicionalmente con el objetivo de que los contratados conozcan sus responsabilidades respecto al sistema de gestión, la norma solicita a la organización la capacitación tanto de sus empleados y la difusión de las políticas en que se impliquen terceros. Este dominio presenta 9 controles:

- Roles y responsabilidades
- Investigación de antecedentes
- Términos y condiciones de empleo
- Responsabilidades de la gerencia
- Conocimiento, educación y capacitación en seguridad de la información
- Proceso disciplinario
- Responsabilidades de terminación

- Devolución de los activos
- Retiro de los derechos de acceso

3.1.5 Controles de seguridad física y ambiental

La norma presenta controles para prevenir el acceso no autorizado, daño o interferencia a los establecimientos y por ende a la información. Establece procedimientos para prevenir el daño o pérdida activos de información. Prevenir extracción o robo y mantener la integridad de la información y los establecimientos donde se procesa la información, mediante chequeos y revisiones periódicas. La norma presenta 13 controles:

- Perímetro de seguridad física
- Controles de ingreso físico
- Aseguramiento de oficinas, habitaciones y medios
- Protección contra amenazas externas e internas
- Trabajo en áreas aseguradas
- Áreas de acceso público, entrega y carga
- Ubicación y protección de equipos
- Servicios públicos de soporte
- Seguridad del cableado

- Mantenimiento del equipo
- Seguridad del equipo fuera del local
- Seguridad de eliminación ó re uso del equipo
- Retiro de la propiedad

Se puede observar que los controles están dirigidos inicialmente a precautelar las instalaciones no solo de acceso autorizado sino también de amenazas como incendios e inundaciones. Luego hace énfasis en el tratamiento de los equipos procesadores de información tanto en instalación, operación, mantenimiento y retiro de los mismos.

3.1.6 Controles de gestión de comunicaciones y operaciones

Es el dominio más extenso con 32 controles propuestos. Solicita a la organización una serie de procedimientos para supervisión de terceros, planificación de capacidad TI, pruebas de seguridad, criterios de aceptación en producción, controles informáticos como antivirus, firewalls, IDS, IPS. Adicionalmente y no menos importante, exige la implantación de procedimientos de respaldos de información

y recuperación de datos. A continuación se enlistan los 32 controles propuestos:

- Procedimientos de operación documentados
- Gestión de cambios
- Segregación de los deberes
- Separación de los medios de desarrollo, prueba y operación
- Entrega del servicio
- Monitoreo y revisión de los servicios de terceros
- Manejo de cambios en los servicios de terceros
- Gestión de la capacidad
- Aceptación del sistema
- Controles contra códigos maliciosos
- Controles contra códigos móviles
- Respaldos o backup’s
- Controles de redes
- Seguridad de los servicios de la red
- Gestión de medios removibles
- Eliminación de medios
- Procedimientos para el manejo de información
- Seguridad de la documentación del sistemas
- Políticas y procedimientos de intercambio de información

- Acuerdos de intercambio
- Medios físicos en tránsito
- Mensajes electrónicos
- Sistemas de información comercial
- Comercio electrónico
- Transacciones en línea
- Información públicamente disponible
- Registro de auditoría
- Uso del sistema de monitoreo
- Protección del registro de información
- Registros del administrador y operador
- Registro de fallas
- Sincronización de relojes

3.1.7 Controles de acceso

En este dominio la norma se refiere al control de acceso lógico a los activos de la empresa, es decir la norma solicita una política para uso de contraseñas, cuidado y protección de medios removibles, escritorios y protectores de pantallas de los computadores. Solicita definir responsabilidades concernientes al sistema de gestión de seguridad de información en los perfiles de los puestos de trabajo. Solicita procedimientos de registro y revocación de cuentas

de usuarios, manejo de privilegios para cada usuario, manejo de contraseñas, y revisiones periódicas.

Los privilegios o niveles de seguridad deben establecer de acuerdo a las necesidades del propietario del activo y el nivel de riesgo del activo. Se presentan 25 controles:

- Política de control de acceso
- Registro del usuario
- Gestión de privilegios
- Gestión de claves secretas de los usuarios
- Revisión de los derechos de acceso del usuario
- Uso de claves secretas
- Equipo del usuario desatendido
- Política de escritorio y pantalla limpios
- Política sobre el uso de los servicios de red
- Autenticación del usuario para las conexiones externas
- Identificación del equipo en las redes
- Protección del puerto de diagnostico y configuración remoto
- Segregación en redes
- Control de conexión a la red
- Control de enrutamiento de la red

- Procedimiento para un registro seguro
- Identificación y autenticación del usuario
- Sistema de gestión de claves secretas
- Uso de las utilidades del sistema
- Cierre de una sesión por inactividad
- Limitación del tiempo de conexión.
- Restricción del acceso a la información
- Aislar el sistema confidencial
- Computación y comunicaciones móviles
- Tele-trabajo

Se observa que la norma también solicita los procedimientos para el acceso remoto y tele-trabajo y entra en los detalles de rutas y puertos TCP/UDP necesarios para estas conexiones, así como políticas para el uso de computadoras portátiles y dispositivos móviles,

3.1.8 Controles de adquisición, desarrollo y mantenimiento de sistemas de información

En este dominio la norma da las directrices para la adquisición de sistemas de información, y/o en caso de que la organización los desarrolla, presenta recomendaciones

de seguridad para el desarrollo de software entre estos el uso de controles criptográficos. Adicionalmente hace énfasis en el mantenimiento de los sistemas de información mediante el seguimiento de parches de seguridad ó herramientas de gestión de vulnerabilidades y/o actualizaciones automáticas. Se presentan 16 controles:

- Análisis y especificación de los requerimientos de seguridad
- Validación de la input data
- Control de procesamiento interno
- Integridad del mensaje
- Validación de la output data
- Política sobre el uso de controles criptográficos
- Gestión de claves
- Control de software operacional
- Protección de la data del sistema
- Control de acceso al código fuente del programa
- Procedimientos de control del cambio
- Revisión técnica de la aplicación después de cambios en el sistema
- Restricciones sobre los cambios en los paquetes de software

- Filtración de información
- Desarrollo de software abastecido externamente
- Control de la vulnerabilidades técnicas

3.1.9 Controles de gestión de incidentes de seguridad de la información

En este dominio la norma solicita a la organización el establecimiento de procedimientos para registrar y reportar los incidentes de seguridad y los problemas de seguridad. Se plantean también el análisis para la adopción de medidas correctivas. Este dominio propone 5 controles:

- Reporte de eventos en la seguridad de la información
- Reporte de las debilidades en la seguridad
- Responsabilidades y procedimientos
- Aprender de los incidentes en la seguridad de la información
- Recolección de evidencia

3.1.10 Controles de gestión de la continuidad comercial

Es uno de los dominios que la norma hace énfasis. Se busca que la organización tenga un plan de recuperación ante un desastre y que este plan le permita seguir operando en el menor tiempo posible luego del suceso. Se le pide a la organización que haga simulacros del evento que le permita evaluar el plan y corregir en caso de ser necesario. Estos simulacros deben tener cierta periodicidad. Los controles propuestos son:

- Continuidad del negocio y evaluación del riesgo
- Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información
- Marco referencial de la planeación de la continuidad del negocio
- Prueba, mantenimiento y re-evaluación de los planes de la continuidad del negocio.

3.1.11 Controles de conformidad

En este dominio la norma propone controles para evitar las violaciones a las leyes vigentes incluyendo el uso de

criptografía. Pone énfasis en la legalidad del uso de los sistemas de información, respecto a la propiedad intelectual de los mismos para evitar algún tipo de piratería informática. Adicionalmente da directrices para evitar que las herramientas de auditoría a los sistemas de información produzcan eventos que atenten contra el sistema de gestión. Los controles son:

- Identificación de la legislación aplicable
- Derechos de propiedad intelectual (IPR)
- Protección de registros organizacionales
- Protección de la data y privacidad de la información personal
- Prevención del mal uso de los medios de procesamiento de la información
- Regulación de controles criptográficos
- Cumplimiento con las políticas y estándares de seguridad
- Chequeo del cumplimiento técnico
- Controles de auditoría de los sistemas de información
- Protección de las herramientas de auditoría de los sistemas de información.

3.1.12 Establecimiento de los controles

La práctica internacional considera obligatorio y común en todo sistema de gestión de la seguridad de la información el establecimiento de un subconjunto de los 133 controles:

- Documento de la política de la seguridad de la información (5.1.1)
- Asignación de las responsabilidades de la seguridad de la información (6.1.3)
- Conocimientos, educación y capacitación en la seguridad de la información (8.2.2)
- Procesamiento correcto de las aplicaciones (12.2)
- Gestión de vulnerabilidad técnica (12.6)
- Gestión de continuidad comercial (14)
- Gestión de incidentes y mejoras de la seguridad de la información (13.2) (5).

La definición de los controles adicionales para este sistema de gestión de la seguridad de la información se presentara en las siguientes secciones.

3.2 Relación entre la reducción del riesgo y la implementación de controles

En el apartado anterior se presenta de manera breve los 133 controles propuestos por el estándar, algunos de ellos son redundantes, otros no tan efectivos. Como se ha presentado anteriormente la gerencia debe tomar la decisión de que controles implementar y cuales dejar a un lado e inclusive si es necesario, la organización puede implementar sus propios controles.

La implementación de controles se relaciona con el riesgo estimado en dos maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenazas
- Reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados, reaccionando y recuperándose de ellos [6].

La gerencia debe adoptar cuál de estas maneras o una combinación de ambas usará para tomar la decisión de que controles implementar, ya que algunos de ellos están enfocados a la reducción de vulnerabilidades y otros enfocados a la reacción ante eventos. Esta es una decisión que generalmente se reduce a motivos comerciales y del giro del negocio.

Sin embargo no existe un método universal para escoger los controles, esto es algo que envuelve numerosas decisiones y consultas, discusiones con todas y cada una de los departamentos de la organización y muchas veces con personal clave, específicamente los dueños de los Activos y el Gerente del Departamento de Gestión de Seguridad de la Información.

Los controles seleccionados por lo general reflejan la cultura organizacional de la empresa, sus activos, sus inversiones y su tolerancia al riesgo, y cada empresa es una entidad muy compleja inclusive dentro del mismo sector de las telecomunicaciones, es decir, los enfoques usados por un proveedor de comunicaciones móviles, pueden ser muy distintos a los utilizados por un proveedor de comunicaciones fijo.

3.3 Aceptación y traspaso del riesgo

Cuando la implementación de controles lleva a la organización a incurrir en costos superiores a los efectos producidos por amenazas concretadas, entonces la organización puede tomar dos posturas:

- Aceptar el riesgo
- Transferir el riesgo a un tercero

La forma más común para el traspaso del riesgo es la utilización de seguros. La organización debe tomar en cuenta las exclusiones y condiciones que ponen las entidades aseguradoras al momento de tomar la decisión de transferir el riesgo.

Otra práctica común es la tercerización de ciertos procesos críticos de la organización para transferir el riesgo aunque la responsabilidad por la seguridad de la información siempre corresponde a la organización original.

En ambos casos, se debe tomar en cuenta el riesgo residual el cual es el riesgo remanente luego de haber realizado el plan de tratamiento teórico, es decir, según la norma, este riesgo debe ser considerado en el primer ejercicio de implantación del sistema de gestión, por lo tanto es un riesgo teórico.

En el caso que el riesgo residual sea considerado inaceptable, se debe volver a realizar el ejercicio de tratamiento del riesgo para tomar una decisión de aceptación o transferencia la cual debe estar documentada.

Ya sea que la organización decida aceptar o transferir el riesgo, esta decisión debe documentarse y definirse claramente para cumplir con las cláusulas 4.2.1(c) (2) y 5.1(f) de la norma ISO 27001:2005, adicionalmente la gerencia debe firmar la aprobación de la decisión tomada.

Para el caso de este proveedor de servicios, la gerencia ha decido por una enfoque combinado entre la reducción de las vulnerabilidades y mejorar la capacidad reactiva en caso de que las amenazas se concreten, para esto todos los controles serán seleccionados bajo el criterio de reducción del riesgo y no de transferencia y/o aceptación del mismo.

3.4 Selección y justificación de los controles

Como se indicó anteriormente existen 133 controles presentados, sin embargo luego del análisis de riesgos, al plantearse el tratamiento del riesgo, este proveedor escogerá los controles basado en los siguientes enfoques:

- Del tratamiento del riesgo, orientados a eliminar vulnerabilidades o minimizar el impactos.
- Los requerimientos legales

- Producto de las operaciones en el negocio de la compañía.

El primer enfoque muestra a este proveedor de servicios tomando acciones para corregir vulnerabilidades encontradas en los procesos a ser certificados.

Respecto a los requerimientos legales estipulados en los controles, se implementarán todos los necesarios para los tres procesos. Finalmente se implementarán los controles enfocados a la reacción y reducción de pérdidas económicas y de imagen producida por eventos de seguridad de la información, aun cuando no estén explícitamente indicados en la lista de 133 controles.

Se llega entonces a presentar el cuadro donde converge todo el análisis y las decisiones tomadas respecto a los controles. Se identifican primeramente las vulnerabilidades y los riesgos en orden de prioridad y los controles del apéndice A del estándar ISO 27001 usados según el enfoque de eliminar vulnerabilidad, minimizar el impacto o de ámbito legal. Esto se presenta en el Anexo 9.

Adicionalmente el estándar requiere que la organización cuente con la declaración de aplicabilidad, este es un documento donde se identifican los controles del anexo A de la norma y se justifican los motivos en los que los controles no serán aplicados.

Dicho de otra manera la norma indica que todos sus controles si son aplicables a una organización y que las excepciones deben ser claramente justificadas. Esta Declaración de aplicabilidad debe ser revisada, aprobada y firmada por Presidencia de la Organización ó la Gerencia General de la misma. El formato de la declaración de aplicabilidad se presenta en el siguiente cuadro:

Tabla 9. Encabezado de la Declaración de la Aplicabilidad.

OBJETIVO DEL CONTROL	CONTROL	APLICA SI/NO	JUSTIFICACIÓN EN CASO DE NO APLICAR

3.5 Registro de incidentes

Uno de los elementos esenciales del sistema de gestión de seguridad de información es la gestión de los incidentes de seguridad. Este proveedor de servicios define un incidente de seguridad a todo evento que viole o amenace los a los activos protegidos por los controles definidos. Es decir cuando la amenaza explota la vulnerabilidad y se materializa en un evento que cause una afectación sobre los activos, entonces se presenta un incidente de seguridad.

A continuación se presenta ciertos ejemplos de incidentes de seguridad:

- Un acceso no autorizado a sistemas de la organización.
- El robo de credenciales y/o contraseñas.
- Prácticas de Ingeniería Social.
- El abuso y/o mal uso de los sistemas y servicios internos o externos de una organización.
- La introducción de código malicioso en la infraestructura tecnológica de una entidad (virus, troyanos, gusanos, malware en general).
- La denegación del servicio o eventos que ocasionen pérdidas, tiempos de respuesta no aceptables o no cumplimiento de acuerdos de niveles de servicio existentes de determinado servicio.

Los controles en la sección 13 de la norma ISO 27002 respecto a la gestión de incidentes de seguridad se enfocan en el reporte no solo de las incidencias de seguridad sino también de los eventos, reporte de las debilidades en la seguridad. Además los controles definen las responsabilidades, procedimientos, aprendizaje es decir la creación de una base de conocimientos, y finalmente la recolección de toda evidencia

Este proveedor de servicios implementa un departamento para responder ante estos incidentes: CERT (Computer Emergency Response Team) con la finalidad de cumplir con los controles de la sección 13 de la norma ISO 27002.

En este proveedor de servicios, el departamento de CERT tiene las siguientes funciones:

- Ayudar a todos los colaboradores de la empresa a atenuar y prevenir incidentes graves de seguridad.
- Difundir la cultura de seguridad informática y crear medios de difusión para este fin.
- Verificar el cumplimiento de los controles implementados.
- Verificar la existencia de nuevas vulnerabilidades para los activos.
- Verificar la existencia de nuevas amenazas para los activos.
- Coordinar de forma centralizada al SGSI.

- Guardar evidencias, en caso que se requiera recurrir a demandas.
- Apoyar y prestar asistencia a usuarios para recuperarse de las consecuencias de los incidentes de seguridad.
- Dirigir de forma centralizada la respuesta a los incidentes de seguridad.

CERT tiene herramientas de software para realizar esta tarea:

- Recepción de reportes de ataques por parte de los equipos de los clientes con direccionamiento público a servidores en Internet.
- Plataforma de prevención de intrusos la cual detecta comportamientos anómalos de los equipos con direccionamiento público, especialmente trafico saliente a internet en el puerto de envió de correo electrónico SMTP que utiliza el puerto 25 TCP. Además esta plataforma verifica puertos TCP muy conocidos como telnet que utiliza el puerto TCP 23, SSH que utiliza el puerto TCP 22.
- Plataforma para registro del seguimiento de las incidencias de seguridad, la cual es accesible vía Web por parte del departamento del NOC, quien recibe las notificaciones y tiene la función de registrarlas en la plataforma indicada y notificar a los administradores de los equipos CPE, que en este caso es el

departamento de soporte corporativo para que procedan a tomar acciones para bloquear dicho trafico utilizando listas de control de acceso (ACL).

- Herramientas de monitoreo del ancho de banda de los enlaces de los clientes y de los enlaces de la red troncal así como de las salidas internacionales a Internet a través de los proveedores como TGS, Sprint, etc. La revisión de estas graficas de ancho de banda por parte del departamento del NOC permite correlacionar la presencia de un evento y/o posible incidente de seguridad.

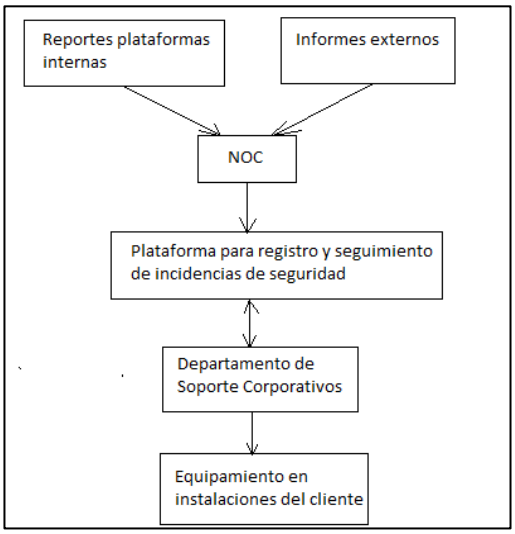


Figura 3.1 Registro y Seguimiento de incidencias de seguridad

CAPÍTULO 4

AUDITORÍAS INTERNAS, MONITOREO, MEJORA CONTINUA Y CERTIFICACIÓN

En el capítulo anterior se definieron e implementaron los controles. Ahora en este capítulo se presentan los mecanismos de revisión de todo el sistema a través de auditorías internas primeramente, las que generaran observaciones y no conformidades que permiten la mejora continua previa a la certificación.

4.1 Definición del proceso de auditoría

Antes de empezar, se define auditoría como el trabajo del auditor. La palabra auditor proviene del latín “audire”, es decir, oír.

Inicialmente personas externas eran contratadas para oír los informes de las organizaciones y luego definir si lo que escuchaban era falso o no.

"La auditoría es, el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado" [7].

Como se puede leer, existen características claves en la definición:

- Independencia del sistema auditado
- Examen sistemático, es decir que es un sistema que posee procesos
- Examen crítico, es decir que los resultados son un juicio para el sistema auditado.

ISO publicó la primera guía para auditoría de sistemas de gestión de calidad y/o ambientales, el estándar ISO 19011:2002. Sin embargo si las organizaciones desean realizar auditorías internas ó externas al sistema de gestión de la seguridad de la información

conforme al estándar ISO 27001:2005, entonces deben considerar aspectos adicionales del nuevo estándar ISO 27007:2011 guía para auditar sistemas de gestión de seguridad de información. Este nuevo estándar estuvo en desarrollo mientras se implementó el sistema de gestión de seguridad de la información de este proveedor de servicios, por lo tanto se tomó en consideración los aspectos generales indicados en el estándar de ISO 19011:2002.

4.1.1 Los elementos, principios y clases de auditoría

El estándar ISO 19011 en la sección de definiciones presenta los elementos en el sistema:

- Auditoría
- Auditado
- Auditor
- Equipo auditor
- Experto técnico
- Criterios de auditoría
- Programa
- Plan
- Alcance
- Evidencia de auditoría

- Hallazgos de auditoría
- Conclusiones de auditoría
- Competencia

Luego el estándar presenta los principios necesarios para que la auditoría sea un elemento útil para el establecimiento y mejora de los sistemas de gestión. Separa los estos principios o valores los presenta respecto a los auditores y respecto a la auditoría misma

Respecto a los auditores:

a) Conducta ética: el fundamento de la profesionalidad. La confianza, integridad, confidencialidad y discreción son esenciales para auditar.

b) Presentación ecuánime: la obligación de informar con veracidad y exactitud. Los hallazgos, conclusiones e informes de la auditoría reflejan con veracidad y exactitud las actividades de la auditoría. Se informa de los obstáculos significativos encontrados durante la auditoría y de las opiniones divergentes sin resolver entre el equipo auditor y el auditado.

c) Debido cuidado profesional: la aplicación de diligencia y juicio al auditar.

Los auditores proceden de acuerdo con la importancia de la tarea que desempeñan y la confianza depositada en ellos por el cliente de la auditoría y por otras partes interesadas. Un factor importante es tener la competencia necesaria.

En referencia a la auditoría misma:

d) Independencia: la base para la imparcialidad de la auditoría y la objetividad de las conclusiones de la auditoría. Los auditores son independientes de la actividad que es auditada y están libres de sesgo y conflicto de intereses. Los auditores mantienen una actitud objetiva a lo largo del proceso de auditoría para asegurarse de que los hallazgos y conclusiones de la auditoría estarán basados sólo en la evidencia de la auditoría.

e) Enfoque basado en la evidencia: el método racional para alcanzar conclusiones de las auditorías fiables y reproducibles en un proceso de auditoría sistemático. La evidencia de la auditoría es verificable. Está basada en muestras de la

información disponible, ya que una auditoría se lleva a cabo durante un período de tiempo delimitado y con recursos finitos. El uso apropiado del muestreo está estrechamente relacionado con la confianza que puede depositarse en las conclusiones de la auditoría.

Se presentan las siguientes clases auditorías:

a) Internas para cubrir el sistema de gestión de la calidad en toda la organización para el año en curso;

b) las auditorías de segunda parte al sistema de gestión de los proveedores potenciales de productos críticos que se van a realizar en un período de seis meses;

c) las auditorías para otorgar y mantener la certificación/registro llevadas a cabo por un organismo de certificación registro de tercera parte sobre un sistema de gestión ambiental dentro de un período de tiempo acordado contractualmente entre el organismo de certificación y el cliente.

Un programa de auditoría también incluye la planificación, la provisión de recursos y el establecimiento de procedimientos apropiados para realizar las auditorías dentro del programa.

4.1.2 Gestión del proceso de auditoría

La gestión del proceso de auditoría presentado por el estándar ISO 19011 está basada en modelo Planear-Hacer-Verificar-Actuar. De esta manera, se permite una mejora continua en el mismo proceso de auditoría, lo que le permite a la empresa realizar cada vez mejoras auditorías internas.

En este proveedor, ya se cuenta de antemano una Gerencia de Gestión de la Calidad, y entre sus funciones está la gestión de las auditorías internas. Para esto se preparó a personal de cada departamento mediante capacitaciones para auditores internos. La empresa usará el mismo esquema de auditorías internas sin embargo para la gestión de la seguridad de información se ha definido trabajar con otro grupo de personas las cuales también fueron capacitadas.

No es objetivo de este capítulo ahondar en todas las actividades de gestión de un proceso de auditoría, sin embargo se presenta la propuesta del estándar ISO 19011 en el siguiente gráfico:

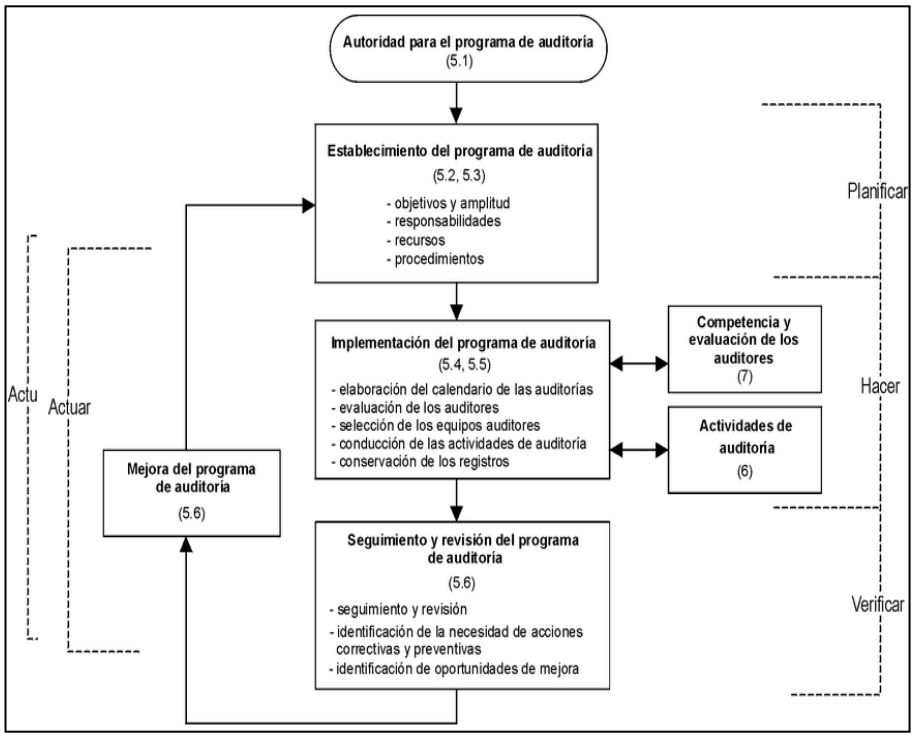


Figura 4.1 Diagrama de flujo para la gestión de un proceso de auditoría [8]

Se puede observar claramente las distintas etapas según el modelo Planear-Hacer-Verificar-Actuar.

La etapa de establecimiento del programa de auditoría es una de las etapas claves en la gestión, debido a que en esta se define el alcance del programa, el encargado o encargados de la gestión completa del proceso, los recursos y procedimientos.

La Presidencia de este proveedor asignó los recursos necesarios y creó más que una Jefatura, dos Gerencias: una para el sistema de Gestión de Calidad, y otra para la Gestión de la Seguridad de Información, ambas tienen entre sus responsabilidades la gestión del proceso de auditoría.

La etapa de implementación fue realizada por este proveedor con la capacitación de personal seleccionado de cada departamento en los procedimientos de auditorías internas.

El seguimiento es realizado por las gerencias arriba mencionadas, adicionalmente este proveedor utiliza el mecanismo de bonos los cuales son acreditados a los integrantes de cada departamento cuando se cumplen las metas y correcciones solicitadas por las auditorías internas.

4.1.3 Preparación de la auditoría y diagrama de árbol

El auditor al preparar la auditoría debe considerar los siguientes aspectos:

- Objetivos y alcances
- Criterio a utilizar
- Conocimiento de la unidad o departamento a auditar.
- Procedimiento creado en base al criterio a utilizar
- Matriz de planificación
- Plan de auditoría
- Listas de chequeo
- Comunicación previa a la auditoría

El criterio a utilizar debe ser el enfoque a procesos ya que son los procesos de este proveedor de servicios los que van a ser certificados. El auditor debe verificar que los procesos estén operando respecto a los límites propuestos. Se debe examinar los insumos, acciones y resultados y verificar que estos estén en armonía con los requerimientos definidos.

El conocimiento del proceso y por ende el conocimiento de las acciones en que participa el departamento a auditar

dentro del proceso es un elemento de suma importancia para poder implementar el procedimiento a ser utilizado.

Dentro de la implementación de este procedimiento, una herramienta muy popular es el diagrama de árbol, el cual es utilizado para preparar las preguntas que se realizarán durante la auditoría.

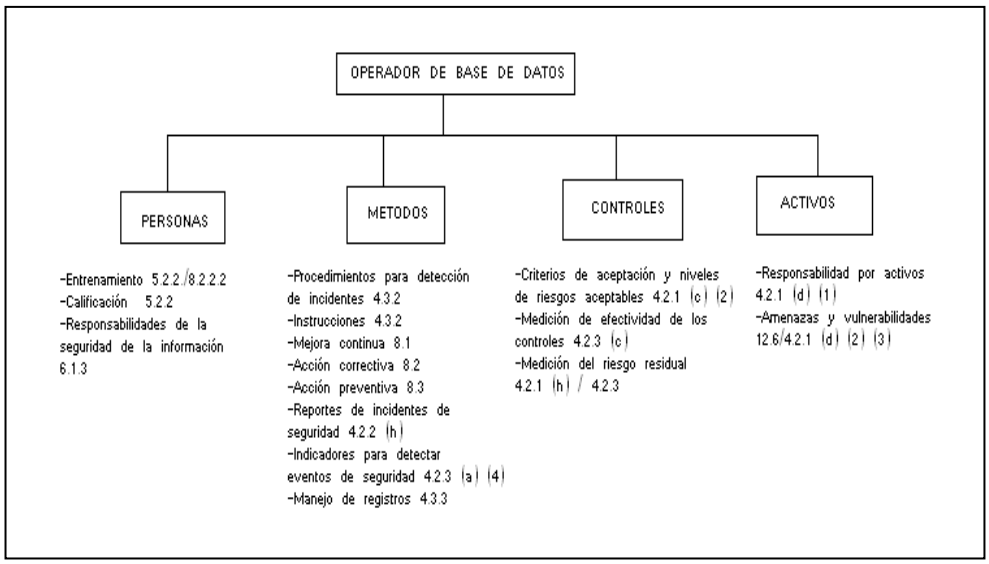


Figura 4.2 Ejemplo de Diagrama de árbol

4.1.4 Plan de auditoría y listas de chequeo

El auditor líder es quien prepara el plan de auditoría. Debe colocar los procesos que van a ser auditados y las fechas en que se realizarán los chequeos. Este plan debe ser verificado por el cliente y aprobado por el mismo. El plan no debe ser

rígido y debe permitir modificaciones en caso de que el cliente las solicite.

En detalle el plan de auditoría debe tener los siguientes ítems:

- Objetivos de auditoría
- Alcance de auditoría
- Documentos de referencia que se usarán durante la auditoría
- Integrantes del equipo auditor
- Departamentos de la empresa a ser auditados
- Fecha exacta en que se auditarán los departamentos
- Tiempo esperado de duración de la actividad de auditoría

Respecto a las listas de chequeo, estas son la guía que auditor tiene para registrar las observaciones más relevantes y evidencias objetivas.

Las listas de chequeo evitan pérdidas de tiempo ya que no se basan solo en la memoria del auditor. Adicionalmente permiten visualizar con antelación si es necesaria la presencia de expertos del proceso.

ISO IEC propone el estándar ISO 27006: Requerimientos para organizaciones proveedores de auditoría y certificación de sistemas de gestión de seguridad de la información específicamente el Anexo D: Guía para revisión de controles del Anexo A del ISO/IEC 27001:2005, como la mejor herramienta para auditorías internas y externas de un sistema de Gestión de la Seguridad de la Información.

Este anexo se convierte en la base para la creación de las listas de chequeo que serán utilizadas por el auditor.

4.1.5 Recopilación y verificación de la información

El auditor durante las entrevistas pactadas con las jefaturas y/o administradores de los activos, observación de las actividades debe recolectar las evidencias de que los procesos están alineados con los requerimientos de la norma.

Las evidencia debe ser información que pueda ser verificable, debe ser información que debe estar registrada en medios físicos y/o electrónicos.

Debido a que la evidencia de la auditoría se basa en muestras de la información disponible, se genera un cierto grado incertidumbre en la auditoría, y aquéllos que actúan sobre las conclusiones de la auditoría deberían ser conscientes de esta incertidumbre.

La siguiente figura muestra el proceso desde la recopilación de la información hasta las conclusiones de la auditoría.

Figura 4.3 Recopilación y conclusiones de auditoría [9]

4.1.6 Informe de auditoría

El informe de la auditoría debería proporcionar un registro completo de la auditoría. El líder del equipo auditor es el responsable de la preparación y del contenido del informe.

Según el estándar ISO 19011. El informe deberá incluir lo siguiente:

- los objetivos de la auditoría;
- el alcance de la auditoría, particularmente la identificación de las unidades de la organización y de las unidades funcionales o los procesos auditados y el intervalo de tiempo cubierto;
- la identificación del cliente de la auditoría;
- la identificación del líder del equipo auditor y de los miembros del equipo auditor;
- las fechas y los lugares donde se realizaron las actividades de auditoría in situ;
- los criterios de auditoría;
- los hallazgos de la auditoría; y
- las conclusiones de la auditoría.
- el plan de auditoría;
- una lista de representantes del auditado;
- un resumen del proceso de auditoría, incluyendo la incertidumbre y/o cualquier obstáculo encontrado

que pudiera disminuir la confianza en las conclusiones de la auditoría;

- la confirmación de que se han cumplido los objetivos de la auditoría dentro del alcance de la auditoría, de acuerdo con el plan de auditoría;
- las áreas no cubiertas, aunque se encuentren dentro del alcance de la auditoría;
- las opiniones divergentes sin resolver entre el equipo auditor y el auditado;
- las recomendaciones para la mejora, si se especificó en los objetivos de la auditoría;
- los planes de acción del seguimiento acordados, si los hubiera;
- una declaración sobre la naturaleza confidencial de los contenidos
- la lista de distribución del informe de la auditoría.

El informe debe ser emitido y distribuido en la fecha planificada a los receptores autorizados por el cliente, en caso de retrasos se deben comunicarse. El informe es de

propiedad del cliente auditado y se debe mantener la confidencialidad del mismo.

4.1.7 Observaciones, no conformidades y oportunidades de mejora

El auditor puede notar malas prácticas las cuales pueden aumentar vulnerabilidades sin embargo no violan ninguno de los requerimientos del sistema de gestión. Estas malas prácticas deben ser reportadas como observaciones.

La no conformidad es una condición que viola un requerimiento indicado en la norma o aun procedimiento del auditado. Para poder determinar la existencia de una no conformidad es necesaria la existencia previa de una evidencia objetiva de la violación de los requerimientos. Se tienen dos tipos de no conformidades:

- No conformidad mayor, generan una ruptura critica del sistema
- No conformidad menor la cuales son la acumulación de deficiencias similares

La oportunidad de mejora es una acción recomendada luego de la auditoría que al ser implementada implica una mejora del sistema de gestión de la seguridad de la información.

4.2 Elaboración del manual de seguridad de la empresa

En su afán de ayudar a las empresas en su tarea de implementar sistemas de gestión de la seguridad de la información, ISO a través de su estándar ISO 27003: Guía para implementación del sistema de gestión de la seguridad de la información; provee una serie de lineamientos generales encaminados a facilitar las distintas etapas de la implementación: valoración de activos, análisis de riesgos, selección de controles, y documentación de políticas. En este apartado, se hace uso del Anexo D de este estándar para poder desarrollar el manual de seguridad para este proveedor de servicios de telecomunicaciones.

El Anexo D del estándar ISO 27003, a través del siguiente gráfico, ilustra el esquema jerárquico que deben tener las políticas de seguridad de la información.

Figura 4.4 Jerarquía de las políticas [10]

Se observan primeramente los Reglamentos o políticas Generales, luego las políticas por específicas por tópico y finalmente las políticas detalladas para cada tópico de seguridad.

El manual de seguridad de la información es el documento de políticas de alto nivel generales, respecto a las distintas áreas de la seguridad de la información. En este manual se encuentran declaradas la política de seguridad de la empresa, la política de privacidad, la política de mercadeo, la política de desarrollo.

Para poder implementar el manual de seguridad, el estándar nos da los siguientes lineamientos generales para la implementación de políticas:

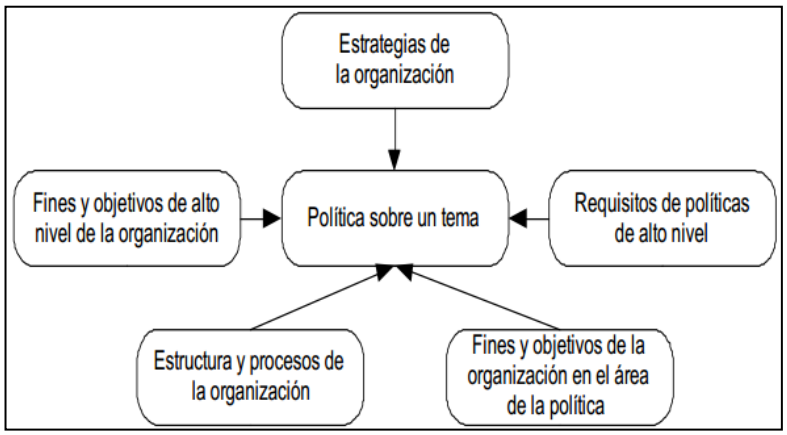


Figura 4.5 Entradas para el desarrollo de una política [11]

Se observa que cualquier política a ser implementada debe estar alineada con la estrategia económica de la empresa, con los objetivos de la misma. Debe tomar en cuenta la estructura organizacional de la misma con la finalidad de asignación de responsabilidades, y finalmente los objetivos específicos de la empresa en el área de aplicación de la política a ser desarrollada.

Según el estándar ISO 27003, las políticas pueden tener la siguiente estructura:

- Sumario o resumen de la política

- Introducción
- Alcance
- Objetivos
- Principios
- Responsabilidades
- Resultados relevantes
- Relación con otras políticas

A continuación la política general de Seguridad de la Información de este proveedor de servicios apegada a los lineamientos del estándar ISO 27003

Resumen de la Política:

“Proveer servicios de telecomunicaciones disminuyendo el riesgo de incidencias que atenten contra la disponibilidad, integridad y confidencialidad de la infraestructura, a través un sistema de gestión de la seguridad de la información fundamentado en la prevención”

Introducción:

Los servicios de transporte de datos y acceso a Internet para medianas y grandes empres en Ecuador es la principal actividad de la empresa. Brindar a los clientes este servicio con alta disponibilidad, integridad, y confidencialidad, es un valor agregado diferenciador en el mercado.

Alcance:

La siguiente política es la política general de seguridad de la información de la empresa y debe ser de conocimiento y cumplimiento de todos los colaboradores.

Objetivos:

Aumentar la disponibilidad de los servicios brindados, disminuyendo el porcentaje de notas de crédito, generadas por el no cumplimiento del SLA ofrecido.

Proveer servicios de transporte de datos e Internet formando al 80% de los empleados en las áreas de: buenas prácticas de

seguridad de información, y análisis de causalidad de incidentes de seguridad, además se implementan los sistemas informáticos para disminuir la carga operativa generada.

Principios:

Todos los colaboradores deberán estar en conocimiento de la importancia de la seguridad de la información y buenas prácticas como parte de su rol laboral.

Se provisionará los sistemas necesarios para la implementación de controles para los procesos de mantenimiento, control de cambios y aprovisionamiento.

Se elabora un sistema de reportes de incidentes de seguridad de la información.

Las acciones que pongan a la organización en contra de disposiciones legales de seguridad de la información no serán toleradas en ninguna forma.

Se clasifica la información y se trata los riesgos alineándolos a los detalles de la política del sistema de gestión de la seguridad de la información.

Responsabilidades:

Las revisiones y actualizaciones de esta política tendrán una periodicidad anual por parte del comité de seguridad o en su defecto en caso de cambios en uno de los objetivos dentro del giro del negocio de la empresa.

Es la gerencia general quien aprueba la política general. La gerencia general apoya activamente la seguridad de la información dentro de la organización

La gerencia general destinará del presupuesto general, rubros para la implementación de proyectos que contribuyan a mejorar la seguridad de la información.

Los Jefes Departamentales tienen la responsabilidad de coordinar y organizar las actividades respecto al sistema de gestión: preparación previas a las auditorías, manejo, reporte y tratamiento de incidencias, capacitación, documentación, diagramas, registro de mantenimientos, acciones correctivas y preventivas, revisión y corrección de procesos interdepartamentales, implementación y revisión de controles, medición de indicadores asignados a estos controles. El departamento de seguridad lógica colabora con las

jefaturas para la correcta ejecución de las actividades arriba descritas.

Resultados esperados:

1. Los incidentes de seguridad no se conformarán en costos y/o disrupciones de nuestras actividades económicas
2. Los servicios y las tareas operativas no serán afectadas adversamente por la implementación del sistema de gestión de seguridad de la información, sino más bien, el SLA en los servicios se mantendrá estable en los niveles contratados y la carga operativa será alivianada con la automatización de un conjunto de ellas.

4.3 Establecimiento de los registros y documentación que va a contener el sistema de gestión de la seguridad de la información según la norma ISO 27001:2005

En esta sección se desarrollan las políticas de alto nivel además de los procedimientos y registros del sistema de gestión de seguridad de la información de este proveedor.

4.3.1 Políticas de alto nivel

Según el anexo D del estándar ISO 27003 de manera informativa las políticas de alto nivel son:

1. Política del sistema de gestión de la seguridad de la información
2. Política del manejo de la información
3. Política respecto de la Gestión de Activos
4. Política respecto a los Recursos Humanos
5. Política respecto a la seguridad física, ambiental, de instalaciones y manejo de equipamiento
6. Política respecto al cableado de redes
7. Política respecto al mantenimiento de equipos
8. Política respecto a la seguridad de equipos fuera de las instalaciones de la organización
9. Política respecto a la seguridad en la reutilización o eliminación de equipos
10. Política de retiro de la propiedad
11. Política de gestión de comunicaciones y operaciones
12. Política de Gestión de cambios
13. Política de tratamiento, monitoreo y entrega de servicio de terceras partes.

14. Política de la gestión de la capacidad
15. Política de aceptación del sistema
16. Política de Documentación de sistemas
17. Política de sistema de información
18. Políticas de control de accesos
19. Políticas de gestión de contraseñas
20. Política de procedimientos de conexión segura
21. Política respecto a comunicaciones y tele trabajo
22. Política respecto al análisis y especificación de los requisitos de seguridad.
23. Políticas respecto al procesamiento correcto de las aplicaciones y código fuente.
24. Política de gestión de incidencias de seguridad de la información.
25. Política respecto a compra de equipos y/o sistemas.
26. Política del plan de continuidad del negocio.
27. Política respecto a la verificación del cumplimiento.

En el Anexo 10 se detallan las políticas de alto nivel de este proveedor de servicios [12]. Adicionalmente, debido al giro del negocio, este proveedor ha implementado una serie de políticas particulares adicionales.

La identificación de los documentos de las políticas dentro del sistema se hace utilizando los prefijos POL SEC seguido del número de política. La política general está identificada como POL SEC 01 y las demás políticas según lo detallado a continuación:

- POL SEC 02: Política de Seguridad para manejo de incidentes con clientes.
- POL SEC 03: Política de manejo de información
- POL SEC 04: Política de trabajo a distancia
- POL SEC 05: Política de uso de medios criptográficos
- POL SEC 06: Política de equipamiento de laboratorio

En los Anexos 11 al 15 se presentan el contenido de las políticas adicionales de este proveedor.

4.3.2 Procedimientos específicos

Este proveedor regula los procedimientos que deben ser realizados por los administradores de los activos y/o el personal en general para el tratamiento de los activos acorde a los controles seleccionados para ser implementados. Estos documentos de procedimientos son identificados por los prefijos INS SEC seguido del número de instructivo. A continuación se enlistan los instructivos:

- Failover del Sistema de Prevención de Intrusos
- Bloqueo a nivel de red de acceso
- Uso del correo electrónico
- Uso de computadora asignada
- Contramedidas para ingeniería social
- Configuración del programa cliente VPN para conexiones remotas
- Almacenamiento para información encriptada.
- Encriptación para mensajería instantánea
- Manejo de archivos encriptados con Filecript
- Cambio de políticas en la red inalámbrica corporativa
- Detección de ataques DDoS con el sistema de detección de intrusos.
- Detección de ataques DDoS con capturas de puertos de switches en modo mirror y Wireshark.
- Identificación de unicast flooding y Broadcast
- Soluciones de Caching de Video

Los procedimientos arriba mencionados son específicos para las plataformas de seguridad, hardware y software de este proveedor por lo que no se adjuntará el contenido de los mismos.

4.3.3 Plan de Continuidad del Negocio

El Plan de Continuidad del Negocio, cuyas siglas en inglés son BCP (Business Continuity Plan) es una de los requisitos del estándar para lograr la disponibilidad de la información, la cual es uno de los pilares de la seguridad lógica.

En todo sistema la disponibilidad de la información en caso de fallos se logra con esquemas de redundancia de equipamiento y de procesos.

Sin embargo el equipamiento y procesos solo pueden ser eficaces si el personal operativo puede ejecutarlos correctamente. Por este motivo se realizan simulacros de fallos de sistemas para poder operar utilizando los sistemas alternos. Esto se logra gracias a la georedundancia de las plataformas críticas para la operación de este proveedor. Los activos críticos de este proveedor ligados al plan de continuidad del negocio son:

- Sistema de gestión de incidencias
- Tareas operativas de seguridad física y lógica
- Servicios de red interna como telefonía IP, correo electrónico, impresoras.
- Plataformas de Prevención de Intrusos a nivel perimetral.

- Plataformas de seguridad en la DMZ del proveedor que albergar sitios Web, ftp y servidores DNS's.

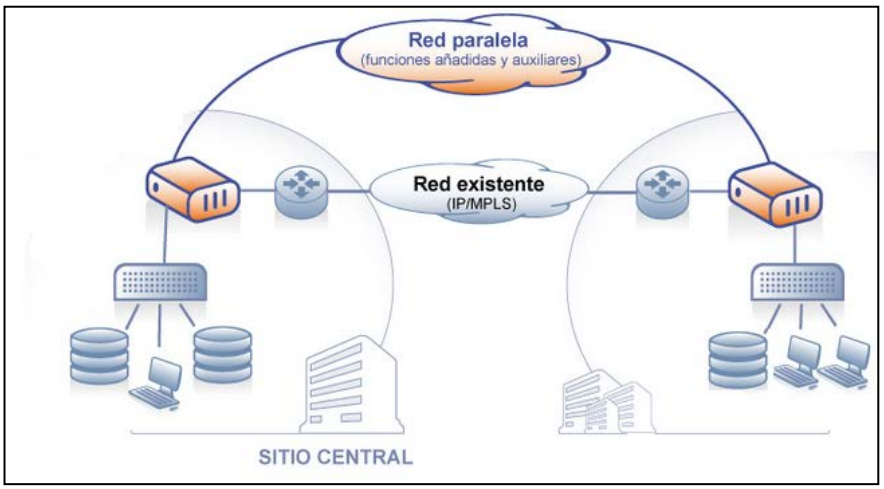


Figura 4.6 Esquema básico para alta disponibilidad

La figura muestra un esquema básico donde se vislumbra la necesidad de un centro de datos alterno para lograr la georedundancia. El centro de datos alterno contendrá los equipos de respaldo. Sin embargo esto no significa que el equipamiento del centro de datos alterno no estará en producción, sino que está sirviendo a los usuarios de la sucursal mayor regional y en caso que el centro de datos en la Matriz presenten fallos y queden fuera de servicio, los equipos alternos asumirán la carga. Por esto, es importante que el diseño de alta disponibilidad tome en cuenta el

dimensionamiento de carga para soportar no solo las operaciones locales sino las operaciones totales de la empresa.

Con una periodicidad trimestral este proveedor a través de su departamento de NOC y Soporte Corporativo ejecutan actividades de simulacro para poner a prueba el plan de continuidad del negocio.

El departamento del NOC ejecuta el procedimiento de failover desactivando puertos de la red de transporte para verificar la correcta conmutación por los caminos alternos en capa 2, que debe ser realizada el protocolo de STP.

Cabe señalar que previamente el costo asociado a las interfaces de red en los switches ya ha sido configurado y el procedimiento de failover en general ha sido diseñado por el departamento de Networking e Ingeniería de este proveedor.

Como se indicó anteriormente, el departamento de Soporte Corporativo también es un elemento activo y ejecuta el plan de continuidad para servicios de correo y telefonía IP de la red interna.

En caso de fallos en las plataformas de correo electrónico y telefonía IP, el empleado debe:

- Configurar su cuenta de correo colocando los nombres de dominio de los servidores alternos SMTP y POP3
- Configurar su cuenta de SIP phone colocando el nombre de dominio del servidor SIP alterno, además de su respectivo usuario y clave.

Como pre requisitos para estas acciones, el operador debe disponer de su computador personal o portátil y conexión fija y/o inalámbrica a la red local.

Con estas tareas, este proveedor mantiene su plan de continuidad del negocio no solo como un procedimiento registrado sino como una práctica entre sus empleados, lo que le permite reaccionar de manera ágil ante un evento disruptivo.

4.3.4 Re certificación y sostenibilidad

Debido a los constantes cambios tecnológicos y aparición de nuevas amenazas, los estándares evolucionan como respuesta a estos nuevos escenarios tecnológicos. ISO no es la excepción y por este motivo a finales de 2013 se lanzó la nueva versión del estándar certificable.

La empresas que están por terminan su proceso con el estándar anterior ISO 27001:2005 puede solicitar la auditoría hasta Octubre

de 2014. Luego de Marzo de 2015 ya no se emitirán más certificaciones bajo el estándar ISO 27001:2005.

Las empresas que ya están certificadas bajo la norma ISO 27001:2005 tendrán que realizar la migración de su sistema de gestión bajo las normas del nuevo estándar ISO 27001:2013 hasta el 01 de Octubre de 2015.

La re certificación y la sostenibilidad del sistema de gestión de seguridad de este proveedor está fundamentada principalmente en el compromiso de los altos directivos al considerarlo como un elemento diferenciador de la competencia, y a nivel técnico, de la labor del Departamento de Seguridad Lógica, que es el llamado a coordinar en conjunto con las Jefaturas del mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

4.3.5 Revisión preliminar de la migración a ISO 27001:2013

Este proveedor ya se está preparando para modificar su sistema de gestión con la finalidad de cumplir los requerimientos del nuevo estándar. Esto no significa que todos los controles enlistados en el Anexo A deban ser reemplazados por unos nuevos, es más ahora

son se tienen 11 secciones en lugar de 14, y 114 controles en lugar de los 133 controles de la norma ISO 27001:2005.

La mayoría de controles anteriores se mantienen se han eliminado algunos y se han agregado los siguientes controles nuevos:

- Seguridad de la información en la gestión de proyectos(A.6.1.5)
- Política de desarrollo seguro (A.14.2.1)
- Principios de construcción de los sistemas seguros (A.14.2.6)
- Pruebas de seguridad de sistemas (A.14.2.8)
- Evaluación de eventos de seguridad y decisiones sobre ellos (A.16.1.4)
- Disponibilidad de instalaciones de procesamiento de información (A.17.2.1)

Otro cambio importante es la aparición del concepto de "dueño del riesgo", ahora la empresa no debe enfocarse en identificar a los dueños de los activos sino que el estándar va más allá al asignar responsables para los riesgos y vulnerabilidades identificadas. Por este motivo la aprobación del plan del tratamiento del riesgo ahora debe ser solicitada a los "dueños del riesgo", si existen muchos de ellos, los riesgos deben ser agrupados y asignados a mandos superiores con autoridades sobre los mandos medios para solicitar

la ejecución de acciones encaminadas a reducir y/o traspasar los riesgos.

Adicionalmente las mediciones y reportería toma una dimensión de revisión estricta en el nuevo estándar. De ser posible todos los objetivos deben ser determinados de tal manera que sean objetivamente medibles. Todas las actividades dirigidas a la gestión del riesgo y oportunidades de mejora deben ser evaluadas. El estándar exige que debe estar definido que es lo que será monitoreado y medido, quien será el responsable de ese monitoreo y mediciones, y quien o quienes evaluarán los resultados. Esto debe ser definido en un documento separado o podría ser incluido en la política seguridad de la empresa.

Los puntos tratados arriba no son un plan de migración, sino más bien una revisión preliminar de los aspectos que se el proveedor está tomando en cuenta para que su sistema de gestión de la seguridad de la información evolucione y cumpla los requerimientos del nuevo estándar ISO 27001:2005

CONCLUSIONES Y RECOMENDACIONES

1. La decisión de implementar la norma ISO 27001:2005 es tomada e impulsada por la alta gerencia. El compromiso del gerente general de la empresa con la implantación del sistema de gestión es el paso inicial en este proyecto.

2. La implementación del departamento de seguridad lógica es un factor de éxito para un correcto arranque de la implementación que es complementada con la colaboración activa de los jefes departamentales.

3. El levantamiento de los activos de información para los procesos involucrados y la evaluación del riesgo son actividades que se deben realizar no solo con las jefaturas sino también con los colaboradores de la organización de interactúan con los mismos, esto es lo que el estándar denomina dueños de los activos.

4. Las decisiones respecto al tratamiento del riesgo y la selección de los controles están sujetas al enfoque de la gerencia general de la empresa.

5. La implementación de los controles seleccionados, en especial la redacción de procedimientos particulares solo puede ser llevada a cabo con la colaboración estrecha de los dueños de los activos

6. La elaboración de los procedimientos específicos es una tarea conjunta del departamento de seguridad lógica, de las jefaturas y delegados departamentales, es decir, los colaboradores de cada departamento que han sido seleccionados por sus jefaturas para esta tarea y para actuar como auditores internos.

7. La capacitación constante de los auditores internos, se levanta como una herramienta fundamental para el mantenimiento del sistema de gestión.

8. La automatización de las tareas que surgen como parte del sistema de gestión es una acción necesaria para lograr eficiencia de la operación del sistema. La búsqueda de la eficiencia se vuelve imperativa puesto que la operación del sistema de gestión no debe generar un aumento en los costos de la operación de la organización.

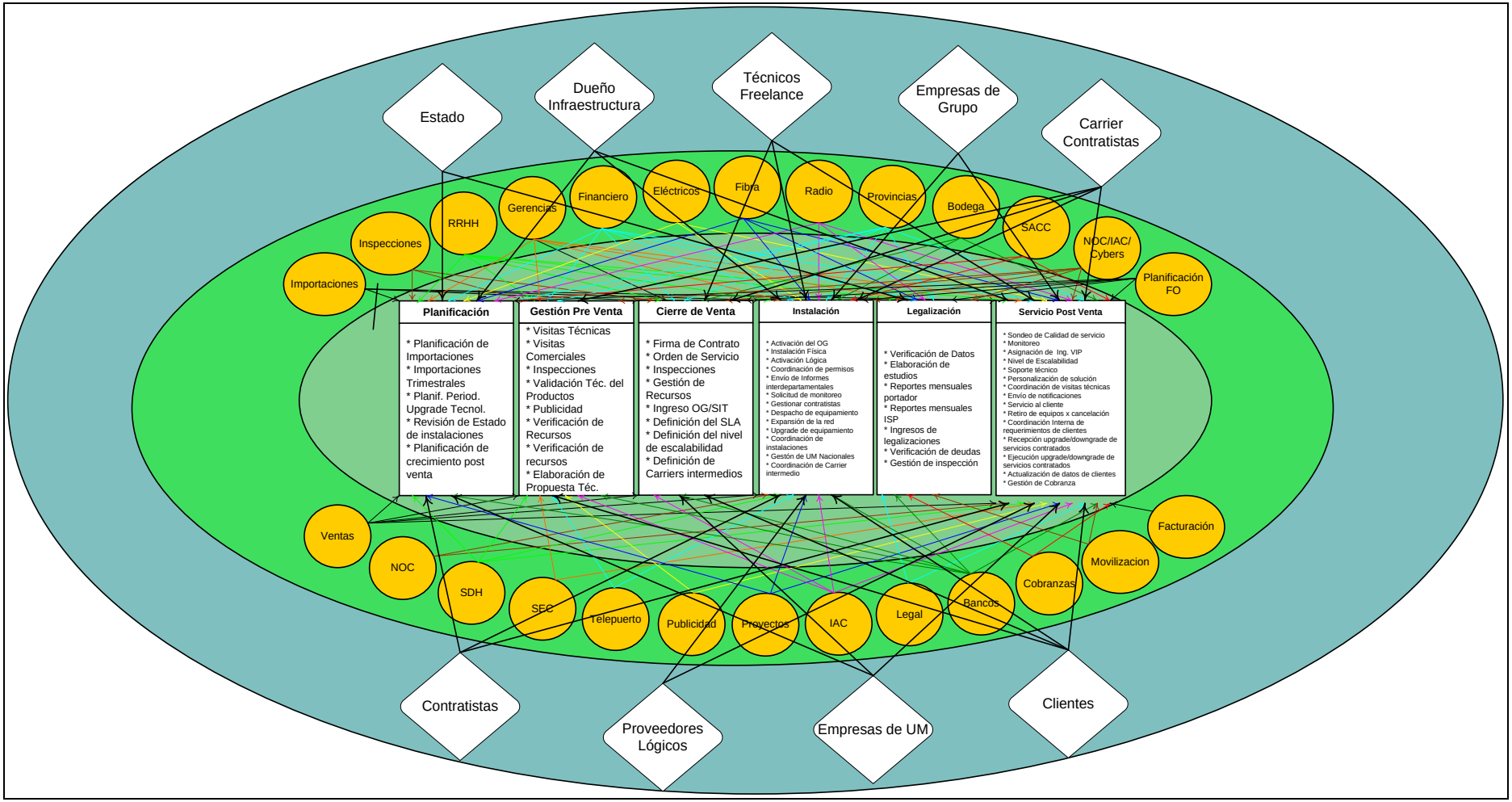
9. La tarea de concientización de la importancia de la seguridad de la información y el cumplimiento de los procedimientos específicos son ejes importantes en la operación del sistema de gestión y deben ser una de las responsabilidades principales del departamento de seguridad lógica.

10. Uno de los elementos claves para el éxito de la operación y mantenimiento del sistema, es el recurso humano. Se debe considerar el principio que el recurso humano tienen el mínimo conocimiento, y esto debe ser considerado como una amenaza que al ser corregida se convierte en una fortaleza organizacional.

ANEXOS

ANEXO 1

DIAGRAMA DE ELIPSES - PROCESO DE APROVISIONAMIENTO



ANEXO 2

EJEMPLO DE SMOP

EJEMPLO DE SMOP

Solicitante: Ing. XXX YYYY

Departamento de Soporte Técnico Corporativo

Compañía: XXX

Objetivo del trabajo: Carga y activación de nuevos sistema operativo IOS

Fecha de Inicio: Lunes, enero 1 de 2012

Hora de Inicio: 00h00

Fecha de Finalización: Lunes, enero 1 de 2012

Hora de Finalización: 00h30

Ubicación del trabajo: Babahoyo – Los Ríos

Servicios Afectados: Clientes corporativos en la ciudad de Babahoyo

Herramientas: laptop con cable serial y nueva imagen IOS

Documentos Adicionales: Ninguno

Procedimiento:

Paso 1

Paso 2

Paso N

Rollback:

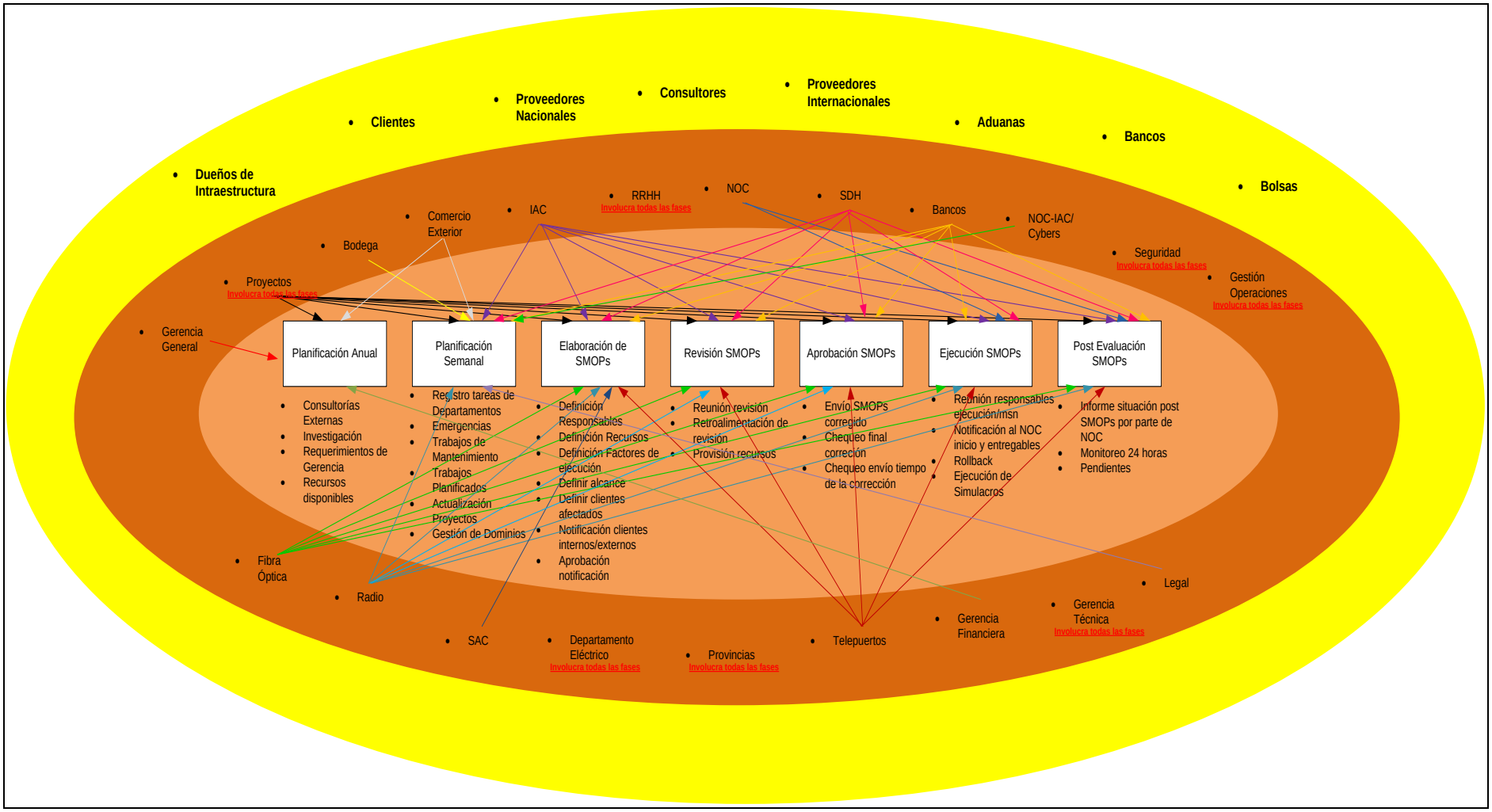
Paso 1

Paso 2

Paso N

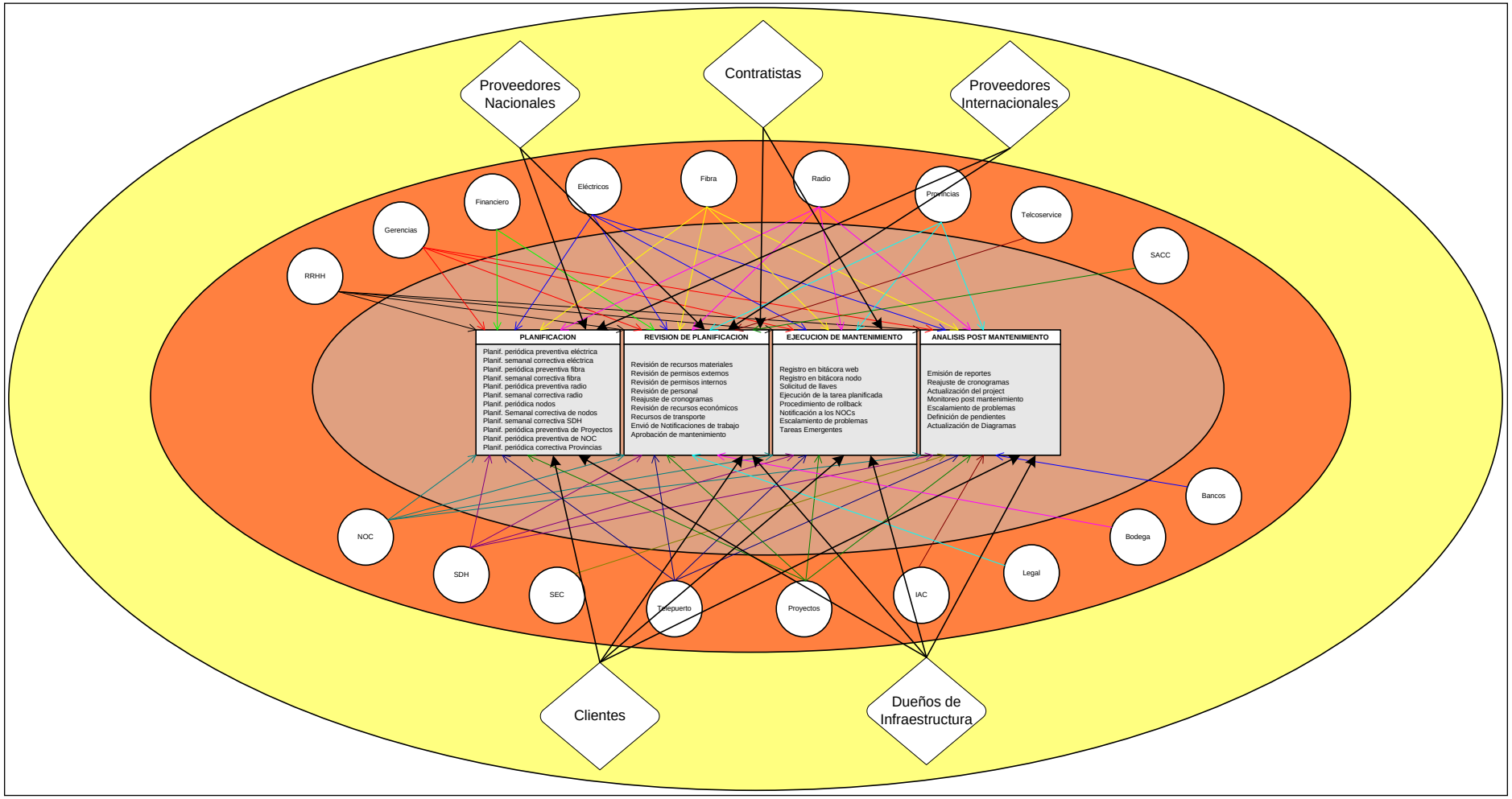
ANEXO 3

DIAGRAMA DE ELIPSES - PROCESO DE CONTROL DE CAMBIOS



ANEXO 4

DIAGRAMA DE ELIPSES - PROCESO DE MANTENIMIENTO



ANEXO 5

VALORACIÓN ACTIVOS - PROCESO APROVISIONAMIENTO

	Confidencialidad	Integridad	Disponibilidad	Promedio	Evaluación del riesgo
Gerencia General	1	5	5	3.666667	SI
Formatos de instalaciones	1	5	5	3.666667	SI
Sistema Integrado SIT	5	5	5	5	SI
Base de datos de clientes	5	5	5	5	SI
Tabla de precios	3	5	5	4.333333	SI
Analisis de mercados	2	3	3	2.666667	NO
Sistema Gestion de Red	1	4	4	3	SI
Sistema Monitoreo	1	5	5	3.666667	SI
Sistema de correo	3	5	5	4.333333	SI
Sistema de Control de Acceso a la Red	5	5	5	5	SI
PBX GYE	1	5	5	3.666667	SI
PBX UIO	1	5	5	3.666667	SI
Proveedor de servicio Telefónico	1	5	5	3.666667	SI
Bodega GYE	1	5	5	3.666667	SI
Sistema de Compras nacionales	1	3	4	2.666667	NO
Sistema de Compras internaciones	1	5	5	3.666667	SI
Personal Administrativo	1	4	4	3	SI
Personal Operativo	1	5	5	3.666667	SI
Computadoras de Personal	1	5	5	3.666667	SI
Manuales y formularios departamentales	1	3	3	2.333333	NO
Sistema Intranet	1	2	2	1.666667	NO
Diagramas de Red	1	3	4	2.666667	NO
Diagramas de clientes	1	3	4	2.666667	NO
Sistema CRM	1	3	3	2.333333	NO
Personal Soporte Corporativo	1	5	5	3.666667	SI
Personal Soporte Clientes VIP	1	5	5	3.666667	SI
Persona Comercial	1	5	5	3.666667	SI
Personal Departamento Legal	1	5	5	3.666667	SI
Contratos con clientes	5	5	5	5	SI
Contratos con duenios de infraestructura	5	5	5	5	SI
Contrato con proveedores de Internet	5	5	5	5	SI
Personal de Monitoreo de Red	1	5	5	3.666667	SI
Personal de Soporte clientes Bancos	1	5	5	3.666667	SI

ANEXO 6

VALORACIÓN DE ACTIVOS - CONTROL DE CAMBIOS

	Confidencialidad	Integridad	Disponibilidad	Promedio	Evaluación del riesgo
PLANIFICACION SEMANAL	1	2	2	1.666667	NO
Sistema de Planificacion	1	5	5	3.666667	SI
Sistema de Correo	1	5	5	3.666667	SI
Equipos de laboratorio	1	5	5	3.666667	SI
Simuladores	1	2	3	2	NO
Documentos de Procedimientos (SMOPS)	2	5	5	4	SI
Sistema de Notificacion a clientes interno y	1	4	5	3.333333	SI
Sistema de Gestion de la Red	1	4	5	3.333333	SI
Equipos de Red	3	5	5	4.333333	SI
Bases de datos de clientes	5	5	5	5	SI
Sistema DNS	1	5	5	3.666667	SI
Sistema Integrado SIT	1	5	5	3.666667	SI
Personal Operativo	1	5	5	3.666667	SI
Personal de Soporte Corporativo	1	5	5	3.666667	SI
Personal de Monitoreo de Red	1	5	5	3.666667	SI
Personal de Gestion de Red	1	5	5	3.666667	SI
Sistema de mensajeria instantanea interna	2	1	1	1.333333	NO
Servicios teléfonicos externos	1	5	5	3.666667	SI
Sistemas de Repositorios de Datos	3	5	5	4.333333	SI
Sistema Intranet	1	4	4	3	SI
Sistema de control de Acceso a la Red	3	5	5	4.333333	SI
Infraestructura de fibra óptica backbone	2	5	5	4	SI
Infraestrucutura de Radio	2	5	5	4	SI
Revision de SMOPs	1	5	5	3.666667	SI
Aprobación de SMOPs	1	5	5	3.666667	SI

ANEXO 7

VALORACIÓN DE ACTIVOS – MANTENIMIENTO

	Confidencialidad	Integridad	Disponibilidad	Promedio	Evaluación del riesgo
Sistema de Planificacion	1	5	5	3.6666667	SI
Formatos de Planificacion Fibra óptica	1	3	3	2.3333333	NO
Formatos de planificacion de Radio	1	3	3	2.3333333	NO
Formatos de planificacion de SDH	1	3	3	2.3333333	NO
Formatos de planificacion Electrica	1	3	3	2.3333333	NO
Formatos de planificacion de Nodos	1	3	3	2.3333333	NO
Diagramas de infraestructura	1	3	3	2.3333333	NO
Solicitud de Permisos a Municipio	1	5	5	3.6666667	SI
Solicitud de Materiales	1	5	5	3.6666667	SI
Transporte	1	5	5	3.6666667	SI
Medidor de antenuacion de enlace de fibra OTDR	1	5	5	3.6666667	SI
Fusionadora de enlaces de fibra	1	5	5	3.6666667	SI
Medidor de potencia en enlaces de fibra	1	5	5	3.6666667	SI
Infraestrucutura de fibra backbone	1	5	5	3.6666667	SI
Infraestrucutra de fibra de acceso	1	5	5	3.6666667	SI
Nodos de backbone	1	5	5	3.6666667	SI
Nodos de acceso	1	5	5	3.6666667	SI
Sistema de control de Acceso a Nodos	5	5	5	5	SI
Personal de Moniitoreo de Red	1	5	5	3.6666667	SI
Personal Mantenimiento fibra	1	5	5	3.6666667	SI
Personal de Mantenimineto electrico	1	5	5	3.6666667	SI
Personal de operaciones fibra	1	5	5	3.6666667	SI
Personal de operacion fibra	1	5	5	3.6666667	SI
Personal de gestion de la Red	1	5	5	3.6666667	SI
Personal de Soporte Corporativo	1	5	5	3.6666667	SI
Personal de Soporte a clientes Bancos	1	5	5	3.6666667	SI
Personal de gestion de Red de Transporte Optico	1	5	5	3.6666667	SI
Infraestrucutra de Radio	2	3	4	3	SI
Infraestuctura de respaldo electrico en nodos	1	5	5	3.6666667	SI
Sistema de correo	1	5	5	3.6666667	SI
Sistema Integrado SIT	1	5	5	3.6666667	SI
Sistema de Monitoreo de la Red	1	5	5	3.6666667	SI
Sistema de Gestion de la Red	1	5	3	3	SI
Computadoras portátiles Laptos	1	3	5	3	SI
Contratos de dueños de infraestructura	1	4	4	3	SI
Sistema de Reportes de trabajo	1	4	4	3	SI
Listas de escalabilidad	1	4	4	3	SI
Caja chica	1	3	4	2.6666667	NO
Documento de Procedimientos	1	3	3	2.3333333	NO
Telepuerto kennedy	3	5	5	4.3333333	SI
Telepuerto bellavista	3	5	5	4.3333333	SI
Telepuerto muros	3	5	5	4.3333333	SI
Telepuerto gosseal	3	5	5	4.3333333	SI
Telepuerto Manta	3	5	5	4.3333333	SI
Telepuerto Loja	3	5	5	4.3333333	SI
Telepuerto Quevedo	3	5	5	4.3333333	SI
Telepuerto Salinas	3	5	5	4.3333333	SI
Telepuerto Cuenca	3	5	5	4.3333333	SI
Telepuerto Portoviejo	3	5	5	4.3333333	SI

ANEXO 8

ANÁLISIS DE RIESGO

	AMENAZAS					
	Amenazas Naturales	Amenazas a Instalaciones	Amenazas Humanas	Amenazas Tecnológicas	Amenazas Operacionales	Amenazas Sociales
Gerencia General	3	1	4	1	3	2
Formatos de instalaciones	3	1	1	1	1	1
Sistema Integrado SIT	3	2	2	4	3	1
Base de datos de clientes	3	2	2	4	3	1
Tabla de precios	3	2	1	1	2	1
Sistema Gestion de Red	3	2	2	4	3	1
Sistema Monitoreo	3	2	2	4	4	1
Sistema de correo	3	2	2	4	5	1
Sistema de Control de Acceso a la Red	3	1	2	5	5	1
PBX GYE	3	2	2	3	5	1
PBX UIO	3	2	2	3	5	1
Proveedor de servicio Telefónico	3	2	3	3	5	1
Bodega GYE	3	4	4	2	5	3
Sistema de Compras internaciones	3	1	1	1	3	2
Personal Administrativo	3	1	4	1	3	3
Personal Operativo	3	1	4	1	5	2
Computadoras de Personal	3	1	4	4	4	1
Personal Soporte Corporativo	3	1	4	1	5	2
Personal Soporte Clientes VIP	3	1	4	1	5	2
Persona Comercial	3	1	4	1	5	2
Personal Departamento Legal	3	1	4	1	5	2
Contratos con clientes	3	3	4	4	5	2
Contratos con duenios de infraestructura	3	3	4	4	5	2
Contrato con proveedores de Internet	3	3	4	4	5	2
Personal de Monitoreo de Red	3	1	4	1	5	2
Personal de Soporte clientes Bancos	3	1	4	1	5	2
Sistema de Planificacion	3	2	2	5	2	1
Equipos de laboratorio	3	2	2	5	2	1
Documentos de Procedimientos (SMOPS)	3	2	2	1	2	1
Sistema de Notificacion a clientes interno y externo	3	2	2	5	3	2
Equipos de Red	3	2	2	4	5	1
Sistema DNS	3	2	2	3	5	1
Sistemas de Repositorios de Datos	3	2	2	4	5	1
Sistema Intranet	3	2	2	4	3	1
Infraestructura de fibra óptica backbone	4	4	4	2	5	1
Infraestrucutura de Radio	4	4	4	2	5	1
Revision de SMOPs	3	2	2	1	1	1
Aprobación de SMOPs	3	2	2	1	1	1
Sistema de Planificacion	3	2	2	5	1	1
Solicitud de Permisos a Municipio	2	2	2	1	4	2
Solicitud de Materiales	2	2	2	1	4	1
Transporte	3	2	3	2	4	3
Medidor de antenuacion de enlace de fibra OTDR	3	2	4	2	5	1
Fusionadora de enlaces de fibra	3	4	4	2	5	1
Medidor de potencia en enlaces de fibra	3	2	4	2	5	1
Infraestrucutura de fibra backbone	3	2	2	1	5	1
Infraestrucutra de fibra de acceso	3	2	2	1	5	1
Nodos de backbone	3	2	2	1	5	1
Nodos de acceso	3	2	2	1	5	3
Sistema de control de Acceso a Nodos	3	2	1	5	1	1
Personal Mantenimiento fibra	3	2	2	1	5	1
Personal de Mantenimiento electrico	3	2	1	1	5	1
Personal de operacion fibra	3	2	2	1	5	1
Personal de gestion de la Red	3	2	1	1	5	1
Personal de gestion de Red de Transporte Optico	3	2	1	1	5	1
Infraestrucutra de Radio	3	2	2	2	3	1
Infraestuctura de respaldo electrico en nodos	3	2	2	2	3	1
Computadoras portátiles Laptos	3	2	3	5	2	1
Contratos de dueños de infraestructura	3	2	1	1	4	1
Sistema de Reportes de trabajo	3	2	1	5	1	1
Listas de escalabilidad	3	2	1	1	2	1
Telepuerto kennedy	2	2	2	1	5	1
Telepuerto bellavista	2	2	2	1	5	1
Telepuerto muros	2	2	2	1	5	1
Telepuerto gosseal	2	2	2	1	5	1
Telepuerto Manta	2	2	2	1	5	1
Telepuerto Loja	2	2	2	1	5	1
Telepuerto Quevedo	2	2	2	1	5	1
Telepuerto Salinas	2	2	2	1	5	1
Telepuerto Cuenca	2	2	2	1	5	1
Telepuerto Portoviejo	2	2	2	1	5	1

	VULNERABILIDADES				
	Seguridad Recursos Humanos	**Control de Acceso**	**Seguridad Física y Ambiental**	**Operación y Comunicaciones**	**Mantenimiento, operación y Adquisición de sistemas**
Gerencia General	4	4	4	3	1
Formatos de instalaciones	1	2	2	1	1
Sistema Integrado SIT	1	4	2	4	5
Base de datos de clientes	1	4	2	4	5
Tabla de precios	1	2	2	1	1
Sistema Gestion de Red	1	4	2	5	5
Sistema Monitoreo	1	4	2	5	5
Sistema de correo	1	4	2	5	5
Sistema de Control de Acceso a la Red	1	5	3	5	5
PBX GYE	1	2	4	5	5
PBX UIO	1	2	4	5	5
Proveedor de servicio Telefónico	2	2	3	5	2
Bodega GYE	2	4	4	2	2
Sistema de Compras internaciones	2	4	1	3	3
Personal Administrativo	4	4	4	3	1
Personal Operativo	4	4	4	3	1
Computadoras de Personal	1	4	2	4	5
Personal Soporte Corporativo	4	4	4	3	1
Personal Soporte Clientes VIP	4	4	4	3	1
Persona Comercial	4	4	4	3	1
Personal Departamento Legal	4	4	4	3	1
Contratos con clientes	3	3	3	2	2
Contratos con duenios de infraestructura	3	3	3	2	2
Contrato con proveedores de Internet	3	3	3	2	2
Personal de Monitoreo de Red	4	4	4	3	1
Personal de Soporte clientes Bancos	4	4	4	3	1
Sistema de Planificacion	2	3	2	2	4
Equipos de laboratorio	1	3	2	1	2
Documentos de Procedimientos (SMOPS)	1	1	1	1	1
Sistema de Notificacion a clientes interno y externo	1	1	2	2	4
Equipos de Red	1	3	2	4	3
Sistema DNS	2	3	2	4	4
Sistemas de Repositorios de Datos	2	3	2	4	4
Sistema Intranet	2	4	2	1	4
Infraestructura de fibra óptica backbone	2	3	3	4	1
Infraestrucutura de Radio	1	3	3	2	1
Revision de SMOPs	1	1	1	1	1
Aprobación de SMOPs	1	1	1	1	1
Sistema de Planificacion	2	3	2	1	4
Solicitud de Permisos a Municipio	2	1	1	3	1
Solicitud de Materiales	1	1	1	1	1
Transporte	3	2	2	4	1
Medidor de antenuacion de enlace de fibra OTDR	3	2	1	4	1
Fusionadora de enlaces de fibra	3	2	1	4	1
Medidor de potencia en enlaces de fibra	3	2	1	4	1
Infraestrucutura de fibra backbone	2	2	2	4	1
Infraestrucutra de fibra de acceso	2	2	2	4	1
Nodos de backbone	2	2	2	4	1
Nodos de acceso	2	2	2	4	1
Sistema de control de Acceso a Nodos	3	3	2	1	4
Personal Mantenimiento fibra	4	1	3	4	1
Personal de Mantenimiento electrico	4	1	3	4	1
Personal de operacion fibra	4	1	3	4	1
Personal de gestion de la Red	4	1	3	4	1
Personal de gestion de Red de Transporte Optico	4	1	3	4	1
Infraestrucutra de Radio	1	2	1	2	1
Infraestuctura de respaldo electrico en nodos	3	2	2	4	1
Computadoras portátiles Laptos	4	4	1	3	4
Contratos de dueños de infraestructura	2	1	1	3	1
Sistema de Reportes de trabajo	1	3	1	1	4
Listas de escalabilidad	1	1	1	1	1
Telepuerto kennedy	3	2	2	5	4
Telepuerto bellavista	3	2	2	5	4
Telepuerto muros	3	2	2	5	4
Telepuerto gosseal	3	2	2	5	4
Telepuerto Manta	3	2	2	5	4
Telepuerto Loja	3	2	2	5	4
Telepuerto Quevedo	3	2	2	5	4
Telepuerto Salinas	3	2	2	5	4
Telepuerto Cuenca	3	2	2	5	4
Telepuerto Portoviejo	3	2	2	5	4

	ESTIMACIÓN DEL RIESGO			EVALUACIÓN DEL IMPACTO			
	Promedio	Valor del Activo	Medición del riesgo	Impacto Económico	Tiempo de Recuperación	Imagen	Interrupción de Actividad
Gerencia General	2.727272727	3.6666667	10	4	3	2	1
Formatos de instalaciones	1.363636364	3.6666667	5	1	1	1	1
Sistema Integrado SIT	2.818181818	5	14.09090909	4	3	2	3
Base de datos de clientes	2.818181818	5	14.09090909	5	3	2	4
Tabla de precios	1.545454545	4.3333333	6.696969697	2	3	1	1
Sistema Gestion de Red	2.909090909	3	8.727272727	3	3	2	2
Sistema Monitoreo	3	3.6666667	11	3	3	2	2
Sistema de correo	3.090909091	4.3333333	13.39393939	3	3	3	3
Sistema de Control de Acceso a la Red	3.272727273	5	16.36363636	2	3	1	2
PBX GYE	3	3.6666667	11	4	3	3	4
PBX UIO	3	3.6666667	11	4	3	3	4
Proveedor de servicio Telefónico	2.818181818	3.6666667	10.33333333	4	4	3	4
Bodega GYE	3.181818182	3.6666667	11.66666667	2	5	1	3
Sistema de Compras internaciones	2.181818182	3.6666667	8	3	4	1	2
Personal Administrativo	2.818181818	3	8.454545455	4	5	3	4
Personal Operativo	2.909090909	3.6666667	10.66666667	4	5	4	4
Computadoras de Personal	3	3.6666667	11	1	3	1	4
Personal Soporte Corporativo	2.909090909	3.6666667	10.66666667	3	5	4	4
Personal Soporte Clientes VIP	2.909090909	3.6666667	10.66666667	3	5	4	4
Persona Comercial	2.909090909	3.6666667	10.66666667	4	5	4	4
Personal Departamento Legal	2.909090909	3.6666667	10.66666667	3	5	3	4
Contratos con clientes	3.090909091	5	15.45454545	2	2	3	2
Contratos con duenios de infraestructura	3.090909091	5	15.45454545	2	3	3	2
Contrato con proveedores de Internet	3.090909091	5	15.45454545	4	4	4	3
Personal de Monitoreo de Red	2.909090909	3.6666667	10.66666667	3	5	4	4
Personal de Soporte clientes Bancos	2.909090909	3.6666667	10.66666667	3	5	4	4
Sistema de Planificacion	2.545454545	3.6666667	9.333333333	1	3	1	1
Equipos de laboratorio	2.181818182	3.6666667	8	1	3	1	1
Documentos de Procedimientos (SMOPS)	1.454545455	4	5.818181818	1	1	1	1
Sistema de Notificacion a clientes interno y externo	2.454545455	3.3333333	8.181818182	2	3	2	1
Equipos de Red	2.727272727	4.3333333	11.81818182	4	3	3	4
Sistema DNS	2.818181818	3.6666667	10.33333333	4	3	3	4
Sistemas de Repositorios de Datos	2.909090909	4.3333333	12.60606061	4	3	1	3
Sistema Intranet	2.545454545	3	7.636363636	2	3	1	
Infraestructura de fibra óptica backbone	3	4	12	4	2	3	4
Infraestrucutura de Radio	2.727272727	4	10.90909091	2	2	2	2
Revision de SMOPs	1.363636364	3.6666667	5	1	1	1	1
Aprobación de SMOPs	1.363636364	3.6666667	5	1	1	1	1
Sistema de Planificacion	2.363636364	3.6666667	8.666666667	1	3	1	1
Solicitud de Permisos a Municipio	1.909090909	3.6666667	7	3	2	2	3
Solicitud de Materiales	1.545454545	3.6666667	5.666666667	1	1	1	2
Transporte	2.636363636	3.6666667	9.666666667	3	3	2	3
Medidor de antenuacion de enlace de fibra OTDR	2.545454545	3.6666667	9.333333333	1	3	2	3
Fusionadora de enlaces de fibra	2.727272727	3.6666667	10	1	3	2	3
Medidor de potencia en enlaces de fibra	2.545454545	3.6666667	9.333333333	1	3	2	3
Infraestrucutura de fibra backbone	2.272727273	3.6666667	8.333333333	4	2	3	2
Infraestrucutra de fibra de acceso	2.272727273	3.6666667	8.333333333	4	2	3	2
Nodos de backbone	2.272727273	3.6666667	8.333333333	4	2	3	2
Nodos de acceso	2.454545455	3.6666667	9	3	2	3	2
Sistema de control de Acceso a Nodos	2.363636364	5	11.81818182	1	3	1	1
Personal Mantenimiento fibra	2.454545455	3.6666667	9	3	5	3	4
Personal de Mantenimiento electrico	2.363636364	3.6666667	8.666666667	3	5	3	4
Personal de operacion fibra	2.454545455	3.6666667	9	3	5	3	4
Personal de gestion de la Red	2.363636364	3.6666667	8.666666667	3	5	3	4
Personal de gestion de Red de Transporte Optico	2.363636364	3.6666667	8.666666667	3	5	3	4
Infraestrucutra de Radio	1.818181818	3	5.454545455	2	2	2	2
Infraestuctura de respaldo electrico en nodos	2.272727273	3.6666667	8.333333333	2	2	2	2
Computadoras portátiles Laptos	2.909090909	3	8.727272727	2	2	1	4
Contratos de dueños de infraestructura	1.818181818	3	5.454545455	3	3	3	3
Sistema de Reportes de trabajo	2.090909091	3	6.272727273	1	2	1	1
Listas de escalabilidad	1.363636364	3	4.090909091	1	1	1	1
Telepuerto kennedy	2.636363636	4.3333333	11.42424242	5	5	4	4
Telepuerto bellavista	2.636363636	4.3333333	11.42424242	5	5	4	4
Telepuerto muros	2.636363636	4.3333333	11.42424242	5	5	4	4
Telepuerto gosseal	2.636363636	4.3333333	11.42424242	5	5	4	
Telepuerto Manta	2.636363636	4.3333333	11.42424242	5	5	4	4
Telepuerto Loja	2.636363636	4.3333333	11.42424242	5	5	4	4
Telepuerto Quevedo	2.636363636	4.3333333	11.42424242	5	5	4	4
Telepuerto Salinas	2.636363636	4.3333333	11.42424242	5	5	4	4
Telepuerto Cuenca	2.636363636	4.3333333	11.42424242	5	5	4	4
Telepuerto Portoviejo	2.636363636	4.3333333	11.42424242	5	5	4	4

	PROMEDIO	EVALUACIÓN TOTAL DEL RIESGO
Gerencia General	2.5	25
Formatos de instalaciones	1	5
Sistema Integrado SIT	3	42.27272727
Base de datos de clientes	3.5	49.31818182
Tabla de precios	1.75	11.71969697
Sistema Gestion de Red	2.5	21.81818182
Sistema Monitoreo	2.5	27.5
Sistema de correo	3	40.18181818
Sistema de Control de Acceso a la Red	2	32.72727273
PBX GYE	3.5	38.5
PBX UIO	3.5	38.5
Proveedor de servicio Telefónico	3.75	38.75
Bodega GYE	2.75	32.08333333
Sistema de Compras internaciones	2.5	20
Personal Administrativo	4	33.81818182
Personal Operativo	4.25	45.33333333
Computadoras de Personal	2.25	24.75
Personal Soporte Corporativo	4	42.66666667
Personal Soporte Clientes VIP	4	42.66666667
Persona Comercial	4.25	45.33333333
Personal Departamento Legal	3.75	40
Contratos con clientes	2.25	34.77272727
Contratos con duenios de infraestructura	2.5	38.63636364
Contrato con proveedores de Internet	3.75	57.95454545
Personal de Monitoreo de Red	4	42.66666667
Personal de Soporte clientes Bancos	4	42.66666667
Sistema de Planificacion	1.5	14
Equipos de laboratorio	1.5	12
Documentos de Procedimientos (SMOPS)	1	5.818181818
Sistema de Notificacion a clientes interno y externo	2	16.36363636
Equipos de Red	3.5	41.36363636
Sistema DNS	3.5	36.16666667
Sistemas de Repositorios de Datos	2.75	34.66666667
Sistema Intranet	2	15.27272727
Infraestructura de fibra óptica backbone	3.25	39
Infraestrucutura de Radio	2	21.81818182
Revision de SMOPs	1	5
Aprobación de SMOPs	1	5
Sistema de Planificacion	1.5	13
Solicitud de Permisos a Municipio	2.5	17.5
Solicitud de Materiales	1.25	7.083333333
Transporte	2.75	26.58333333
Medidor de antenuacion de enlace de fibra OTDR	2.25	21
Fusionadora de enlaces de fibra	2.25	22.5
Medidor de potencia en enlaces de fibra	2.25	21
Infraestrucutura de fibra backbone	2.75	22.91666667
Infraestrucutra de fibra de acceso	2.75	22.91666667
Nodos de backbone	2.75	22.91666667
Nodos de acceso	2.5	22.5
Sistema de control de Acceso a Nodos	1.5	17.72727273
Personal Mantenimiento fibra	3.75	33.75
Personal de Mantenimiento electrico	3.75	32.5
Personal de operacion fibra	3.75	33.75
Personal de gestion de la Red	3.75	32.5
Personal de gestion de Red de Transporte Optico	3.75	32.5
Infraestrucutra de Radio	2	10.90909091
Infraestuctura de respaldo electrico en nodos	2	16.66666667
Computadoras portátiles Laptos	2.25	19.63636364
Contratos de dueños de infraestructura	3	16.36363636
Sistema de Reportes de trabajo	1.25	7.840909091
Listas de escalabilidad	1	4.090909091
Telepuerto kennedy	4.5	51.40909091
Telepuerto bellavista	4.5	51.40909091
Telepuerto muros	4.5	51.40909091
Telepuerto gosseal	4.666666667	53.31313131
Telepuerto Manta	4.5	51.40909091
Telepuerto Loja	4.5	51.40909091
Telepuerto Quevedo	4.5	51.40909091
Telepuerto Salinas	4.5	51.40909091
Telepuerto Cuenca	4.5	51.40909091
Telepuerto Portoviejo	4.5	51.40909091

ANEXO 9

CONTROLES

SECCIÓN ISO/IEC 27002	CONTROLES	TIPO					
		Reducir Amenaza (Disuadir)	Eliminar Situación de Riesgo	Reducir Vulnerabilidad (Prevenir)	Detectar Incidentes	Reaccionar ante Incidentes	Recuperarse ante Incidentes
5	**Política de Seguridad**						
5.1	**Política de seguridad de la información**						
5.1.1	Documento de la política de la seguridad de la información	**P**	**P**	**P**		**P**	**P**
5.1.2	Revisión de la política de la seguridad de la información	**P**	**P**	**P**		**P**	**P**
6	**Organización de la seguridad de la información**						
6.1	**Organización interna**						
6.1.1	Compromiso de la gerencia con la seguridad de la información	**P**	**P**	**P**		**P**	**P**
6.1.2	Coordinación de la seguridad de la información		**P**	**P**		**P**	**P**
6.1.3	Asignación de las responsabilidades de la seguridad de la información		**P**	**P**	**P**	**P**	**P**
6.1.4	Autorización de proceso para facilidades procesadoras de información		**P**				
6.1.5	Acuerdos de Confidencialidad		**P**	**P**			
6.1.6	Contacto con las autoridades		**P**			**P**	
6.1.7	Contacto con grupos de interés especial		**P**	**P**	**P**		
6.1.8	Revisión independiente de la seguridad de la información		**P**	**P**	**P**	**P**	**P**
6.2	**Grupos o personas externas**						
6.2.1	Identificación de los riesgos relacionados con los grupos externos	**P**	**P**	**P**			
6.2.2	Tratamiento de la seguridad cuando se lidia con clientes	**P**	**P**	**P**			
6.2.3	Tratamiento de la seguridad en	**P**	**P**	**P**	**P**	**P**	**P**

	acuerdos con terceros						
7	**Gestión de Activos**						
7.1	**Responsabilidad por los activos**						
7.1.1	Inventario de los activos		**P**	**P**			**P**
7.1.2	Propiedad de los activos		**P**	**P**	**P**	**P**	**P**
7.1.3	Uso aceptable de los activos		**P**	**P**			
7.2	**Clasificación de la información**						
7.2.1	Lineamientos de clasificación		**P**				
7.2.2	Etiquetado y manejo de la información	**P**		**P**	**P**		
8	**Seguridad de Recursos Humanos**						
8.1	**Antes del empleo**						
8.1.1	Roles y responsabilidades	**P**	**P**	**P**			
8.1.2	Investigación de antecedentes	**P**	**P**				
8.1.3	Términos y condiciones del empleo	**P**	**P**				
8.2	**Durante el empleo**						
8.2.1	Responsabilidades de la gerencia	**P**	**P**	**P**	**P**		
8.2.2	Conocimiento, educación y capacitación en seguridad de la información	**P**	**P**	**P**	**P**		
8.2.3	Proceso disciplinario	**P**	**P**	**P**	**P**		
8.3	**Terminación o cambio de empleo**						
8.3.1	Responsabilidades de terminación		**P**	**P**			
8.3.2	Devolución de los activos		**P**				
8.3.3	Retiro de los derechos de acceso		**P**	**P**			
9	**Seguridad Física y Ambiental**						
9.1	**Áreas Seguras**						
9.1.1	Perímetro de la seguridad física	**P**	**P**	**P**			
9.1.2	Controles de ingreso físico	**P**	**P**	**P**	**P**		
9.1.3	Aseguramiento de oficinas, habitaciones y medios	**P**	**P**	**P**	**P**		
9.1.4	Protección contra amenazas internas y externas		**P**	**P**			

9.1.5	Trabajando en áreas aseguradas	**P**		**P**			
9.1.6	Áreas de acceso público, entrega y carga	**P**	**P**	**P**			
9.2	**Equipo de seguridad**						
9.2.1	Ubicación y protección del equipo		**P**	**P**	**P**		
9.2.2	Servicios públicos de soporte		**P**	**P**		**P**	**P**
9.2.3	Seguridad del Cableado			**P**			
9.2.4	Mantenimiento del equipo		**P**	**P**	**P**		
9.2.5	Seguridad del equipo fuera del local		**P**				
9.2.6	Seguridad de la eliminación o reuso del equipo	**P**	**P**	**P**			
9.2.7	Retiro de la propiedad	**P**	**P**	**P**	**P**		
10	**Gestión de las comunicaciones y operaciones**						
10.1	**Procedimientos y responsabilidades operacionales**						
10.1.1	Procedimientos de operación documentados		**P**	**P**		**P**	**P**
10.1.2	Gestión de Cambio	**P**	**P**	**P**			
10.1.3	Segregación de los deberes	**P**	**P**	**P**			
10.1.4	Separación de los medios de desarrollo, prueba y operación	**P**	**P**	**P**			
10.2	**Gestión de la entrega del servicio de terceros**						
10.2.1	Entrega del servicio	**P**	**P**	**P**	**P**	**P**	**P**
10.2.2	Monitoreo y revisión del servicio de terceros				**P**		

10.2.3	Manejo de cambios en los servicios de terceros		**P**	**P**			
10.3	**Planeación y aceptación del sistema**						
10.3.1	Gestión de la Capacidad		**P**				
10.3.2	Aceptación del sistema			**P**	**P**		
10.4	**Protección contra código malicioso y móvil**						
10.4.1	Controles contra código malicioso	**P**		**P**	**P**	**P**	**P**
10.4.2	Controles contra códigos móviles		**P**	**P**			
10.5	**Copia de Seguridad**						
10.5.1	Información de Copia de Seguridad		**P**	**P**			**P**
10.6	**Gestión de la Seguridad de Red**						
10.6.1	Controles de redes			**P**			
10.6.2	Seguridad de los servicios de red		**P**	**P**	**P**		
10.7	**Gestión de Medios**						
10.7.1	Gestión de medios removibles	**P**	**P**	**P**			
10.7.2	Disposición de medios		**P**	**P**			
10.7.3	Procedimientos para el manejo de la información		**P**	**P**			
10.7.4	Seguridad de la documentación del sistema			**P**			
10.8	**Intercambio de Información**						
10.8.1	Políticas y procedimientos para el intercambio de la información		**P**	**P**			
10.8.2	Acuerdos de Intercambio		**P**	**P**			
10.8.3	Medios físicos en tránsito		**P**	**P**			
10.8.4	Mensajería Electrónica	**P**		**P**			
10.8.5	Sistemas de Información Comercial	**P**		**P**			**P**
10.9	**Servicios de Comercio electrónico**						

10.9.1	Comercio electrónico	**P**	**P**	**P**			
10.9.2	Transacciones en línea	**P**	**P**	**P**			
10.9.3	Información públicamente disponible			**P**			
10.1	**Monitoreo**						
10.10.1	Registro de auditoría	**P**			**P**	**P**	
10.10.2	Uso del sistema de monitoreo	**P**			**P**	**P**	
10.10.3	Protección del registro de información	**P**	**P**	**P**			
10.10.4	Registros del administrador y operador	**P**			**P**		
10.10.5	Registro de fallas				**P**		**P**
10.10.6	Sincronización de relojes		**P**	**P**			
11	**Control de Acceso**						
11.1	**Requerimiento del negocio para el control acceso**						
11.1.1	Política de control de acceso	**P**		**P**			
11.2	**Gestión de Acceso del usuario**						
11.2.1	Registro del usuario	**P**	**P**				
11.2.2	Gestión de privilegios		**P**	**P**			
11.2.3	Gestión de las claves secretas de los usuarios			**P**			
11.2.4	Revisión de los derechos de acceso del usuario	**P**		**P**	**P**		
11.3	**Responsabilidades del usuario**						
11.3.1	Uso de las claves secretas		**P**	**P**			
11.3.2	Equipo del usuario desatendido	**P**		**P**			
11.3.3	Política de escritorio y pantalla limpios		**P**	**P**			
11.4	**Control de Acceso a la Red**						
11.4.1	Política sobre el uso de los servicios de la red		**P**	**P**			

11.4.2	Autenticación del usuario para las conexiones externas	**P**	**P**	**P**			
11.4.3	Identificación del equipo en las redes	**P**	**P**	**P**			
11.4.4	Protección del puerto de diagnóstico y configuración remoto		**P**	**P**			
11.4.5	Segregación en redes	**P**		**P**			
11.4.6	Control de conexión a la red	**P**		**P**			
11.4.7	Control de enrutamiento de la red	**P**		**P**			
11.5	**Control de acceso al sistema operativo**						
11.5.1	Procedimientos para un logoneo seguro	**P**	**P**	**P**			
11.5.2	Identificación y autenticación del usuario	**P**		**P**			
11.5.3	Sistema de gestión de claves secretas	**P**		**P**			
11.5.4	Uso de las utilidades del sistema			**P**			
11.5.5	Cierre de sesión por inactividad	**P**		**P**		**P**	
11.5.6	Limitación del tiempo de conexión	**P**	**P**				
11.6	**Control de acceso a la aplicación y la información**						
11.6.1	Restricción de acceso a la información	**P**		**P**			
11.6.2	Aislar el sistema confidencial	**P**		**P**			
11.7	**Computación móvil y tele trabajo**						
11.7.1	Computación móvil y comunicaciones			**P**			
11.7.2	Tele trabajo			**P**			
12	**Adquisición, desarrollo y mantenimiento de los sistemas de información**						
12.1	**Requerimientos de seguridad de los sistemas de información**						
12.1.1	Análisis y especificación de los requerimientos de seguridad		**P**				
12.2	**Procesamiento correcto en las aplicaciones**						
12.2.1	Validación de la input data		**P**				
12.2.2	Control del procesamiento interno			**P**			

12.2.3	Integridad del mensaje		**P**				
12.2.4	Validación de la output data			**P**			
12.3	**Controles Criptográficos**						
12.3.1	Política sobre el uso de controles criptográficos		**P**				
12.3.2	Gestión de claves		**P**				
12.4	**Seguridad de los archivos del sistema**						
12.4.1	Control del software operacional		**P**				
12.4.2	Protección de la data del sistema			**P**			
12.4.3	Control de acceso al código fuente del programa		**P**	**P**			
12.5	**Seguridad en los procesos de desarrollo y soporte**						
12.5.1	Procedimientos del control de cambios		**P**				
12.5.2	Revisión técnica de la aplicación después de cambios en el sistema				**P**		
12.5.3	Restricciones sobre los cambios en los paquetes de software		**P**	**P**			
12.5.4	Filtración de la información		**P**	**P**			
12.5.5	Desarrollo de software abastecido externamente	**P**	**P**	**P**			
12.6	**Gestión de la Vulnerabilidad técnica**						
12.6.1	Control de las vulnerabilidades técnicas		**P**				
13	**Gestión de un incidente en la seguridad de la información**						
13.1	**Reporte de los eventos y debilidades de la seguridad de la información**						
13.1.1	Reporte de eventos en la seguridad de la información				**P**	**P**	

13.1.2	Reporte de las debilidades en la seguridad	**P**			**P**		
13.2	**Gestión de los incidentes y mejoras en la seguridad de la información**						
13.2.1	Responsabilidades y procedimientos					**P**	**P**
13.2.2	Aprender de los incidentes en la seguridad de la información		**P**				**P**
13.2.3	Recolección de evidencia	**P**		**P**		**P**	
14	**Gestión de la continuidad del Negocio**						
14.1	**Aspecto de la seguridad de la información de la gestión de la continuidad del negocio**						
14.1.1	Incluir la seguridad de la información en el proceso de la gestión de continuidad del negocio		**P**			**P**	**P**
14.1.2	Continuidad del negocio y evaluación del riesgo		**P**			**P**	**P**
14.1.3	Desarrollar e implementar los planes de continuidad incluyendo seguridad de información						**P**
14.1.4	Marco referencial de la planeación de la continuidad del negocio					**P**	**P**
14.1.5	Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio					**P**	**P**
15	**Cumplimiento**						
15.1	**Cumplimiento de los requerimientos legales**						
15.1.1	Identificación de la legislación aplicable			**P**			
15.1.2	Derechos de propiedad intelectual			**P**			
15.1.3	Protección de los registros organizacionales			**P**		**P**	**P**
15.1.4	Protección de la data y de la privacidad de la información personal			**P**			
15.1.5	Prevención del mal uso de los medios de procesamiento de la información	**P**		**P**			

15.1.6	Regulación de los controles criptográficos			**P**			
15.2	**Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico**						
15.2.1	Cumplimiento con las políticas y estándares de seguridad	**P**			**P**		
15.2.2	Chequeo del cumplimiento técnico					**P**	
15.3	**Consideraciones de auditoría de los sistemas de información**						
15.3.1	Controles de auditoría de los sistemas de información	**P**			**P**		
15.3.2	Protección de las herramientas de auditoría de los sistemas de información			**P**	**P**		

SECCIÓN ISO/IEC 27002	CONTROLES	OBJETIVO PRIMARIO			APLICABILIDAD	
		Confidencialidad	Integridad	Disponibilidad	Aplica?	Justificación (en caso de no aplicar)
5	**Política de Seguridad**					
5.1	**Política de seguridad de la información**					
5.1.1	Documento de la política de la seguridad de la información	**P**	**P**	**P**	**P**	
5.1.2	Revisión de la política de la seguridad de la información	**P**	**P**	**P**	**P**	
6	**Organización de la seguridad de la información**					
6.1	**Organización interna**					
6.1.1	Compromiso de la gerencia con la seguridad de la información	**P**	**P**	**P**	**P**	
6.1.2	Coordinación de la seguridad de la información	**P**	**P**	**P**	**P**	
6.1.3	Asignación de las responsabilidades de la seguridad de la información	**P**	**P**	**P**	**P**	
6.1.4	Autorización de proceso para facilidades procesadoras de información	**P**	**P**	**P**	**P**	
6.1.5	Acuerdos de Confidencialidad	**P**			**P**	
6.1.6	Contacto con las autoridades	**P**	**P**	**P**	**P**	
6.1.7	Contacto con grupos de interés especial	**P**	**P**	**P**	**P**	
6.1.8	Revisión independiente de la seguridad de la información	**P**	**P**	**P**	**P**	
6.2	**Grupos o personas externas**					
6.2.1	Identificación de los riesgos relacionados con los grupos externos	**P**	**P**	**P**	**P**	
6.2.2	Tratamiento de la seguridad cuando se lidia con clientes	**P**	**P**	**P**	**P**	
6.2.3	Tratamiento de la seguridad en acuerdos con terceros	**P**	**P**	**P**	**P**	
7	**Gestión de Activos**					
7.1	**Responsabilidad por los activos**					
7.1.1	Inventario de los activos	**P**	**P**	**P**	**P**	

7.1.2	Propiedad de los activos	**P**	**P**	**P**	**P**	
7.1.3	Uso aceptable de los activos	**P**	**P**	**P**	**P**	
7.2	**Clasificación de la información**					
7.2.1	Lineamientos de clasificación		**P**	**P**	**P**	
7.2.2	Etiquetado y manejo de la información	**P**	**P**	**P**	**P**	
8	**Seguridad de Recursos Humanos**					
8.1	**Antes del empleo**					
8.1.1	Roles y responsabilidades	**P**	**P**		**P**	
8.1.2	Investigación de antecedentes	**P**	**P**	**P**	**P**	
8.1.3	Términos y condiciones del empleo	**P**	**P**	**P**	**P**	
8.2	**Durante el empleo**					
8.2.1	Responsabilidades de la gerencia	**P**	**P**	**P**	**P**	
8.2.2	Conocimiento, educación y capacitación en seguridad de la información	**P**	**P**	**P**	**P**	
8.2.3	Proceso disciplinario	**P**	**P**	**P**	**P**	
8.3	**Terminación o cambio de empleo**					
8.3.1	Responsabilidades de terminación	**P**	**P**	**P**	**P**	
8.3.2	Devolución de los activos	**P**	**P**	**P**	**P**	
8.3.3	Retiro de los derechos de acceso	**P**	**P**	**P**	**P**	
9	**Seguridad Física y Ambiental**					
9.1	**Áreas Seguras**					
9.1.1	Perímetro de la seguridad física	**P**	**P**	**P**	**P**	
9.1.2	Controles de ingreso físico	**P**	**P**	**P**	**P**	
9.1.3	Aseguramiento de oficinas, habitaciones y medios	**P**	**P**	**P**	**P**	
9.1.4	Protección contra amenazas internas y externas			**P**	**P**	
9.1.5	Trabajando en áreas aseguradas	**P**	**P**	**P**	**P**	
9.1.6	Áreas de acceso público, entrega y carga	**P**	**P**	**P**	**P**	
9.2	**Equipo de seguridad**					

9.2.1	Ubicación y protección del equipo	**P**	**P**	**P**	**P**	
9.2.2	Servicios públicos de soporte			**P**	**P**	
9.2.3	Seguridad del Cableado	**P**		**P**	**P**	
9.2.4	Mantenimiento del equipo		**P**	**P**	**P**	
9.2.5	Seguridad del equipo fuera del local	**P**	**P**	**P**		Los únicos equipos que están fuera de las instalaciones de la empresa son los CPE, por contrato, los clientes son responsables de reponer ese equipo en caso de robo, en caso de avería, el proveedor cuenta con una cantidad grande de equipos para reposición, por lo que los equipos no son asegurados. Se trata de que sean del menor costo posible
9.2.6	Seguridad de la eliminación o reuso del equipo	**P**			**P**	
9.2.7	Retiro de la propiedad	**P**	**P**	**P**	**P**	
10	**Gestión de las comunicaciones y operaciones**					
10.1	**Procedimientos y responsabilidades operacionales**					
10.1.1	Procedimientos de operación documentados	**P**	**P**	**P**	**P**	
10.1.2	Gestión de Cambio	**P**	**P**	**P**	**P**	
10.1.3	Segregación de los deberes	**P**	**P**	**P**	**P**	
10.1.4	Separación de los medios de desarrollo, prueba y operación	**P**	**P**	**P**	**P**	
10.2	**Gestión de la entrega del servicio de terceros**					
10.2.1	Entrega del servicio	**P**	**P**	**P**	**P**	

10.2.2	Monitoreo y revisión del servicio de terceros	**P**	**P**	**P**	**P**	
10.2.3	Manejo de cambios en los servicios de terceros	**P**	**P**	**P**	**P**	
10.3	**Planeación y aceptación del sistema**					
10.3.1	Gestión de la Capacidad			**P**	**P**	
10.3.2	Aceptación del sistema			**P**	**P**	
10.4	**Protección contra código malicioso y móvil**					
10.4.1	Controles contra código malicioso		**P**	**P**	**P**	
10.4.2	Controles contra códigos móviles		**P**	**P**		Este proveedor no usa tecnología móvil pública para sus operaciones
10.5	**Copia de Seguridad**					
10.5.1	Información de Copia de Seguridad		**P**	**P**	**P**	
10.6	**Gestión de la Seguridad de Red**					
10.6.1	Controles de redes	**P**	**P**	**P**	**P**	
10.6.2	Seguridad de los servicios de red	**P**	**P**	**P**	**P**	
10.7	**Gestión de Medios**					
10.7.1	Gestión de medios removibles	**P**	**P**	**P**		Este proveedor no usa tecnología de medios removibles, todo es utilizado por la red.
10.7.2	Disposición de medios	**P**	**P**	**P**	**P**	
10.7.3	Procedimientos para el manejo de la información	**P**	**P**	**P**	**P**	
10.7.4	Seguridad de la documentación del sistema	**P**	**P**		**P**	
10.8	**Intercambio de Información**					
10.8.1	Políticas y procedimientos para el intercambio de la información	**P**	**P**	**P**	**P**	
10.8.2	Acuerdos de Intercambio	**P**	**P**		**P**	

10.8.3	Medios físicos en tránsito			**P**		Este proveedor no hace traspaso de información sensible en medios físicos
10.8.4	Mensajería Electrónica	**P**	**P**	**P**	**P**	
10.8.5	Sistemas de Información Comercial	**P**	**P**			Este proveedor no usa sistemas de información comercial.
10.9	**Servicios de Comercio electrónico**					
10.9.1	Comercio electrónico	**P**	**P**			Este proveedor no tiene plataforma de e-commerce
10.9.2	Transacciones en línea	**P**	**P**			Este proveedor no tiene un portal de ventas ni de compras
10.9.3	Información públicamente disponible		**P**			Este proveedor tiene un portal meramente informativo de servicios y contactos, la información publicada ahí no es sensible
10.1	**Monitoreo**					
10.10.1	Registro de auditoría	**P**	**P**	**P**	**P**	
10.10.2	Uso del sistema de monitoreo	**P**	**P**		**P**	
10.10.3	Protección del registro de información	**P**	**P**	**P**	**P**	
10.10.4	Registros del administrador y operador	**P**	**P**	**P**	**P**	
10.10.5	Registro de fallas			**P**	**P**	
10.10.6	Sincronización de relojes		**P**		**P**	
11	**Control de Acceso**					
11.1	**Requerimiento del negocio para el control acceso**					
11.1.1	Política de control de acceso	**P**	**P**		**P**	
11.2	**Gestión de Acceso del usuario**					

11.2.1	Registro del usuario	**P**	**P**		**P**	
11.2.2	Gestión de privilegios	**P**	**P**		**P**	
11.2.3	Gestión de las claves secretas de los usuarios	**P**	**P**		**P**	
11.2.4	Revisión de los derechos de acceso del usuario	**P**	**P**		**P**	
11.3	**Responsabilidades del usuario**					
11.3.1	Uso de las claves secretas	**P**	**P**		**P**	
11.3.2	Equipo del usuario desatendido	**P**	**P**		**P**	
11.3.3	Política de escritorio y pantalla limpios	**P**			**P**	
11.4	**Control de Acceso a la Red**					
11.4.1	Política sobre el uso de los servicios de la red	**P**	**P**		**P**	
11.4.2	Autenticación del usuario para las conexiones externas	**P**	**P**		**P**	
11.4.3	Identificación del equipo en las redes	**P**	**P**		**P**	
11.4.4	Protección del puerto de diagnóstico y configuración remoto	**P**	**P**	**P**	**P**	
11.4.5	Segregación en redes	**P**	**P**		**P**	
11.4.6	Control de conexión a la red	**P**	**P**		**P**	
11.4.7	Control de enrutamiento de la red	**P**	**P**		**P**	
11.5	**Control de acceso al sistema operativo**					
11.5.1	Procedimientos para un logoneo seguro	**P**	**P**		**P**	
11.5.2	Identificación y autenticación del usuario	**P**	**P**		**P**	
11.5.3	Sistema de gestión de claves secretas	**P**	**P**		**P**	
11.5.4	Uso de las utilidades del sistema	**P**	**P**	**P**	**P**	
11.5.5	Cierre de sesión por inactividad	**P**	**P**		**P**	
11.5.6	Limitación del tiempo de conexión	**P**	**P**		**P**	
11.6	**Control de acceso a la aplicación y la información**					
11.6.1	Restricción de acceso a la información	**P**	**P**		**P**	

11.6.2	Aislar el sistema confidencial	**P**	**P**		**P**	
11.7	**Computación móvil y tele trabajo**					
11.7.1	Computación móvil y comunicaciones	**P**	**P**	**P**		Este proveedor no tiene un plataforma para transacciones móviles para clientes ni empleados
11.7.2	Tele trabajo	**P**	**P**		**P**	
12	**Adquisición, desarrollo y mantenimiento de los sistemas de información**					
12.1	**Requerimientos de seguridad de los sistemas de información**					
12.1.1	Análisis y especificación de los requerimientos de seguridad	**P**	**P**	**P**	**P**	
12.2	**Procesamiento correcto en las aplicaciones**					
12.2.1	Validación de la input data		**P**		**P**	
12.2.2	Control del procesamiento interno		**P**		**P**	
12.2.3	Integridad del mensaje		**P**		**P**	
12.2.4	Validación de la output data		**P**		**P**	
12.3	**Controles Criptográficos**					
12.3.1	Política sobre el uso de controles criptográficos	**P**	**P**		**P**	
12.3.2	Gestión de claves	**P**	**P**		**P**	
12.4	**Seguridad de los archivos del sistema**					
12.4.1	Control del software operacional	**P**	**P**	**P**	**P**	
12.4.2	Protección de la data del sistema		**P**		**P**	
12.4.3	Control de acceso al código fuente del programa		**P**		**P**	
12.5	**Seguridad en los procesos de desarrollo y soporte**					
12.5.1	Procedimientos del control de cambios		**P**	**P**	**P**	
12.5.2	Revisión técnica de la aplicación después de cambios en el sistema		**P**		**P**	

12.5.3	Restricciones sobre los cambios en los paquetes de software		**P**			Este proveedor tiene su propio departamento de desarrollo de software y sus propios sistemas de información
12.5.4	Filtración de la información	**P**				La información sensible no está disponible para colaboradores.
12.5.5	Desarrollo de software abastecido externamente	**P**	**P**			Este proveedor tiene su propio departamento de desarrollo de software y sus propios sistemas de información
12.6	**Gestión de la Vulnerabilidad técnica**					
12.6.1	Control de las vulnerabilidades técnicas		**P**			Los sistemas de información son de acceso vía browser y se ejecutan sobre plataformas de software libre.
13	**Gestión de un incidente en la seguridad de la información**					
13.1	**Reporte de los eventos y debilidades de la seguridad de la información**					
13.1.1	Reporte de eventos en la seguridad de la información	**P**	**P**	**P**	**P**	
13.1.2	Reporte de las debilidades en la seguridad	**P**	**P**	**P**	**P**	
13.2	**Gestión de los incidentes y mejoras en la seguridad de la información**					
13.2.1	Responsabilidades y procedimientos	**P**	**P**	**P**	**P**	
13.2.2	Aprender de los incidentes en la seguridad de la información	**P**	**P**	**P**	**P**	
13.2.3	Recolección de evidencia	**P**	**P**	**P**	**P**	
14	**Gestión de la continuidad del Negocio**					
14.1	**Aspecto de la seguridad de la información de la gestión de la continuidad del negocio**					

14.1.1	Incluir la seguridad de la información en el proceso de la gestión de continuidad del negocio			**P**	**P**	
14.1.2	Continuidad del negocio y evaluación del riesgo			**P**	**P**	
14.1.3	Desarrollar e implementar los planes de continuidad incluyendo seguridad de información			**P**	**P**	
14.1.4	Marco referencial de la planeación de la continuidad del negocio			**P**	**P**	
14.1.5	Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio			**P**	**P**	
15	**Cumplimiento**					
15.1	**Cumplimiento de los requerimientos legales**					
15.1.1	Identificación de la legislación aplicable	**P**	**P**	**P**	**P**	
15.1.2	Derechos de propiedad intelectual	**P**			**P**	
15.1.3	Protección de los registros organizacionales	**P**	**P**	**P**	**P**	
15.1.4	Protección de la data y de la privacidad de la información personal	**P**				Este proveedor prohíbe que sus colaboradores utilicen los sistemas de hardware y software con fines personales
15.1.5	Prevención del mal uso de los medios de procesamiento de la información			**P**		Este proveedor bloquea el mal uso de los sistemas de hardware y software de la organización
15.1.6	Regulación de los controles criptográficos	**P**				Este control es redundante y ya es tratado en el sección 12.3
15.2	**Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico**					
15.2.1	Cumplimiento con las políticas[y estándares de seguridad	**P**	**P**	**P**	**P**	

15.2.2	Chequeo del cumplimiento técnico	**P**	**P**		**P**	
15.3	**Consideraciones de auditoría de los sistemas de información**					
15.3.1	Controles de auditoría de los sistemas de información			**P**	**P**	
15.3.2	Protección de las herramientas de auditoría de los sistemas de información		**P**		**P**	

Nota: La letra "P" representa: validado, seleccionado, chequeado (passed, chequed, validated).

SECCIÓN ISO/IEC 27002	CONTROLES	IMPLEMENTACIÓN Departamentos	Sistemas
5	**Política de Seguridad**		
5.1	**Política de seguridad de la información**		
5.1.1	Documento de la política de la seguridad de la información	Documentación	
5.1.2	Revisión de la política de la seguridad de la información	Reuniones Semestrales con la Gerencia	Sistema de Bitácora de Reuniones y préstamo de sala de sesiones
6	**Organización de la seguridad de la información**		
6.1	**Organización interna**		
6.1.1	Compromiso de la gerencia con la seguridad de la información	Documentación y planeación	
6.1.2	Coordinación de la seguridad de la información	El departamento de CERT (Computer Emergency Team) ha sido creado como coordinador general del sistema de gestión de la seguridad de la información	
6.1.3	Asignación de las responsabilidades de la seguridad de la información	Las responsabilidades han sido asignadas en las tareas de todas las jefaturas	
6.1.4	Autorización de proceso para facilidades procesadoras de información	Documentación	
6.1.5	Acuerdos de Confidencialidad	Documentación	
6.1.6	Contacto con las autoridades	Departamento Legal	
6.1.7	Contacto con grupos de interés especial	Gerencia Técnica	
6.1.8	Revisión independiente de la seguridad de la información	Consultorías Externas	
6.2	**Grupos o personas externas**		
6.2.1	Identificación de los riesgos relacionados con los grupos externos	CERT	
6.2.2	Tratamiento de la seguridad cuando se lidia con clientes	Documentación y Contratos	
6.2.3	Tratamiento de la seguridad en acuerdos con terceros	Documentación y Contratos	
7	**Gestión de Activos**		

7.1	**Responsabilidad por los activos**		
7.1.1	Inventario de los activos	Bodega y Jefaturas	Sistema de Inventarios
7.1.2	Propiedad de los activos	Jefaturas y Colaboradores	Sistema de Inventarios
7.1.3	Uso aceptable de los activos	Jefaturas y Colaboradores	
7.2	**Clasificación de la información**		
7.2.1	Lineamientos de clasificación	CERT	
7.2.2	Etiquetado y manejo de la información	CERT	
8	**Seguridad de Recursos Humanos**		
8.1	**Antes del empleo**		
8.1.1	Roles y responsabilidades	Departamento de Desarrollo Humano	Sistema de Nomina e Intranet
8.1.2	Investigación de antecedentes	Departamento de Desarrollo Humano	Sistema de Nomina e Intranet
8.1.3	Términos y condiciones del empleo	Departamento de Desarrollo Humano	Sistema de Nomina e Intranet
8.2	**Durante el empleo**		
8.2.1	Responsabilidades de la gerencia	Gerencias	
8.2.2	Conocimiento, educación y capacitación en seguridad de la información	Gerencia Técnica y CERT	Biblioteca, sistema de videoconferencia en alta definición, grabación de las sesiones de capacitación
8.2.3	Proceso disciplinario	Jefaturas	Sistema de Incidencias laborales y desempeño laboral. Sistema de control de asistencia
8.3	**Terminación o cambio de empleo**		
8.3.1	Responsabilidades de terminación	Departamento de Desarrollo Humano	Sistema de Nomina e Intranet
8.3.2	Devolución de los activos	Departamento de Desarrollo Humano	Sistema de Nomina e Intranet
8.3.3	Retiro de los derechos de acceso	CERT	Sistema de Autenticación, Autorización y Registro
9	**Seguridad Física y Ambiental**		
9.1	**Áreas Seguras**		
9.1.1	Perímetro de la seguridad física	Gerencia Técnica y CERT	Sistemas de seguridad, video vigilancia, vigilancia privada, sistema contra incendios
9.1.2	Controles de ingreso físico	Gerencia Administrativa y CERT	Sistemas de seguridad, video vigilancia y vigilancia privada

9.1.3	Aseguramiento de oficinas, habitaciones y medios	Gerencia Administrativa y CERT	Sistema de video vigilancia, vigilancia privada y sistema contra incendios
9.1.4	Protección contra amenazas internas y externas	Gerencia Administrativa y CERT	Vigilancia privada, alarmas, convenio con Departamento de Policía
9.1.5	Trabajando en áreas aseguradas	Gerencia Administrativa y CERT	Sistemas de seguridad, video vigilancia, vigilancia privada, sistema contra incendios
9.1.6	Áreas de acceso público, entrega y carga	Gerencia Administrativa y CERT	Vigilancia privada, alarmas y video vigilancia.
9.2	**Equipo de seguridad**		
9.2.1	Ubicación y protección del equipo	Jefaturas	
9.2.2	Servicios públicos de soporte	Gerencia Administrativa y CERT	
9.2.3	Seguridad del Cableado	Jefaturas y Departamento de Servicios de Cableado y Escritorio	Departamento de Servicios de Cableado y Escritorio
9.2.4	Mantenimiento del equipo	Jefaturas y Departamento de Servicios de Cableado y Escritorio	Departamento de Servicios de Cableado y Escritorio
9.2.5	Seguridad del equipo fuera del local		Routers con seguridades lógicas y hardware robusto que soporta cambios bruscos de temperatura
9.2.6	Seguridad de la eliminación o reuso del equipo	Jefaturas y Departamento de Servicios de Cableado y Escritorio	Departamento de Servicios de Cableado y Escritorio
9.2.7	Retiro de la propiedad	Desarrollo Humano y Jefaturas	
10	**Gestión de las comunicaciones y operaciones**		
10.1	**Procedimientos y responsabilidades operacionales**		

10.1.1	Procedimientos de operación documentados	Jefaturas	Sistema de Gestión de Cambios, MOPs
10.1.2	Gestión de Cambio	Jefaturas y Sistemas	Sistema de Gestión de Cambios, MOPs
10.1.3	Segregación de los deberes	Gerencias, CERT y Jefaturas	
10.1.4	Separación de los medios de desarrollo, prueba y operación	Jefaturas y Sistemas	
10.2	**Gestión de la entrega del servicio de terceros**		
10.2.1	Entrega del servicio	IAC, BANCOS, OTN	IAC, BANCOS, OTN
10.2.2	Monitoreo y revisión del servicio de terceros	NOC, IAC, BANCOS, OTN	Sistema de Monitoreo de Enlaces
10.2.3	Manejo de cambios en los servicios de terceros	COMERCIAL, ADMINISTRATIVO, NOC, IAC, BANCOS, OTN	Sistema de Gestión de Red
10.3	**Planeación y aceptación del sistema**		
10.3.1	Gestión de la Capacidad	Gerencia Técnica y Sistemas	
10.3.2	Aceptación del sistema	Gerencia Técnica y Sistemas	
10.4	**Protección contra código malicioso y móvil**		
10.4.1	Controles contra código malicioso	CERT y Jefaturas	Servidor Centralizado de Antispam, anti virus, malware
10.4.2	Controles contra códigos móviles	Este proveedor no usa tecnología móvil pública para sus operaciones	
10.5	**Copia de Seguridad**		
10.5.1	Información de Copia de Seguridad	CERT y Jefaturas	Sistema de Respaldos
10.6	**Gestión de la Seguridad de Red**		
10.6.1	Controles de redes	CERT y Jefaturas	Firewall, IPS, IDS
10.6.2	Seguridad de los servicios de red	CERT y Jefaturas	Firewall, IPS, IDS
10.7	**Gestión de Medios**		
10.7.1	Gestión de medios removibles		
10.7.2	Disposición de medios	CERT y Jefaturas	

10.7.3	Procedimientos para el manejo de la información	CERT y Jefaturas	
10.7.4	Seguridad de la documentación del sistema	Gerencia, CERT y Jefaturas	Sistema de Respaldos
10.8	**Intercambio de Información**		
10.8.1	Políticas y procedimientos para el intercambio de la información	Gerencia y CERT	Firewall y VPNs
10.8.2	Acuerdos de Intercambio	CERT	Firewall y VPNs
10.8.3	Medios físicos en tránsito		
10.8.4	Mensajería Electrónica	CERT y Networking	Firmas Digitales
10.8.5	Sistemas de Información Comercial		
10.9	**Servicios de Comercio electrónico**		
10.9.1	Comercio electrónico		
10.9.2	Transacciones en línea		
10.9.3	Información públicamente disponible		
10.1	**Monitoreo**		
10.10.1	Registro de auditoría	CERT y Networking	Sistema de Autenticación, Autorización y Registro
10.10.2	Uso del sistema de monitoreo	CERT y Networking	Sistema de Autenticación, Autorización y Registro
10.10.3	Protección del registro de información	CERT y Networking	Sistema de Autenticación, Autorización y Registro
10.10.4	Registros del administrador y operador	CERT y Networking	Sistema de Autenticación, Autorización y Registro
10.10.5	Registro de fallas	CERT, Networking y Sistemas	Sistema de Registro de Incidentes de Seguridad de la información

10.10.6	Sincronización de relojes	CERT y Networking	Servidor NTP
11	**Control de Acceso**		
11.1	**Requerimiento del negocio para el control acceso**		
11.1.1	Política de control de acceso	CERT, Gerencia Administrativa y Sistemas	Sistema de Autenticación, Autorización y Registro
11.2	**Gestión de Acceso del usuario**		
11.2.1	Registro del usuario	CERT y Sistemas	Controlador de Dominio
11.2.2	Gestión de privilegios	CERT y Sistemas	Controlador de Dominio
11.2.3	Gestión de las claves secretas de los usuarios	CERT y Sistemas	Controlador de Dominio
11.2.4	Revisión de los derechos de acceso del usuario	CERT y Sistemas	Controlador de Dominio
11.3	**Responsabilidades del usuario**		
11.3.1	Uso de las claves secretas	CERT y Jefaturas	Sistema de Autenticación, Autorización y Registro
11.3.2	Equipo del usuario desatendido	CERT y Jefaturas	Controlador de Dominio
11.3.3	Política de escritorio y pantalla limpios	CERT y Jefaturas	Controlador de Dominio
11.4	**Control de Acceso a la Red**		
11.4.1	Política sobre el uso de los servicios de la red	CERT y Sistemas	
11.4.2	Autenticación del usuario para las conexiones externas	CERT y Sistemas	Servidor VPN y Acceso Remoto
11.4.3	Identificación del equipo en las redes	CERT y Sistemas	Controlador de Dominio
11.4.4	Protección del puerto de diagnóstico y configuración remoto	CERT y Sistemas	Controlador de Dominio
11.4.5	Segregación en redes	CERT	Routers Switches y Vlans
11.4.6	Control de conexión a la red	CERT	Servidor VPN y Acceso Remoto
11.4.7	Control de enrutamiento de la red	CERT	Routers
11.5	**Control de acceso al sistema operativo**		
11.5.1	Procedimientos para un logoneo seguro	Sistemas	Sistema de Autenticación, Autorización y Registro
11.5.2	Identificación y autenticación del usuario	Sistemas	Controlador de Dominio
11.5.3	Sistema de gestión de claves secretas	Sistemas	Controlador de Dominio

11.5.4	Uso de las utilidades del sistema	Sistemas	Controlador de Dominio
11.5.5	Cierre de sesión por inactividad	CERT y Sistemas	Sistema de Autenticación, Autorización y Registro. Controlador de Dominio y Servidor de VPN
11.5.6	Limitación del tiempo de conexión	CERT y Sistemas	Sistema de Autenticación, Autorización y Registro. Controlador de Dominio y Servidor de VPN
11.6	**Control de acceso a la aplicación y la información**		
11.6.1	Restricción de acceso a la información	CERT y Sistemas	Controlador de Dominio y perfiles en SIT
11.6.2	Aislar el sistema confidencial	CERT y Sistemas	Controlador de Dominio y perfiles en SIT
11.7	**Computación móvil y tele trabajo**		
11.7.1	Computación móvil y comunicaciones		
11.7.2	Tele trabajo	CERT y Sistemas	Sistema de Autenticación, Autorización y Registro. Controlador de Dominio y Servidor de VPN
12	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
12.1	**Requerimientos de seguridad de los sistemas de información**		
12.1.1	Análisis y especificación de los requerimientos de seguridad	Sistemas	
12.2	**Procesamiento correcto en las aplicaciones**		
12.2.1	Validación de la input data	Sistemas	
12.2.2	Control del procesamiento interno	Sistemas	
12.2.3	Integridad del mensaje	Sistemas	
12.2.4	Validación de la output data	Sistemas	
12.3	**Controles Criptográficos**		
12.3.1	Política sobre el uso de controles criptográficos	CERT	Servidor de VPN, Controlador de Dominio
12.3.2	Gestión de claves	CERT y Sistemas	Sistema de Autenticación, Autorización y Registro.
12.4	**Seguridad de los archivos del sistema**		

12.4.1	Control del software operacional	Sistemas	
12.4.2	Protección de la data del sistema	Sistemas	
12.4.3	Control de acceso al código fuente del programa	Sistemas	
12.5	**Seguridad en los procesos de desarrollo y soporte**		
12.5.1	Procedimientos del control de cambios	CERT y Sistemas	Sistema de Control de Cambios
12.5.2	Revisión técnica de la aplicación después de cambios en el sistema	CERT y Sistemas	Sistema de Control de Cambios
12.5.3	Restricciones sobre los cambios en los paquetes de software		
12.5.4	Filtración de la información		
12.5.5	Desarrollo de software abastecido externamente		
12.6	**Gestión de la Vulnerabilidad técnica**		
12.6.1	Control de las vulnerabilidades técnicas		
13	**Gestión de un incidente en la seguridad de la información**		
13.1	**Reporte de los eventos y debilidades de la seguridad de la información**		
13.1.1	Reporte de eventos en la seguridad de la información	Jefaturas, colaboradores y Sistemas	Sistema de Registro y Seguimiento de Incidentes de Seguridad de la información
13.1.2	Reporte de las debilidades en la seguridad	Jefaturas, colaboradores y Sistemas	Sistema de Registro y Seguimiento de Incidentes de Seguridad de la información
13.2	**Gestión de los incidentes y mejoras en la seguridad de la información**		
13.2.1	Responsabilidades y procedimientos	Todos los departamentos y Gerencias	Sistema de Registro y Seguimiento de Incidentes de Seguridad de la información

13.2.2	Aprender de los incidentes en la seguridad de la información	Todos los departamentos y Gerencias	Sistema de Registro y Seguimiento de Incidentes de Seguridad de la información
13.2.3	Recolección de evidencia	Jefaturas, colaboradores y Sistemas	Sistema de Registro y Seguimiento de Incidentes de Seguridad de la información
14	**Gestión de la continuidad del Negocio**		
14.1	**Aspecto de la seguridad de la información de la gestión de la continuidad del negocio**		
14.1.1	Incluir la seguridad de la información en el proceso de la gestión de continuidad del negocio	Gerencia General, Gerencia Técnica, CERT y NOC	
14.1.2	Continuidad del negocio y evaluación del riesgo	Gerencia General, Gerencia Técnica, CERT y NOC	PBX IP, enlaces redundantes, data center redundante, proveedores de telefonía y comunicaciones redundantes
14.1.3	Desarrollar e implementar los planes de continuidad incluyendo seguridad de información	Gerencia General, Gerencia Técnica, CERT y NOC	PBX IP, enlaces redundantes, data center redundante, proveedores de telefonía y comunicaciones redundantes
14.1.4	Marco referencial de la planeación de la continuidad del negocio	Gerencia General, Gerencia Técnica, CERT y NOC	
14.1.5	Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio	Gerencia Técnica, CERT, Sistemas y NOC	
15	**Cumplimiento**		
15.1	**Cumplimiento de los requerimientos legales**		
15.1.1	Identificación de la legislación aplicable	Departamento Legal	Departamento Legal
15.1.2	Derechos de propiedad intelectual	CERT y Departamento Legal	CERT y Departamento Legal
15.1.3	Protección de los registros organizacionales	Gerencia Técnica, CERT, Sistemas y NOC	Gerencia Técnica, CERT, Sistemas y NOC
15.1.4	Protección de la data y de la privacidad de la información personal		
15.1.5	Prevención del mal uso de los medios de procesamiento de la información		

15.1.6	Regulación de los controles criptográficos		
15.2	**Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico**		
15.2.1	Cumplimiento con las políticas y estándares de seguridad	CERT	
15.2.2	Chequeo del cumplimiento técnico	CERT	
15.3	**Consideraciones de auditoría de los sistemas de información**		
15.3.1	Controles de auditoría de los sistemas de información	CERT y Jefaturas	
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	CERT y Jefaturas	

ANEXO 10

POLÍTICAS ESPECÍFICAS

POLÍTICA, ORGANIZACIÓN y RESPONSABILIDADES DE LA SEGURIDAD DE INFORMACIÓN

3 La política de seguridad de Información debe ser de conocimiento y cumplimiento para todos los empleados.

4 Esta política será revisada y actualizada anualmente por parte del comité de seguridad o en su defecto cuando haya cambiado uno de los objetivos dentro del negocio de la empresa y cuando la situación lo amerite.

5 La política de Seguridad será explícitamente aprobada por la Gerencia General.

6 La Gerencia General debe apoyar activamente la seguridad de la información dentro de la organización a través de un compromiso demostrado y la asignación de las responsabilidades de seguridad de la información. Para ello, dentro del presupuesto anual se definirán rubros para la implementación de nuevos proyectos de seguridad de la información.

7 Los Jefes Departamentales serán los responsables de coordinar y organizar las actividades respecto a seguridad de la información en sus departamentos. Entiéndase estas como: Preparación para auditorías, manejos, reporte, tratamiento de Incidencias, capacitación , elaboración de procesos, documentos, diagramas, mantenimientos de registros, acciones correctivas, acciones preventivas, revisión y corrección de procesos interdepartamentales, implementación y revisión de controles, medición de indicadores asignados a estos controles. Dpto. de Seguridad Lógica de la Empresa brindará el soporte a las Jefaturas para la realización de las acciones arriba indicadas.

8 La Organización reconocerá a los empleados por cumplimiento de todos sus deberes y responsabilidades dentro del sistema de gestión de seguridad de información con un BONO de hasta el 7,5% de su sueldo. El valor acreditado será directamente proporcional al cumplimiento. El incumplimiento de estos deberes y responsabilidades serán considerados dentro de la Evaluación Anual de Gerentes y Jefaturas, que realiza el departamento de recursos humanos en conjunto con el directorio de la empresa.

9 La periodicidad de las auditorías externas e internas de seguimiento del sistema de gestión de seguridad de información será semestral.

10 El departamento Legal será el encargado de mantener contacto con las autoridades o estar actualizado con los reglamentos pertinentes para que se cumplan los requisitos legales definidos en el SGSI.

11 Es responsabilidad del departamento de recursos humanos solicitar la firma de un acuerdo de confidencialidad a todos los empleados. Estos documentos serán

mantenidos por el departamento de recursos humanos.

12 Cada Jefe Departamental debe solicitar la firma de compromisos de confidencialidad con los contratistas existentes: contratistas de cableado de fibra óptica, de fabricación y colocación de torres para equipos de radio, de obras civiles, con una actividad continúa en la empresa mayor a 1 mes. Estos documentos serán mantenidos por cada departamento y copia a recursos humanos.

13 Cada gerente o jefe departamental analizará y evaluará el riesgo ante la contratación de un servicio y definirá si es necesario la firma de un acuerdo confidencialidad, en base a las políticas establecidas por el departamento de seguridad lógica.

14 Todo pasante o cliente que realice actividades dentro de la empresa con el motivo de pruebas de laboratorio o aprendizaje firmará un acuerdo de confidencialidad que será mantenido por el departamento involucrado y con copia al departamento de recursos humanos.

15 Las visitas técnicas de terceros a las instalaciones serán autorizadas por la gerencia técnica regional y se permitirán con el acompañamiento de un representante de la empresa. Quedan prohibidas las fotos o anotaciones donde sean legibles los detalles de diagramas, direccionamiento IP de equipos, nombres de equipos, se respetarán los acuerdos de confidencialidad firmados.

MANEJO DE INFORMACION

16 Todos los documentos son considerados confidenciales excepto las notificaciones de trabajo a clientes, notificaciones de incidencias a clientes externos, reportes para clientes, publicidad de la compañía.

17 La información confidencial solicitada por un cliente será entregada cumpliendo el compromiso de confidencialidad previamente firmado por el representante de la empresa que interactúa con el cliente. El gerente o jefe departamental mantendrá y registrará esta documentación. El documento de confidencialidad tendrá las aprobaciones de departamento de seguridad lógica, gerencia general y gerencia/subgerencia técnica regional.

18 Toda la solicitud de información interdepartamental alejada de procesos laborales entre los departamentos, deberá ser registrada y mantenida por el gerente y jefe departamental.

19 Para el tratamiento de la seguridad de la información en las relaciones con los clientes se debe seguir lo establecido en el Documento: Políticas de Seguridad con Clientes POL SEC 02.

GESTIÓN ACTIVOS

20 Todos los Gerentes o Jefes departamentales deben tener un inventario de los Activos de Información físicos o de procesamiento que manejen. Este inventario debe ser actualizado en la carpeta respectiva dentro del servidor de Intranet cada vez que se produzca algún cambio

21 Los Gerentes o Jefes Departamentales serán los responsables de velar por los activos de información que están asignados al departamento a su cargo. En caso

de la asignación de un nuevo activo, serán quienes elabore el análisis y evaluación y tratamiento de riesgo relacionado a este activo para su posterior implantación de controles si los resultados lo ameritan. Los Gerentes/Jefes Departamentales recibirán la ayuda del Departamento de Seguridad Lógica en torno a la gestión del riesgo.

22 Todos los Gerentes o Jefes departamentales son los responsables de medir la efectividad de los controles asignados a sus activos u operaciones y deberán enviar un reporte mensual de los mismos al Dpto. de Seguridad con copia a GTN/SGTN y Gerencia General. El Dpto. de Seguridad calculará en base a esto el bono de Seguridad mencionado en el inciso # 6.

RECURSOS HUMANOS

23 La implementación, mantenimiento y registro del proceso formal de vinculación, inducción y desvinculación a la compañía será llevado a cabo por el Departamento de Desarrollo Humanos, y debe contemplar directrices de Seguridad de la información definidas por el Departamento de Seguridad Lógica.

24 Todas las responsabilidades, funciones y competencias de los empleados respecto a la seguridad de información deben estar registrados dentro de su hoja de vida manejada por DDHH o en el sistema de información del departamento de recursos humanos.

25 Toda mala conducta que atente contra la seguridad de información de la compañía será sancionada según lo descrito en el reglamento interno de la compañía.

26 Los datos personales de los empleados deben ser tratados de forma privada.

27 El cumplimiento de políticas y procedimientos del Sistema de Gestión de la Seguridad de Información será una de las métricas consideradas en la evaluación anual del personal.

SEGURIDAD FÍSICA, AMBIENTAL, DE INSTALACIONES Y MANEJO DE EQUIPAMIENTO

28 Todos los Tele-puertos de la empresa deben poseer mecanismos de control de acceso ya sean automáticos o manuales y dichos registros deben ser almacenados durante 1 mes en medios magnéticos o físicos.

29 Todos los empleados que ingresen a un Tele-puerto o Nodo deben registrar su entrada y salida de dicho nodo.

30 Los Responsables de los Tele-puertos deben velar por el cumplimiento de las buenas prácticas establecidas y mantener una constante retroalimentación con GTR.

31 Todo equipo debe ser mantenido en perfecto estado de funcionamiento, por lo que deberá ser revisado periódicamente por el departamento custodio del mismo o por el personal a cargo (si tiene la capacitación para la revisión del mismo), de ser equipo especializado deberá ser enviado a centros técnicos acreditados para realizar las revisiones y mantenimientos adecuados.

32 Todo equipo debe ser guardado en lugares seguros cuando no está siendo utilizado.

33 Las áreas operativas cuentan con check-list de herramientas, las cuales deben ser mantenidas en vigencia.

34 Herramientas que por uso hayan sufrido desgaste o que no sirvan para su propósito deberán ser cambiadas a través del departamento de bodega, quien deberá recibir el requerimiento respectivo para reemplazo de herramienta y proceder con el cambio de la misma. La herramienta desgastada debe ser devuelta antes de la entrega de la nueva.

35 Al regresar de cualquier trabajo, las baterías de las linternas, radios, equipos de medición deben ser puestas a cargar, si se trata de pilas descartables las mismas deberán ser eliminadas y colocar nuevas como reemplazo en las unidades.

36 Los vehículos de los departamentos operativos deben quedar cargados con gasolina en las noches (tanque de gasolina mínimo con ¾).

37 Todo vehículo debe tener en perfecto estado la llanta de emergencia y tener llave de ruedas, gata, triángulos de emergencia, extintor.

38 Generadores a gasolina deben ser guardados en lugares ventilados y fuera de sitios transitados o expuestos al personal.

39 Tanques de gas deben ser guardados en lugar seguro, ventilado y de preferencia en el Tele-puerto.

40 Se debe tener tanto los tanques de gas como los generadores a gasolina, llenos.

41 Cuando los equipos queden a bordo de los vehículos, se debe levantar un inventario de lo que se deja (sea equipo o no) con los guardias de la entrada para constancia.

42 Todo equipo, vehículo, herramienta que se detecte que comienza a fallar deberá ser reportado INMEDIATAMENTE para tomar las acciones correspondientes y garantizar así que las cuadrillas tienen los equipos en excelente estado de funcionamiento.

43 En el caso de pérdida o daño de equipo o herramienta, que no sea imputable al uso normal del mismo o que se dé por negligencia del custodio, el valor de ésta será cobrada por su respectivo valor actual y será repuesta.

44 En caso de pérdida de herramienta o equipo, queda terminantemente prohibida la compra y reemplazo del mismo sin conocimiento y autorización de la GTN/SGTN y de la Gerencia Financiera Nacional.

SERVICIO DE APOYO

45 Toda instalación (nodo, repetidora, tele-puertos, oficinas) debe tener las seguridades eléctricas estandarizadas por el departamento eléctrico de la empresa con aprobación de GTN/SGTN.

46 Las instalaciones deben tener respaldos eléctricos como UPS´s, banco de baterías, ATS´s, generadores, climatización, de acuerdo a la estandarización definida.

47 Las instalaciones deben contar con supresores de picos, en los lugares que se amerite deberán contar con pararrayos, mallas de tierras.

48 Los UPS´s deben tener sistema de monitoreo para poder observar los tiempos de carga, tiempos de respaldo, alarmas a distancia que indiquen el momento en que han entrando a funcionar.

49 Los sitios que por su naturaleza de operación tengan generadores a gas, deberán tener un sistema de monitoreo de capacidad de los tanques (balanzas) que adviertan del consumo del mismo para proceder con sus recargas.

50 Los sistemas de climatización, dependiendo de la funcionalidad del sitio en donde se encuentren deberán tener sistemas de encendido automático al momento de regresar la energía eléctrica.

51 Existirán sitios los cuales tendrán instalados sensores de movimiento, apertura de puerta, arranque de generador, cámaras de video para mantener el control de los nodos / repetidoras y sus accesos, autorizados o no.

SEGURIDAD DEL CABLEADO

52 Toda instalación eléctrica deberá ser validada por el Jefe Eléctrico, quien se guiará por el diseño del Gerente de Área Nacional

53 En los telepuertos, cuartos fríos e instalaciones críticas de la empresa, sólo podrán realizar el cableado el personal autorizado por GTR para dicha labor, ningún departamento está autorizado a que por sí sólo realice cableado para sus trabajos, o pruebas en estos sitios.

54 En los nodos / repetidoras, el cableado deberá ser mantenido con orden, limpieza, identificación, y colocado dentro de los organizadores de cables.

55 Todo deterioro o daño de cableado deberá ser reportado al departamento eléctrico quien a su vez será el responsable de tomar las medidas correctivas y preventivas necesarias.

56 Todo cableado en nodos o Telepuertos deben cumplir los estándares de cableado definidos por GTN/SGTN.

MANTENIMIENTO DE EQUIPOS

57 Todo equipo deberá regirse al manual del fabricante para tomar nota de los mantenimientos recomendados, tanto en periodicidad como en fechas específicas indicadas por el mismo.

58 Se debe tener archivadas las garantías de todos los equipos, así como los registros de los mantenimientos para tener un histórico de estos.

59 Cuando se requiera dar mantenimiento a cualquier equipo, este debe ser retirado de operación y colocar uno de reemplazo hasta que el primero sea reintegrado a sus labores.

60 Los equipos eléctricos de los nodos / repetidoras serán monitoreados dentro de los mantenimientos planificados del departamento eléctrico, quienes en base a un

cronograma darán el mismo a nivel nacional.

61 Se efectuarán mensualmente pruebas de contingencia de los sistemas eléctricos y sus respaldos para detectar oportunamente algún elemento o sistema con problemas para su inmediata solución. El Departamento de Instalaciones Eléctricas mantendrá el registro de las revisiones mensuales.

62 Los vehículos de los departamentos operativos se regirán a las tablas de kilometraje recorrido para sus mantenimientos menores y mayores, esto no exime de mantenimientos en cualquier momento por la detección de cualquier problema.

63 Si se tratase de equipo computacional, este deberá ser reportado al jefe inmediato superior para que este contacte al encargado del soporte a nivel de esta clase de equipos, para que proceda con la revisión y solución del problema presentado, en caso de ser necesario que indique si el equipo debe ser cambiado para que el jefe tramite el cambio del mismo, lo antes posible.

SEGURIDAD DE EQUIPOS FUERA DE LAS INSTALACIONES DE LA ORGANIZACIÓN

64 Al llegar a la oficina con equipo de cómputo deberemos llamar al guardia para que sea él quien baje el equipo y lo ingrese a la empresa, en este lapso se procederá a parquear el vehículo en el que llegamos.

65 En caso de llegar en vehículo de alquiler o que alguien nos deje en la puerta, igual llamaremos al guardia para que esté cerca al momento de bajarnos del carro.

66 Equipos de cómputo deben ser dejados momentáneamente con el guardia a la salida, hasta que se traiga el vehículo en el cual nos iremos.

67 Si nos recogen, deberemos pedir al guardia que nos acompañe hasta abordar el vehículo que ha venido por nosotros.

68 Si los equipos son los de las cuadrillas de trabajo operativo, estos deberán ser colocados correctamente en el interior de los vehículos para que vayan seguros y no sufran daño en la transportación.

69 Ningún equipo de trabajo debe ser dejado sin observación por parte del personal de la empresa o del custodio del mismo.

70 El custodio del equipo es el responsable del mismo, por lo que debe evitar “prestar” su equipo, o enviar el mismo con otra persona a las oficinas o cualquier otra ubicación.

71 Cuando se deba trabajar en sitios poco seguros de la ciudad o campo, se deberá solicitar al departamento administrativo que proporcione resguardo adicional para trabajar en el sitio.

SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACION DE EQUIPOS

72 Toda información que se tenga almacenada en los equipos de medición, deberá ser guardada como respaldo en medios magnéticos, en equipo de la oficina que no sea sacado de la oficina, antes de volver a utilizarlo evitando con esto que dicha información se pierda en la nueva utilización.

73 Las cámaras fotográficas provistas por la empresa se consideran herramientas de trabajo, y al regresar a la oficina toda la información que se encuentre en ellas debe ser archivada en la computadora asignada al colaborador en la empresa, medios magnéticos asignados, servidor de archivos de la empresa, etc.

74 Cuando los equipos deban ser dados de baja por cualquier razón y los mismos tenga discos duros como elementos de ellos, estos deben ser formateados para asegurarnos que no queda información que pueda ser recuperada por terceros, si el disco duro no puede ser formateado este deberá ser destruido.

75 Todos los equipos que se den de baja deberán cumplir con las políticas administrativas y de auditoría para eliminación de activos de la empresa.

RETIRO DE LA PROPIEDAD

76 Solo personal autorizado puede sacar equipos de cómputo con información de la empresa, acorde a sus áreas de trabajo.

77 Todo el personal debe cumplir las disposiciones dadas por el departamento de Seguridad Lógica en cuanto a encriptación de información en el disco duro.

78 Toda instalación de software deberán ser manejada por el responsable de seguridad lógica a cargo de esta actividad.

79 Cuando se trate de software especializado, éstos deberán estar bajo custodia del departamento que los utiliza y como protección deberán ser archivados en un servidor de la empresa.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

80 La documentación de procesos operativos generados por la GTR serán publicados internamente a las áreas que corresponda tener conocimiento de ella, o a toda la empresa si es de interés general.

81 Esta documentación estará bloqueada como sistema de control sobre la misma, con lo cual no se podrá cambiar / modificar / eliminar / agregar nada que no tenga autorización del área creadora de la propia documentación.

82 Cuando cualquier área requiera conocer la documentación sobre un tema específico operativo deberá requerirla al área de forma escrita e indicar cuál es la finalidad de la solicitud.

83 Si no existiese documentación sobre algún procedimiento que sea requerido por alguna de las áreas y fuera necesario para la misma el tenerlo, dicha área en conjunto con GTR y GP la elaborarán y una vez definido y pulido, se procederá a la publicación de la misma a nivel interno.

84 El literal 80 no exime de que cada área por si misma pueda crear sus propios documentos operativos que apliquen al interior de la misma, GTR y GP pueden ser consultados o solicitar su apoyo, ya sea para elaborarla y/o revisarla.

85 Si los procedimientos de un área tienen interacción con otra área, deben desarrollar los procedimientos en conjunto con la otra área, GTR y GP consensualmente.

86 Si los procedimientos interactúan con más de un área, se debe solicitar a la GTR y GP que normen el mismo para su aplicación a nivel nacional, para lo cual se

requerirá de toda la retroalimentación con las partes involucradas vía conferencias con todos ellos.

GESTION DE CAMBIO

87 Todos los trabajos programados deben quedar registrados en el aplicativo de actividades y deben cumplir con las políticas y lineamientos definidos en el documento PRO GTR 01 Planificación Técnica.

88 En las reuniones de planificación deberá estar presente el Jefe de Seguridad Lógica nacional o su delegado para evaluar los impactos potenciales a nivel de seguridad de los trabajos aprobados. Su opinión deberá ser registrada por escrito (i.e. correo electrónico) ó sentada en actas.

89 Todo cambio en la red IP (núcleo y distribución) debe ser aprobado por un COMITE DE CAMBIOS compuesto estrictamente por GTN y SGTN; o sus respectivos delegados. El resultado de la aprobación se dará vía el sistema de actividades posterior a su análisis en la reunión de inicio de semana con los GAN o sus delegados. Esta aprobación se realizará siguiendo los parámetros y políticas previamente establecidas y publicadas para autorización de trabajos. En caso de que el GTN y el SGTN no estén de acuerdo en la interpretación de las políticas, GG dirimirá.

90 Todo cambio en la red Clear Channel (SDH, DWDM, etc) y fibra oscura debe ser aprobado por un COMITE DE CAMBIOS compuesto estrictamente por GTN y SGTN; o sus respectivos delegados en base a los informes del Dpto. de OTN. El resultado de la aprobación se dará vía el sistema de actividades posterior a su análisis en la reunión de inicio de semana con los GAN o sus delegados. Esta aprobación se realizará siguiendo los parámetros y políticas previamente establecidas y publicadas para autorización de trabajos. En caso de que el GTN y el SGTN no estén de acuerdo en la interpretación de las políticas, GG dirimirá.

91 Todo cambio en la red IP, en la capa de acceso (Sobre Clientes) debe ser aprobado por el Jefe de Soporte Técnico Corporativo en Guayaquil para la región 1 y el Jefe de Soporte Técnico Corporativo en Quito para la región 2.

92 Todo trabajo a realizarse a nivel lógico y físico en la red interna de datos o voz de los edificios administrativos, debe ser coordinado/supervisado por el Técnico de Soporte LAN y aprobado por el GTR respectivo en cada región. El departamento de Seguridad Lógica será quien revise los cambios planteados previos a ser autorizados.

93 Queda estrictamente prohibido a cualquier departamento instalar el mínimo elemento dentro de la red interna sin previa autorización de GTR respectiva, y sin el cumplimiento los estándares definidos por Seguridad Lógica.

94 Todo el resto de trabajos de operación y/o mantenimiento a realizar en la empresa debe tener la autorización por GTR respectivas. Sin esta autorización ningún trabajo podrá ser realizado.

95 Las autorizaciones de trabajo que no apliquen al sistema de actividades (según PRO GTR 01 Planificación Técnica) se las enviará por correo electrónico y como último recurso se aceptará una autorización verbal por parte del GTR para luego regularizarse vía correo electrónico.

96 Todo trabajo programado deberá ser clasificado como “Notificado” o como “No notificado”. Un trabajo Notificado debe ser informado a todos los clientes cuyo servicio pudiera ser afectado con el mismo. Un trabajo “No notificado” solo debe ser informado internamente en la empresa. Existirán excepciones donde un trabajo no notificado sea puntualmente notificado.

97 En caso de existir diferencias entre la fecha de ejecución de un trabajo o de su notificación, será GTN/SGTN responsable de dirimir sobre dicha actividad.

98 Los trabajos deben alinearse a la ISO27001 por lo tanto clasificar su origen como: acción correctiva, acción preventiva u oportunidad de mejora. Las acciones correctivas pueden ser de modalidad planificada, emergente o emergencia.

99 Todo cambio que involucre la red IP a nivel del núcleo (anillos de backbone y la infraestructura de interconexión entre ciudades) debe ser simulado y documentado en un SMOP.

100 Todo cambio que involucre la red IP a nivel de distribución debe ser documentado en un SMOP.

101 Los Jefes de IAC de cada región, Bancos y OTN serán quienes decidan (según el nivel de sofisticación) cuando un trabajo con clientes amerita la elaboración de un documento tipo SMOP o similar, para su ejecución. La revisión y aprobación estará a cargo sobre las jefaturas en mención.

102 Todo SMOP debe ser cumplir la especificación: FOR PROY 10 SMOP.

103 Antes de empezar todo trabajo por cualquier área, estas deben comunicarse OBLIGATORIAMENTE con el NOC, así mismo al terminar deben notificar al NOC para que este efectúe la revisión.

104 Todo trabajo efectuado debe quedar registrado en una bitácora manejada por el NOC y así mismo máximo al día siguiente deben emitir un reporte sobre los trabajos efectuados indicando los pormenores de los mismos.

105 Toda falla en la red fuera de lo previsto en los SMOPs debe ser comunicada por el NOC al GTN, SGTN y GANs.

106 Todo equipamiento nuevo en la red debe ser probado en laboratorio en cuanto a aspectos físicos (hardware) y lógicos (software) .El resultado de las pruebas debe ser enviado vía email y aprobado por el COMITE de CAMBIOS y/o GANs (cuando aplique)

107 Para equipamiento no estándar en la red IP, se debe contar con una validación del diseño por parte del vendedor del equipamiento y a su vez que los técnicos del área involucrada hayan hecho las respectivas pruebas de laboratorio. Ante cualquier situación de incertidumbre sobre dicho equipamiento se pedirá autorización a GTN y/o SGTN

SEPARACIÓN DE LOS RECURSOS PARA EL DESARROLLO, PRUEBA/ENSAYO Y OPERACIÓN

108 Para todos los proyectos, se debe proporcionar mínimo dos ambientes de trabajo que son: desarrollo y operación.

109 No se debe manipular y/o cambiar ninguna configuración, versión de sistema

operativo, arquitectura de red, etc., sin previas prueba en el ambiente de desarrollo

110 Las pruebas de laboratorio serán puestas en producción con el visto bueno de la Gerencia de Networking y previa autorización de GTN/SGTN.

111 Los equipos de ambiente de desarrollo deberán tener claves de acceso diferentes a los de ambiente de producción y es obligatorio utilizar claves con encriptación

TRATAMIENTO, MONITOREO y ENTREGA DE SERVICIO DE TERCERAS PARTES

112 Los contratos con terceras partes que impacten el servicio de la empresa deberán ser analizados y aprobados por un COMITE DE PROVEDURIA compuesto al menos por un representante de alto nivel del Área Comercial, del Área de Ingeniería, del Área Operativa y del Área Legal.

113 Se deberán realizar acuerdos con los proveedores que tengan alto impacto en el servicio, de tal manera de poder traspasar dichos acuerdos a nuestros clientes.

114 En ningún caso se podrá ofrecer a los clientes más de lo que se ha logrado pactar con el proveedor, a menos que se haya asegurado un mejor nivel de servicio gracias a la diversificación de proveedores.

115 (GTN/SGTN) deberá solicitar a sus proveedores los pormenores del servicio entregado, tales como procedimientos de control de cambios, diagramas técnicos del servicio o producto, mecanismos de continuidad del servicio, procedimiento de apertura de tickets, niveles de escalamiento y en general todo lo necesario para garantizar que el servicio del proveedor cumple con los requisitos definidos en el contrato.

116 Los proveedores de servicio de Internet deben presentar reportes mensuales de la calidad de su servicio, reconociendo los créditos respectivos por fallas en el mismo. Dichos reportes deben ser comparados con reportes internos y validados por el NOC. Mensualmente debe existir un informe de la revisión de dichos reportes por parte del NOC.

117 El reporte del NOC debe explicitar los puntos de discrepancia y acuerdo entre el reporte del proveedor y el reporte interno. En base a este reporte, GTN/SGTN o Gerencia Financiera negociará (en caso de requerirse) con el proveedor los niveles de crédito debidos y las mejoras que debe realizar el proveedor en su servicio.

118 El reporte del NOC debe ir con el visto bueno del Jefe del NOC y ser aprobado luego por el GTN/SGTN. Al final de este procedimiento, el reporte pasará a manos de Gerencia Financiera para el arreglo de pagos y la solicitud de crédito respectivas.

119 En caso de incidencias o fallas del proveedor de cualquier índole (i.e. físicas, lógicas, seguridad, etc.), el NOC abrirá un ticket interno y no lo cerrará hasta tener la versión oficial escrita del proveedor respecto a las acciones correctivas tomadas.

120 Independientemente de los parámetros de calidad de servicios medidos por el proveedor, la empresa llevara una estadística de las siguientes variables aplicables a proveedores de Internet:
e.1 Jitter, delay y pkt loss de los canales

e.2 Mean Time to Repair (MTTR) ante cualquier outage de la red
e.3 Número de trabajos de mantenimiento y/o emergencia del proveedor.

121 La empresa tendrá como política utilizar todos los mecanismos de seguridad que el proveedor de Internet ofrezca (i.e. Remote Triggered Blackhole, ACLs, Firewall, etc.), pero en ningún caso se permitirá degradación del servicio debido a estos controles o que existan controles aplicados y no notificados.

122 En casos de incidentes de seguridad, GTN/SGTN o su delegado solicitará la activación de los mecanismos de seguridad respectivos al proveedor. Así mismo, se deberá requerir la respectiva desactivación (en donde aplique).

123 La empresa debe exigir a sus proveedores una política de control de cambios debidamente documentada. Esta información debe ser solicitada por GTN/SGTN y almacenada por el NOC.

124 El NOC deberá monitorear proactivamente si el proveedor ha realizado algún cambio notificado o sin notificación (i.e. cambio de traceroutes, cambio de caminos, variación en parámetros de calidad de servicio, alteración de disponibilidad de ancho de banda, etc.) e incluir los resultados de dicho monitoreo en el reporte mensual del NOC para comparación con el reporte mensual del proveedor.

125 La empresa hará su mejor esfuerzo por contar con capacidad adicional a sus canales de Internet internacionales, tomando en cuenta que factores económicos inciden en la decisión.

126 Todos los clientes deberían contar con respaldo automático en caso de falla de un proveedor de Internet. La degradación del servicio que pudiese ocurrir en este caso deberá ser controlado mediante mecanismos de control de ancho de banda centralizados. En casos extremos se deberá prescindir de los protocolos de menor uso por parte de nuestros clientes (i.e. peer to peer).

127 Existirá un Capacity Manager en la red, nombrado en COMITE DE CAMBIOS, quien se encargará de informar proactivamente de las acciones factibles de realizar para evitar futuras congestiones de tráfico en los proveedores internacionales.

GESTION DE LA CAPACIDAD

128 La responsabilidad de la Gestión de la Capacidad estará a cargo de las GTRs quienes delegarán la función de Capacity Manager, en sus diferentes áreas, a las Jefaturas operativas respectivas.

129 El Capacity Manager debe utilizar todas las herramientas necesarias junto con la información acerca del ancho de banda vendido, capacidad de proveedores de Internet, capacidad de procesamiento de los equipos, capacidad de almacenamiento, densidad de puertos, entre otros y así poder determinar la capacidad usada de los canales y equipamiento, para proyectar su crecimiento y alertar tempranamente una falta de capacidad.

130 Los Capacity Manager darán un informe de novedades de la capacidad en las reuniones técnicas de inicio de semana. Mediante este informe, GTRs tomará las acciones preventivas posibles y necesarias para evitar la falta de capacidad y comunicará de dichas acciones a la Gerencia Comercial Nacional.

POLÍTICA DE ACEPTACIÓN DEL SISTEMA

131 Toda aceptación de un nuevo sistema ya sea que provenga del interior de la empresa o de un proveedor externo, deberá pasar por una etapa de pruebas antes de ser colocado en producción. GTN/SGTN revisará y autorizará la puesta en producción de sistemas de información, configuraciones, equipos de networking y demás elementos relacionados con la infraestructura lógica y diseño de red, así como también la puesta en producción de infraestructura física en los nodos.

132 En un sistema aceptado, pueden presentarse oportunidades de mejoras, sugeridas por los GANs que serán ejecutadas por los departamentos responsables, bajo autorización de GTN/SGTN cuando la trascendencia del sistema lo amerite.

133 Todo nuevo nodo deber pasar por el checklist de verificación FOR GTR 18 Checklist Nodos

134 Toda nueva implementación de infraestructura debe pasar por el checklist FOR GTR 22 Control de cumplimiento de Infraestructura.

135 Todo nuevo sistema de información debe pasar por el checklist FOR GTN 0X Control de Cumplimiento de Sistemas Informáticos.

136 Cualquier otro nuevo sistema debe ser normado según los requerimientos de seguridad de la información (Disponibilidad, Confidencialidad e integridad), los cuales debe ser establecidos previos al inicio del proyecto según sea el caso. Bajo la aprobación final de GTN/SGTN y el GANS de la empresa deberá emitir su criterio respecto a aspectos de seguridad a considerarse.

137 El tratamiento de las excepciones de alguno los puntos exigidos en los checklist serán manejadas por GTN/SGTN y de ser necesario escaladas a GG.

138 Para proveedores internacionales de transmisión de datos deberá realizarse pruebas de transparencia de canales, saturación de canales y otros servicios provistos según lo indicado en la parte contractual. Las pruebas deberán realizarse según los lineamientos del área del servicio que se está recibiendo (i.e. Enlaces Internet por Networking, Tecnologías de Transporte Óptico por OTN,etc)

139 Un nuevo sistema aprobado debe tener al menos un simulacro anual de falla en sinergia con los escenarios de amenazas del BCP planteado. El departamento responsable del sistema debe diseñar el instructivo respectivo el mismo que será ejecutado según los lineamientos establecidos en la estrategia de recuperación del BCP.

DOCUMENTACION DE SISTEMAS

140 Los manuales de usuario son de acceso público para personal de la empresa

141 Los manuales técnicos son de acceso restringido para el área de técnica

142 Los documentos internos deberán ser accedidos vía web con usuario autorizado

SISTEMA DE INFORMACIÓN

143 Todo sistema de información interno debe ser accedido con usuarios individuales y diferentes para cada persona.

144 Sólo se considerará información no confidencial todo lo que el Comité de

Seguridad explícitamente indique. Todo el resto será considerado como información confidencial.

145 El manejo de la información dentro del sistema dependerá de los perfiles asociados a los usuarios.

146 La información sensible como tarjetas de crédito, claves, etc. deberá ser cifrada en todos los medios de transmisión, almacenamiento.

147 La información del sistema no podrá ser eliminada/modificada sin previa autorización gerencial de su jurisdicción por escrito/email.

148 La interconexión del sistema interno con la red pública de datos se realizará de manera segura a través de un canal seguro que cifre la información

149 Se debe contar con un sistema de registro de logs a nivel nacional. Este sistema debe tener un tiempo de validez mínimo de 360 días.

150 Toda ejecución realizada por cualquier usuario a través de cualquier aplicación sobre los equipos de red debe quedar registrada en el sistema de logs.

151 Todo evento deberá quedar registrado en el sistema de logs.

152 Personal autorizado por las GTR podrá acceder a los logs para fines de investigación o seguimiento de control de acceso bajo solicitudes de GAN/GTR/GTN/SGTN/GG.

153 De acuerdo a la política de confidencialidad de la empresa, la información obtenida de los registros de logs es de propiedad de la empresa. Sólo GG/GTN/SGTN o la GANS(Gerente de Area Nacional Seguridad) bajo políticas previamente establecidas podrán autorizar la liberación de esta información al público o a clientes.

154 Personal autorizado (NOC, personal técnico autorizado por GANS) podrá acceder a los logs para fines de investigación, seguimiento de eventos, monitoreo y seguimiento de control de acceso.

155 La base de datos de logs será de uso interno por personal de la empresa, su acceso será única y exclusivamente en los casos aquí dispuestos.

156 Se utilizará un sistema gestor de claves para acceso de lectura a los equipos, actualmente el TACACS.

157 Para trabajos programados NOC facilitará la clave de emergencia al responsable de la actividad en caso de ser necesario, en caso de incidentes la persona asignada por GANN/GTN/SGTN, podrá solicitar la clave de emergencia a NOC, la misma que tiene privilegios de administrador.

158 Para precaución, el sistema gestor de cambio de claves, generará el cambio de claves nacional automáticamente después de 4 horas de haber entregado la clave de administrador al NOC.

159 Se deberá cambiar las claves de acceso a todos los dispositivos cada vez que personal técnico deje de laborar para la empresa, removiendo las claves de las personas individuales. El Jefe de RRHH notificará la salida de la persona. GANS

se encargará de asegurar la ejecución de remoción de claves a través de las personas correspondientes.

160 Se deberá dar de baja a las cuentas de los usuarios que dejan de laborar para la empresa en todos los dispositivos y/o aplicaciones. El Jefe de RRHH notificará la salida de la persona. GANS se encargará de asegurar la ejecución de remoción de claves a través de las personas correspondientes.

161 Toda ejecución realizada por el administrador y todos los operadores de los sistemas a través de cualquier aplicación sobre los equipos de red debe quedar registrada en el sistema de logs.

162 Todo análisis de un incidente deberá estar basado en la información que proporcionan los logs amén de cualquier otra información pertinente. Con el resultado del análisis se deberán tomar las acciones correctivas y preventivas apropiadas.

163 Se debe contar con un servidor de sincronización de tiempo a nivel nacional, todo dispositivo de la red debe sincronizarse con este servidor de tiempo.

CONTROL DE ACCESOS

164 El acceso a la información de la empresa deberá ser controlado mediante perfiles de usuarios, los niveles de acceso y determinación de perfiles serán realizados por un Comité conformado por GANS, GTN, SGTN, GTRs y GG.

165 Todos los usuarios deberán tener un único nombre de usuario y una sola clave cifrada para poder acceder a la información a la que estén autorizados.

166 Los accesos deberán estar seccionados según el tipo de información permitida.

167 Deberá mantenerse un registro de acceso y de las actividades realizadas.

168 Para obtener el acceso a los sistemas internos, se deberá solicitar un usuario y clave al Departamento de Sistemas por medio del jefe de área indicando los sistemas internos a los que se les debe permitir el acceso de acuerdo a los roles y en conocimiento de GANS

169 Para revocar usuarios y claves de acceso a personal saliente, el jefe de RRHH deberá solicitar dar de baja al usuario del mismo.

170 Todos los sistemas de información interna deben manejar perfiles y privilegios que permitan el acceso discrecional a diferentes conjuntos de aplicaciones internas en base al usuario.

171 Los perfiles deberán estar acorde al papel que desempeña cada usuario con los sistemas de información. Los privilegios deberán estar de acuerdo con los perfiles asignados.

172 Los cambios obligatorios de contraseña serán realizados únicamente por el usuario a través de una aplicación específica en la Intranet.

173 Un aumento o disminución en los privilegios de acceso de un usuario, deberán ser solicitados por el jefe del área correspondiente al Departamento de Sistemas, con la respectiva justificación bajo conocimiento de GANS

USO DE CONTRASEÑAS

174 Los usuarios deberán utilizar claves de acceso con un mínimo de 8 caracteres que incluyan tres de los siguientes grupos: letras mayúsculas, letras minúsculas, números y símbolos.

PROCEDIMIENTOS DE CONEXIÓN SEGURA

175 Los accesos a todos los sistemas operativos deberán hacerse a través de SSH.

176 Para los casos imprescindiblemente necesarios de acceso a sistemas operativos a través del 23 (telnet) deberá manejarse listas de acceso o firewall para mantenerlos seguros.

177 El usuario y clave proporcionados son de uso personal, por lo tanto el dueño del mismo será responsable de cualquier actividad realizada en los sistemas.

178 Todos los sistemas operativos deben considerar la expiración de sesiones inactivas luego de un tiempo determinado en 10 minutos.

179 Todos los dispositivos de red deben considerar la expiración de sesiones inactivas (10 min) para backbone.

180 Las sesiones inactivas apagadas por el Sistema deberán quedar registradas en un sistema de logs.

181 Los sistemas fuera de banda (OOB) que manejen información confidencial y/o sensible deberán tener un entorno informático dedicado, Y sólo deben estar conectadas a la red pública de datos a través de medios seguros, SSH y listas de control de acceso definidas.

COMPUTACIÓN MÓVIL Y COMUNICACIONES

182 La red móvil de la empresa en caso de ser implementada debe estar segmentada y protegida de cualquier acceso no autorizado desde o hacia dicha red.

TRABAJO A DISTANCIA

183 Los empleados podrán tele-conectarse a la red Interna previa autorización del departamento de Seguridad y siguiendo las especificaciones definidas por ellos y sólo para realizar labores relativas a la empresa.

ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD

184 En la planificación, desarrollo o adquisición de cualquier sistema de información de la empresa debe incluirse los requisitos mínimos de Seguridad, para lo cual es necesario seguir las políticas establecidas por el GANS.

PROCESAMIENTO CORRECTO DE LAS APLICACIONES

185 Se deberán realizar módulos de validación de datos de entrada para todas las aplicaciones internas.

186 Se debe contar con una base de conocimiento para consultar errores pasados conocidos como lecciones aprendidas.

187 Para solicitudes del desarrollo de nuevas aplicaciones se completará el formato FOR-PROY04 Solicitud de Software, estas solicitudes deben ser realizadas por las GTR y deben tener el visto bueno de GTN/SGTN. Estas solicitudes serán analizadas por el Departamento de Software y contestadas en un plazo de 40

horas hábiles. Se deberá presentar un mensaje informativo respecto a los resultados obtenidos por las solicitudes de los usuarios.

188 Para proteger los datos que alimentan los sistemas internos se deben crear canales seguros entre el usuario y los dispositivos de red, aplicaciones y bases de datos. (VPNs, SSL)

189 Las aplicaciones antes de entrar a producción debe pasar el CHECK LIST PARA ACEPTACIÓN DE UN NUEVO SISTEMA anteriormente mencionado.

CÓDIGO FUENTE

190 Todo código fuente desarrollado para los sistemas de información es de propiedad exclusiva de la empresa.

191 El acceso a los servidores de aplicaciones debe permitir acceso únicamente a personal del Departamento de Sistemas desde direcciones IP seguras.

192 Todos los empleados del departamento de desarrollo deben almacenar el código fuente en un directorio que se encuentre controlado su acceso y encriptado su contenido a través del programa de encriptación ej: TrueCrypt.

193 El Jefe del Departamento de Sistemas será el encargado de estandarizar la generación de código además de prever y concientizar ante posibles huecos de seguridad en el desarrollo de aplicaciones sean éstas como: Mal traspaso de variables entre formularios, Sql injection, Buffer overflow, buffer underflow, cross site scripting, etc.

194 Cualquier nuevo módulo o sistemas antes de entrar a producción debe pasar por un scanning de vulnerabilidades lógicas realizado por GANS.

TRATAMIENTO DE INCIDENCIAS

195 Todos los empleados están en la obligación de reportar cuando se encuentre una debilidad o incidente de la seguridad de la información. Dependiendo de la gravedad, el reporte puede realizarse vía email, llamada telefónica o presencial. Para este reporte seguiremos las guías establecidas en el documento ESP SEC 15 Lista escalabilidad de incidencias.

196 El tratamiento de los incidentes debe ser registrado con su respectiva acción correctiva. Si el incidente es de tipo lógico, para ello se usará el sistema de control de incidencias de seguridad. Para cualquier otro tipo de incidentes el tratante guardará el registro del tratamiento de incidentes en la carpeta departamental. Los incidentes registrados podrán estar en dos estados Abiertos o cerrados.

197 El tratamiento de incidentes siempre deben estar orientados a la solución de la causa raíz de problema. Salvo excepciones donde ya no dependa de la organización dicha causa.

COMPRAS EQUIPOS/SISTEMAS

198 Se clasificarán 2 tipos de proveedurías que son, para solución tecnológica y de proveeduría recurrente, los mismos que serán seleccionados acorde a los siguientes lineamientos:

199 Selección de Proveedor para Solución Tecnológica: Los proyectos medianos o grandes, llámese proyectos a aquellos que tienen principio y fin, deberán pasar por el proceso de selección de la tecnología a utilizar considerando además el costo

beneficio para la empresa. Este proceso de selección en el área técnica se lo realizará una sola vez por GTN/SGTN o sus delegados.

200 Proveeduría Recurrente: En relación a la proveeduría local o recurrente es deseable tener una marca estándar que nos beneficia entre otras cosas en expertise, asistencia técnica, precios, garantías, etc. Sin embargo es importante indicar que si se presentaren opciones similares con un precio más conveniente en equipos de proveeduría recurrente como CPEs, transceivers, laptops, etc.; se deberá realizar un informe técnico por parte del área responsable, así como también el análisis comparativo de sus características vs. el producto actual, además de su recomendación para la autorización respectiva en el área técnica de GTN/SGTN.

201 En su mayoría las soluciones tecnológicas tienen una sola representación oficial en el país, sin embargo en el caso de que la misma tenga más de un proveedor, se realizará la evaluación de proveedores la primera vez, autorizado en el área técnica por GTN/SGTN o sus delegados. Solamente, se realizará una nueva evaluación de los proveedores para la respectiva selección de los mismos si:

202 Existen novedades en los resultados de las encuestas anuales realizadas por las diferentes áreas, lo cual es requerido en ISO Calidad.

203 Por cambios drásticos de las políticas del proveedor que afecten a la empresa.

204 Por solicitud de las Gerencias GG/GTN/SGTN.

PLAN DE CONTINUIDAD DEL NEGOCIO

205 La implantación, prueba y mejoramiento de un Plan de Continuidad del Negoció será responsabilidad del Gerente Técnico Nacional, Subgerente Técnico Nacional, Gerente Técnico Regional, Gerente Administrativo de cada localidad y de la Gerencia General. Las pruebas del mismo se deben realizar en ambientes controlados mínimo una vez por año. El éxito o fracaso de este plan será contemplado en la evaluación anual de dicho Gerente, por parte de Recursos Humanos en conjunto con los superiores involucrados en dichas pruebas.

206 La reevaluación de los planes de continuidad del negocio se lo realizará cada año o en su defecto cuando un cambio considerable de la infraestructura lo exija.

207 Se deberán realizar simulacros de falla de la red o sistemas periódicamente con la finalidad de entrenar al personal de soporte para mejorar sus tiempos de respuesta, así como también para detectar cualquier falla no contemplada en trabajos previos y/o cualquier error en los procedimientos.

208 Se deberán realizar simulacros después de cada cambio significativo realizado sobre la red o sistemas internos.

CUMPLIMIENTO

209 El Departamento de Seguridad Lógica será el encargado de comprobar el cumplimiento técnico de los sistemas acorde a las normas de seguridad de información.

210 El Departamento de RRHH será quien aplique las sanciones de incumplimiento.

ANEXO 11

POLÍTICAS DE SEGURIDAD LÓGICA PARA EL MANEJO DE INCIDENTES EN LOS CLIENTES

POL SEC 02 VER 18 09 10

La empresa en su afán de transparentar las relaciones contractuales del servicio prestado a sus clientes, declara mediante este documento las políticas, que deberán ser tomadas por ambas partes como adherentes al contrato principal celebrado por prestación de servicios y que se describen en las cláusulas a continuación:

1) La empresa no se responsabiliza por cualquier clase de incidentes telemáticos (voluntarios o involuntarios), que produzcan los clientes hacia terceros y que afecten la seguridad lógica de aquellos, y se reserva el derecho de tomar las acciones correctivas necesarias en caso de que dichos incidentes afecten a la red de la empresa.

2) La empresa no se responsabiliza por los incidentes de seguridad lógica, que sufran los clientes en sus servidores y/o Equipos (propiedad del cliente), bajo administración del cliente con IP's públicas asignadas por la empresa, producto de la falta de configuraciones seguras por parte del mismo cliente. Cabe enfatizar, que la empresa siempre está dispuesta a colaborar con el cliente, bloqueando conexiones desde y/o hacia las IP's que el cliente solicite.

3) La empresa no se responsabiliza por los incidentes de seguridad lógica, que sufran los clientes en los servidores y/o Equipos (propiedad de la empresa), bajo administración del cliente, con IP's públicas asignadas por la empresa, producto de la falta de configuraciones seguras por parte del mismo cliente. Cabe enfatizar, que la empresa siempre estará predispuesto a colaborar con el cliente bloqueando conexiones desde y/o hacia las IP's que

el cliente solicite.

4) La empresa si se responsabiliza por los incidentes de seguridad lógica, que sufran los clientes en los servidores y/o Equipos (propiedad de la empresa o del cliente), bajo administración y configuración única de la empresa y con IP's públicas asignadas por la misma, producto de la falta de configuraciones seguras; hasta un monto máximo de $1000 dórales americanos.

5) La empresa aplicará constantemente Políticas de seguridad preventivas en su red y así proteger de los diferentes incidentes de seguridad que pudieren afectar a sus clientes y su red propia. El cliente debe prestar toda la colaboración necesaria para este fin.

6) La empresa se reserva el derecho a tomar medidas proactivas y/o reactivas cuando un incidente de seguridad lógica, sea provocado desde el internet, o desde un cliente y ponga en riesgo los principios de seguridad de información (disponibilidad, confidencialidad e integridad) de la red, o de sus clientes.

Se tomará las siguientes medidas reactivas de seguridad, según sea el caso:

6.1) Respecto al SPAM: Todo cliente que genere SPAM será comunicado para que tome las medidas necesarias dentro de su red y se le otorgará un plazo de 2 días laborables para que ejecute las debidas correcciones, pasado este plazo se limitará la salida al puerto TCP 25 en el CPE asignado al cliente o switch de la empresa al cual se conecta.

Únicamente se retirará este bloqueo, una vez que el cliente haya tomado las medidas correctivas, en caso que el cliente sea reincidente en el envío de SPAM se volverá a bloquear la salida hacia el puerto TCP 25 y se lo desbloqueará una vez que el mismo nos envíe las pruebas técnicas pertinentes a las medidas correctivas definitivas que tomen. La empresa no se responsabiliza por el ingreso de las IP's públicas de los clientes en las listas negras de envío de SPAM.

6.2) Respecto a la Propagación de Virus: Todo cliente que se encuentre infectado con algún tipo de malware, sea este un virus, y/o gusano y que esté intentando infectar a otros clientes y/o Equipos de la red de la empresa será notificado y otorgado un plazo de (15 minutos) para desconectar los focos infecciosos dentro de su red. Una vez concluido este plazo se procederá a limitar el puerto de conexión (TCP y/o UDP) por el cual el virus se propaga, y en el caso de ser un puerto de conexión aleatorio, se limitará en el CPE del cliente, la conexión hacia la red de la empresa, de aquellos equipos de la red interna infectados. En el peor de los casos, cuando concluye el plazo otorgado y el CPE es de administración única del cliente se limitará aquella(s) IP(s) públicas del cliente que propaguen el Virus y/o Gusanos. En caso que la situación sea demasiado crítica y ponga

en riesgo la disponibilidad de la red La empresa, se procederá a limitar totalmente dicha conexión e informar posteriormente al cliente de la situación.

6.3) Ataques a la Red: Todo cliente que intente realizar un ataque DOS, DDOS, Exploit scanning, Flooding Atacks y accesos físicos o lógicos no autorizados hacia equipos de la red de la empresa, CPE's de Administración de la empresa u otros clientes o al internet; será bloqueado inmediatamente y notificado.

6.4) Phishing: Todo cliente que aloje páginas falsas con sus IP's públicas asignadas, ya sea voluntaria o involuntariamente, será bloqueado inmediatamente el puerto de servicio (comúnmente http, https) que aloja el sitio web falso y notificado al cliente. En caso que el mismo servidor comprometido este incurriendo en uno de los puntos 6.1-6.3, la IP pública asignada será bloqueada inmediatamente y notificado, puesto que es un equipo totalmente comprometido y foco infeccioso de la red.

En el caso que un cliente sea quien está sufriendo un ataque de phishing, puede solicitar a la empresa el bloqueo de acceso al sitio falso o IP correspondiente, que hospeda el phishing y así disminuir el impacto de dicho ataque dentro de las demás redes asignadas a los clientes de la empresa.

7) Todo cliente que posea enlaces de internet con la empresa y los use para transmisión de datos, mediante IP's públicas sin encapsular en túneles y/o VPNs, será notificado del riesgo que corre. En caso que esta configuración provoque continuos ataques hacia este cliente, se le otorgara un plazo de 45 días calendario para que adopte una configuración basada en encapsulamiento (túneles y/o VPNs) y así sus servicios privados no estén expuestos al internet. Pasado estos 45 días, La empresa no se responsabiliza por el bloqueo de puertos, por parte de nuestro IPS/IDS, debido a los continuos ataques hacia el cliente y que por ende pasan por la red de la empresa.

Cabe recalcar que los ingenieros integrantes del Departamento de Soporte Técnico Corporativo están prestos a colaborar en las sugerencias telefónicas que el cliente necesite para adoptar un esquema de Túneles o VPNs.

8) Todo cliente o personas externas y/o terceras, que haya sufrido algún incidente de seguridad lógica por parte de alguna IP del bloque asignado por la empresa, únicamente podrá solicitar información mediante el proceso legal correspondiente, esto es solicitada por Autoridad competente que haya conocido del mismo.

ANEXO 12

POLÍTICA DE MANEJO DE INFORMACIÓN

POL SEC 03 Ver 18 09 10

Objetivo:

Establecer una política formal para el manejo de información.

1.- Toda información generada en la empresa deberá ser clasificada como PUBLICA o CONFIDENCIAL.

2.- Cada departamento será responsable de clasificar la información que genere como pública ó confidencial.

3.- La información correspondiente a publicidad, contenido del portal Web de la empresa y números telefónicos de soporte será clasificada como PUBLICA.

4.- Será considerada como CONFIDENCIAL, toda información generada en la empresa, sea esta verbal, escrita o digital salvo que se indique lo contrario por parte del Comité de Seguridad del Información.

5.- Cada departamento deberá identificar la información y los departamentos con los que puede intercambiarla.

6.- Cada departamento deberá cumplir un tratamiento adecuado de eliminación de la información.

7.- Toda información de carácter confidencial que se encuentre almacenada digitalmente en las computadoras de la empresa, sean desktops o laptops debe ser encriptada. Para esto se deberá utilizar el instructivo INS SEC Almacenamiento de Información Encriptada.

8.- Toda información confidencial deberá ser respaldada digitalmente con encriptamiento en un servidor dedicado para este propósito, el mismo que no deberá ser publicado al Internet y cuyo acceso será restringido para el personal interno de la empresa.

9.- Toda información confidencial que se transfiera por correo electrónico, deberá ser encriptada por una firma digital.

10.- Toda información impresa antes de ser desechada, debe ser destruida de tal manera que no pueda ser recompuesta posteriormente.

12.- Todo el personal deberá aplicar las buenas prácticas de divulgación de información referenciada en el documento INS SEC Contramedidas para la ingeniería social.

13.- El riesgo de la pérdida o fuga de información en las computadoras desktop o laptop del personal debe ser disminuido con el cumplimiento las buenas prácticas de seguridad mencionadas en el documento INS SEC Buenas prácticas para el uso de PC.

ANEXO 13

POLÍTICA DE TRABAJO A DISTANCIA

POL SEC 04 Ver 18 09 10

Objetivo:

Establecer una política formal para el trabajo a distancia

1.- Ciertos integrantes de las áreas técnicas y/o administrativas podrá contar con enlaces dedicados hacia su domicilio previa autorización de su jefatura y justificación de la necesidad.

2.- El ancho de banda asignado para estos enlaces será 1024 kbps, en caso de requerirse más ancho de banda se deberá contar con la aprobación del Jefe directo.

3.- Todos las conexiones hacia los domicilios deberán estar registradas debidamente en el sistema de información de la empresa con valor de ancho de banda asignado de 1024 kbps.

4.- Todas estas conexiones deberán establecer con un CPE de administración de la empresa, el cual deberá estar configurado con filtros de seguridad definidos por el departamento de soporte técnico corporativo.

5.- Serán los empleados los responsables por el uso de su enlace y del CPE instalado, y deberán seguir las buenas prácticas del uso del PC establecidas por el departamento de Seguridad de Información.

6.- La instalación de dispositivos de interconexión inalámbrica luego del CPE en estos enlaces, deberá ser registrada y autorizada por el departamento de seguridad lógica.

7.- El empleado brindará facilidades para la instalación del enlace y ubicación del CPE dentro de su domicilio.

8.- El acceso a la red corporativa a través de estos enlaces solo será posible posterior a la autorización y registro de este enlace por el departamento de seguridad lógica.

9.- Las conexiones a la red interna desde estos enlaces sólo serán posibles a través de una VPN remote access.

10.- El uso del correo electrónico desde redes externas a la empresa solo podrá realizarse a través del acceso Web al mismo.

12.-El acceso de nivel administrativo a equipos en la red corporativa desde redes externas solo podrá realizarse previa autorización y registro del departamento de seguridad lógica y con las herramientas de encriptación dispuestas para esta actividad.

ANEXO 14

POLÍTICAS DE USO DE MEDIOS CRIPTOGRÁFICOS

POL SEC 05 Ver 08 09 10

Objetivo:

Establecer una política formal para el uso de medios criptográficos.

1.- Para el cumplimiento de los objetivos de la seguridad de la información, el intercambio de información digital definida como confidencial para la empresa deberá utilizar medios criptográficos.

2.- La supervisión del cumplimiento de la política de uso de medios criptográficos es responsabilidad de los jefes departamentales.

3.- El departamento de Seguridad Lógica determinará la confiabilidad de los medios previo a su implantación.

4.- En caso de excepciones al uso de medios criptográficos, la información se protegerá con las buenas prácticas de manejo de información establecidas en el documento IN SEC 04 Buenas prácticas del uso del PC, emitidas por el departamento de Seguridad Lógica.

5.- La supervisión del desempeño de los medios criptográficos será responsabilidad del departamento de Seguridad Lógica.

6.- Todo el personal deberá regirse cumplir con los procedimientos del uso de medio criptográficas definidas por el departamento de Seguridad Lógica de la empresa.

7.- Se acoge como estándar el uso AES para el cifrado y SHA-1 para el Hash.

8.- En el caso de las VPNs site to site y remote acces, el estándar será IPSEC con los algoritmos AES o 3DES de cifrado y SHA-1 de hash.

9.- Los firmas electrónicas serán generadas mínimo con una llave (key) de 1024 bits.

10.- Los certificados digitales web serán cifrados con el algoritmo AES.

11.- Solo se usarán firmas digitales personales y certificados web emitidos por una entidad de Registro reconocida nacionalmente.

ANEXO 15

POLÍTICAS DE USO DE EQUIPAMIENTO DE LABORATORIO

POL SEC 06 Ver 18 09 10
Objetivo: Establecer una política formal para el uso de equipos de laboratorio. 1.- Todo equipo de laboratorio debe tener una identificación lógica y física. 2.- Los equipos de laboratorio deben estar conectados de manera aislada, lo que significa que no deben ser vistos por redes ajenas a la red de la empresa 3.- Para conexiones a la red pública de la empresa, deberá existir la autorización previa del CTO, GTR, Gerente de Seguridad o sus delegados. 4.- Los servidores con software de simulación/emulación, deben ser configurados con accesos restringidos al personal autorizado para usarlo y deben tener deshabilitados todos los servicios excepto los específicos de su tarea. Estos servidores deben utilizar direccionamiento IP privadas.

5.- Todo equipamiento dedicado para el desarrollo laboratorios debe ser inventariado por su respectivo departamento. 6.- Los equipos de laboratorio como routers o switches deberán tener la configuración de fábrica luego de su respectivo uso

BIBLIOGRAFÍA

[1] ISO/IEC 27001:2005, Information Technology - Security Techniques - Information Security Management Systems – Requirements, 15 de Octubre 2005, Página 2.

[2] ISO/IEC 27001:2005, Information Technology - Security Techniques - Information Security Management Systems – Requirements, 15 de Octubre 2005, Página VI.

[3] ISO/IEC 27005:2008, Information Technology - Security Techniques - Risk Management, 19 de Septiembre 2009, Página 5.

[4] Peltier, T., Information Security Risk Analysis, 2001.

[5] Alexander, A., Diseño de un Sistema de Gestión de Seguridad de Información Óptica ISO 27001:2005, 2007, Página 57.

[6] Alexander, A., Diseño de un Sistema de Gestión de Seguridad de Información Óptica ISO 27001:2005, 2007, Página 56.

[7] Portal Definición, Internet, http://definicion.de/auditoría/, fecha de publicación 27 de Diciembre 2014.

[8] ISO/IEC 19011, Guidelines for quality and/or environmental management systems auditing, 10 de Julio 2002, Página 5.

[9] ISO/IEC 19011, Guidelines for quality and/or environmental management systems auditing, 10 de Julio 2002, Página18.

[10] ISO/IEC 27003, Information Technology — Security Techniques — Information Security Management – System Implementation Guidance, 1 de Febrero 2010, Página 55.

[11] ISO/IEC 27003, Information Technology — Security Techniques — Information Security Management – System Implementation Guidance, 1 de Febrero 2010, Página 55.

[12] Telconet S.A, SGSI — Políticas Específicas, 2010.