ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

IMPLEMENTACION DEL PRIMER SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION, EN EL ECUADOR, CERTIFICADO BAJO LA NORMA ISO 27001:2005

INFORME DE TRABAJO PROFESIONAL

Previa a la obtención del Título de:

INGENIERO EN COMPUTACIÓN ESPECIALIZACION SISTEMAS TECNOLÓGICOS

Presentado por:

José Alfonso Aranda Segovia

Guayaquil-Ecuador

AÑO

2009

DEDICATORIA

DESEO DEDICAR ESTE TRABAJO A MI ESPOSA JENNY Y A MIS HIJOS KENNY Y GAETHANA, QUIENES SON LOS QUE ME DAN LA FUERZA DE VOLUNTAD E INSPIRACIÓN EN LA VIDA. TAMBIEN A MIS PADRES Y HERMANOS POR SU INCONDICIONAL APOYO

AGRADECIMIENTO

MI MÁS SINCERO AGRADECIMIENTO A DIOS POR GUIARME EN LA TOMA DE DECISIONES, A MIS PADRES POR APOYARME SIEMPRE EN MIS ESTUDIOS Y A MI AMADA FAMILIA POR SACRIFICAR NUESTRO TIEMPO DE ESPARCIMIENTO.

TRIBUNAL DE GRADO

_____	_____
Ing. Jorge Aragundi	Ing. Freddy Pincay
SUB-DECANO DE LA FIEC	**DIRECTOR DE TRABAJO PROFESIONAL**
_____	_____
Ing. Galo Valverde	Ing. Cristina Abad
VOCAL	**VOCAL**

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo Profesional, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de graduación de la ESPOL)

_____

José Alfonso Aranda Segovia

RESUMEN

Dada la evolución de la Tecnologías de la información y su relación directa con los objetivos del negocio de la organizaciones, el universo de amenazas y vulnerabilidades aumenta por lo tanto es necesario proteger uno de los activos más importantes de la organización, la información, garantizando siempre la disponibilidad, la confidencialidad e integridad de la misma. La forma más adecuada para proteger los activos de información es mediante una correcta gestión del riesgo, logrando así identificar y focalizar esfuerzos hacia aquellos elementos que se encuentren más expuestos.

La implementación de un Sistema de Gestión de Seguridad de la información garantiza que la organización adopte las buenas prácticas sugeridas por la ISO 27001:2005 para un correcto tratamiento del riesgo. En el presente informe de trabajo profesional, se expone un caso de éxito de una implementación de un SGSI y su respectiva certificación bajo la norma ISO 27001:2005

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

SGSI	Sistema de Gestión de Seguridad de la Información
ISO	Organización de Estándares Internacionales
BCP	Plan de Continuidad del Negocio
PDCA	Plan-Hacer-Revisar-Actuar
BIA	Análisis del Impacto del Negocio
RPO	Punto objetivo de recuperación
WRT	Tiempo para recuperar el trabajo
RTO	Tiempo objetivo de recuperación
MTD	Tiempo máximo tolerable para estar fuera o caído
NOC	Centro de Operación de la Red
SOC	Centro de Operación de seguridad de la red
BSI	Empresa Certificadora, British Standard Institute
BQVI	Empresa Certificadora, Bureau Veritas
SGS	Empresa Certificadora
ANAB	Organismo Americano Acreditador
UKAS	Organismo Acreditar del Reino Unido

JITTER	Variación de tiempo de respuesta en una conexión
DELAY	Tiempo de respuesta de una conexión
PHISHING	Técnica utilizada para falsificar sitios Web y lograr el robo de datos de usuarios reales de dicho sitio
BUGS	Fallas técnicas que se detectan cuando el elemento tecnológico, como hardware o software, ya se encuentra en producción
IDS/IPS	Sistema de seguridad perimetral que cumple funcione de detección de intrusos y también de prevención de intrusiones.

INTRODUCCION.

Justificación.

En la actualidad uno de los principales activos que las organizaciones poseen, es la información. Por lo cual es necesario que toda organización que busque una excelencia en los servicios o productos que ofrece, adopte una Sistema de Gestión para el manejo adecuado de la información, garantizando así su disponibilidad, confidencialidad e integridad. Toda organización que desee convertirse en un proveedor confiable debería garantizar la continuidad de su negocio ante posibles escenarios de amenazas que pudieran presentarse.

Para cubrir estas necesidades la ISO -Organización Internacional para la Estandarización- creó una norma certificable que permite a las organizaciones encaminarse en un Sistema de Gestión de Seguridad de la Información, la ISO 27001:2005.

¿Qué es un Sistema de Gestión de Mejora Continua?

Según el British Standard Institute es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización. Las empresas que operan en el siglo XXI se enfrentan a muchos retos, significativos, entre ellos: Rentabilidad, competitividad, globalización, velocidad de los cambios, capacidad de adaptación, crecimiento y tecnología. Equilibrar estos y otros requisitos empresariales puede constituir un proceso difícil y desalentador. Es aquí donde entran en juego los sistemas de gestión, al permitir aprovechar y desarrollar el potencial existente en la organización.

La implementación de un sistema de gestión eficaz puede ayudar a:

- Gestionar los riesgos sociales, medioambientales y financieros.
- Mejorar la efectividad operativa.
- Reducir costos.
- Aumentar la satisfacción de clientes y partes interesadas.
- Proteger la marca y la reputación.
- Lograr mejoras continuas.
- Potenciar la innovación.
- Eliminar las barreras al comercio.

- Aportar claridad al mercado.

El uso de un sistema de gestión probado le permite renovar constantemente su objetivo, sus estrategias, sus operaciones y niveles de servicio.

¿Qué es la Norma ISO 27001:2005?.

Es la normativa certificable para los Sistemas de Gestión de Seguridad de la Información, la cual evolucionó del estándar ISO 17799 que a su vez se derivó de la BS 7799. La finalidad de esta norma es permitir de forma sistemática minimizar el riesgo y proteger la información en las empresas.

La norma ISO 27701:2005 está constituida por 8 clausulas y Anexos, de los cuales la parte medular del sistema son desde la cláusula 4 a la 8 y el Anexo A. Las cláusulas indican los procedimientos que deben ser implementados, los documentos que deben ser elaborados y los registros que deben ser mantenidos dentro de la organización. El anexo A indica los controles y objetivos de control a implementar con el fin de ser salvaguardas o contramedidas, los mismos que se encuentran distribuidos en 11 dominios de cobertura que son:

- A.5 Política de seguridad
- A.6 Organización de la seguridad de la información
- A.7 Gestión de activos
- A.8 Seguridad de los recursos humanos
- A.9 Seguridad física y ambiental
- A.10 Gestión de las comunicaciones y operaciones
- A.11 Control de acceso
- A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información
- A.13 Gestión de incidentes en seguridad de la información
- A.14 Gestión de la continuidad del negocio
- A.15 Cumplimiento

La metodología de los sistemas de gestión se basa en el Ciclo de Deming, llamado así en honor a su creador el estadista estadounidense William Edwards Deming, cuyas pasos son: Planear, Implantar, Revisar y Mejorar o PLAN-DO-CHECK-ACT (PDCA). La representación gráfica del ciclo de Deming abstrae el concepto de mejora continua por la retroalimentación del paso final al paso inicial.

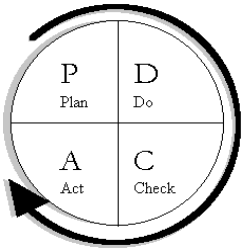


Figura 1. Ciclo de Deming (ref.1).

Las clausulas de la Norma se distribuyen usando como base el ciclo en mención cuya adopción operativa en la organización, constituye un factor clave para el Sistema de Gestión de Seguridad de la información (SGSI) o Information Security Management System (ISMS) por sus siglas en inglés .

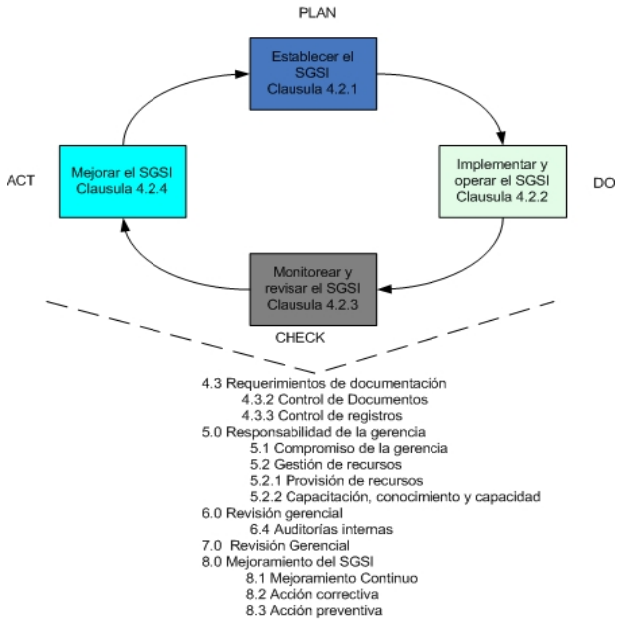


Figura 2. Clausulas de la Norma ISO 27001 distribuidas en Ciclo de Deming.

Descripción del escenario empresarial.

El contenido este documento se basa en el desarrollo de un sistema de gestión de la información para una empresa ecuatoriana autorizada como carrier, cuyo objetivo comercial es proveer servicio de telecomunicaciones mediante una Metroethernet y cuyo mercado mayoritario son: corporaciones, proveedores de Internet, entidades financieras, operadores celulares, entre otros.

Las principales motivaciones para que una empresa de servicios implante un SGSI son:

- Minimizar las pérdidas mediante la gestión del riesgo.
- Cumplimiento con leyes nacionales e internacionales.
- Diferenciador de la competencia.
- Exigencia por parte de sus clientes.
- Ingresar a mercados internacionales, más exigentes.
- Convertirse en un proveedor confiable y contar con un BCP.

1. Implantación del Sistema de Gestión de Seguridad de la Información.

El ciclo metodológico para la implantación de un sistema de gestión de seguridad de la información ISO 27001:2005 comienza con un entendimiento de los requerimientos del modelo y se retroalimenta en el último paso con la certificación del Sistema, como se lo muestra en la figura adjunta.

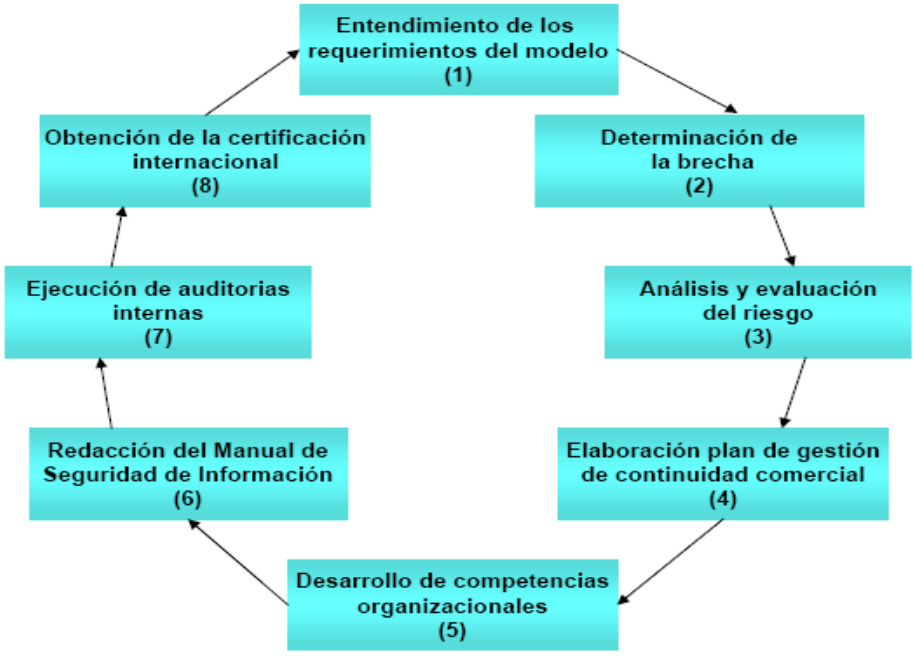


Figura 3. Ciclo Metodológico de implantación ISO 27001:2005.

Enfocándonos en la fase de arranque del ciclo metodológico, donde se indica que la organización debe entender los requerimientos del modelo, la recomendación es que se debe contar con personal cuyas competencias sean las adecuadas o en su defecto es válida la contratación de asesoría externa con experiencia comprobada. Si la variable tiempo no es crítica, las competencias del personal pueden ser desarrolladas mediante cursos enfocados a la interpretación e implantación de la Norma ISO 27001:2005.

Los capítulos e ítems que se redactan continuación constituyen la metodología sistemática detallada para implantar el SGSI ISO27001:2005 y cuya secuencia de redacción corresponde a una cronología real dentro de nuestro escenario empresarial, un proveedor de servicio de telecomunicaciones.

1.1 Metodología de implantación.

La metodología de implantación debe desarrollarse acorde a la cláusulas 4.2 descrita en la Norma ISO 27001:2005 correspondiente al establecimiento y operación de SGSI. La misma que nos indica que debemos definir el alcance y límites del SGSI en términos de las características del negocio, la organización,

su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance.

La definición del alcance del sistema es responsabilidad de la dirección de la organización bajo el asesoramiento del equipo de trabajo destinado a la gerencia del proyecto. También se acostumbra , para la toma de decisiones coyunturales, constituir un comité de seguridad liderado por el Director o Gerente General y conformado por Gerencias de diferentes áreas como la de tecnología, financiera, Recursos Humanos, Comercial, operaciones, etc.

El alcance para el proveedor de Servicio de Telecomunicaciones es:

"La provisión de un sistema de gestión de seguridad de información, para los procesos de: monitoreo, control de cambios, aprovisionamiento y mantenimiento de la red de telecomunicaciones en Guayaquil y Quito".

La clausula 4.2.1 de la norma también nos indica que debemos establecer una política de seguridad de la información acorde a las características del negocio, organización, activos, regulaciones y tecnología. Es muy poco exacto redactar una política de seguridad para toda la organización al iniciar el proceso de

implantación, la buena práctica es redactarla en paralelo al proceso de acuerdo a las necesidades del sistema, que irán apareciendo. Lo que se recomienda es redactar una Política de Seguridad de Información GENERAL que guíe lo que queremos conseguir mediante nuestro SGSI. Para nuestro caso la política general es:

"Proveer Servicios de Telecomunicaciones con un Sistema de Gestión de Seguridad de la Información basado en la Prevención y enfocado a minimizar el riesgo de incidentes que atenten contra la confidencialidad, integridad y disponibilidad de la Red " .

1.1.1 Identificación los procesos.

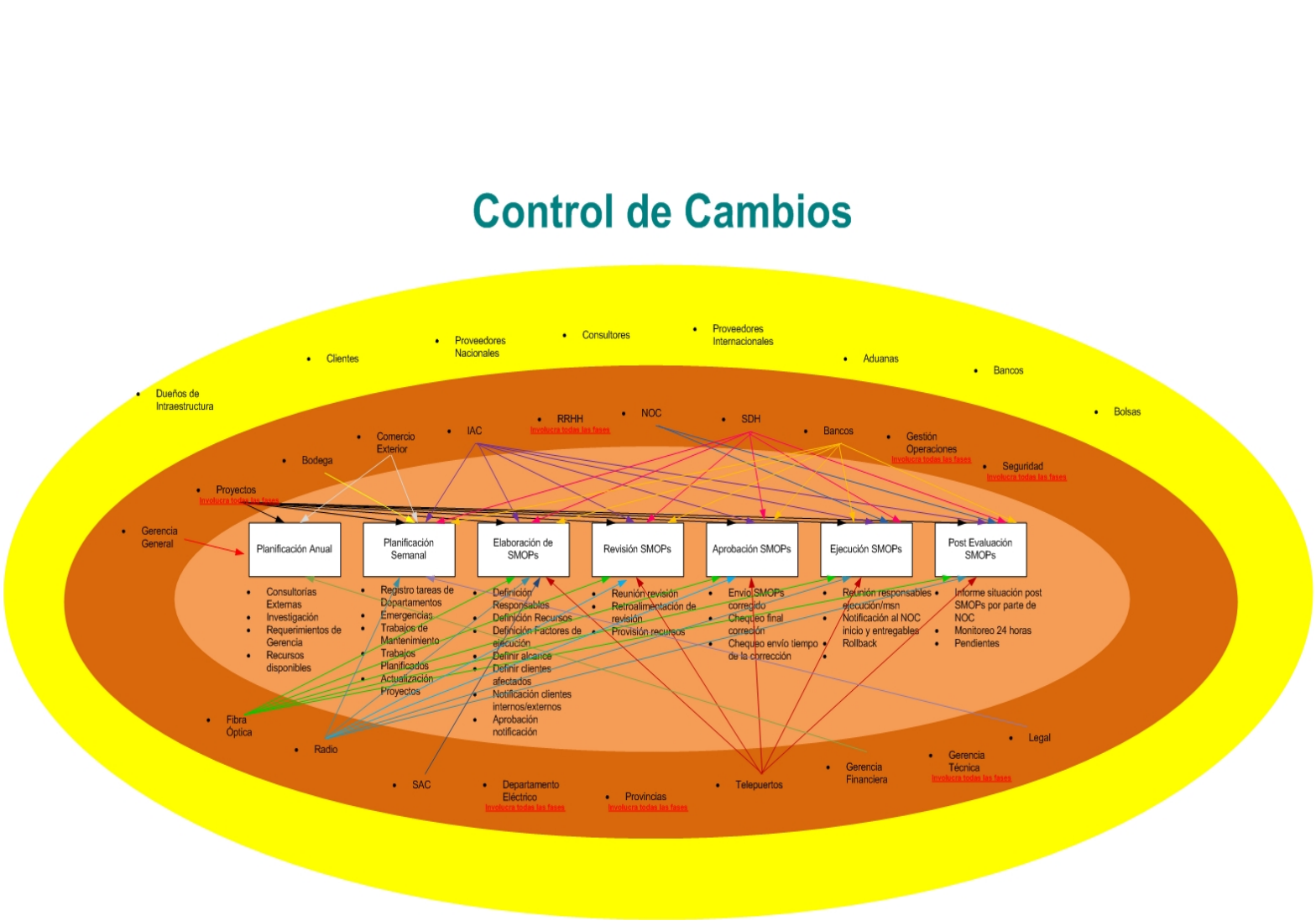
La identificación de procesos dentro del alcance constituye un pilar fundamental para el enfoque del SGSI. En nuestro caso los procesos involucrados son: Monitoreo, Control de cambios, mantenimiento y aprovisionamiento.

Para una organización donde no exista una cultura de procesos o simplemente no se los tiene identificado es recomendable primero realizar un correcto levantamiento de procesos antes de avanzar con la implantación del SGSI.

Métodos de las elipses.

El método de las elipses es un mecanismo que permite identificar dentro de un proceso todas las relaciones de sus subprocesos y actividades con otras áreas de la organización, y entidades externas. Una vez establecidas las relaciones es casi natural poder identificar los activos de información que se usan en dicha relaciones.

A continuación se presenta el resultado del método de las elipses para el proceso control de cambios. Este trabajo se lo realiza a manera de un taller interno multidisciplinario para cubrir todas las percepciones.



ACTIVOS
Project Server
Sistema email
Guía Técnica
Guía operativa
Servidor Project server
Reporte de emergencia
Listado de tareas determinada
Equipos laboratorio
Simuladores
Equipo para elaborar SMOP
Notificación de trabajo
Lista de clientes afectados
Email
SMOPs
BD desarrollo
Script server desarrollo
Sistemas AAAA
Documentos SMOP corregido
Revisión SMOPs
SMOPs revisados
MSN
Equipos backbone
Script server producción
BD producción
Sistemas DNS
Sistemas monitoreo
ORION/WUP
Sistema OG
Repositorios contingencias
Diagramas de red
Sistema asignación de claves
Instructivos simulacros
Sistema intranet
Sistema de autentificación de los equipos
Scripts
Fibra óptica backbone
Enlaces radio backbone
Sistemas de backup
Reporte trabajos programados
Personal noc
Standby proyectos
Gantt planificación annual
Forecast de ventas
Presupuesto annual
Sistema rrhh
Sistema NAF
Contactos RRHH
SLA

Figura 4. Método de las elipses.

1.1.2 Identificación y tasación de activos.

Los activos de información pueden ser el software, el hardware, los enlaces, el equipamiento, los documentos, las personas que manejen (Procesen, trasladen, almacenen) información de valor para el negocio de la organización. El proceso de tasación de activo también es recomendado hacerlo mediante un taller multidisciplinario.

Las relaciones encontradas mediante el método de las elipses nos permitieron visualizar con claridad los activos involucrados. El siguiente paso es tasar el listado de los activos para quedarnos con aquellos de mayor valor. La pregunta para evaluar es ¿la pérdida o deterioro de este activo, cómo afecta la disponibilidad, confidencialidad e integridad del proceso del negocio de la compañía? , en nuestro caso se usó la escala de 1 a 5, siendo el 1 de menor afectación y 5 de mayor afectación. El valor total del activo es el promedio entero de los valores asignados a la disponibilidad, confidencialidad e integridad. Una vez calculado el valor por cada activo seleccionamos aquellos de mayor valor, el valor umbral queda a discreción de cada organización por ejemplo serán de importancia aquellos con un valor mayor a 3.

TASACIÓN DE ACTIVOS

1. ¿Para qué sirve la tasación de activos?: Sirve para ver el impacto que tienen los activos en la empresa

2. PREGUNTA A SER REALIZADA CADA VEZ QUE TASAMOS UN ACTIVO: ¿Un deterioro o perdida en el activo X como impacta la confidencialidad, integridad y disponibilidad en el proceso de MONITOREO?

	Dueño	Confidencialidad	Integridad	Disponibilidad	TOTAL
Sistema Og	Sistemas	1	1	4	2
Sistema whastup	NOC	1	1	5	2
Sistema Orion	NOC	1	1	4	2
sistema aaaa	Ingeniería	4	4	2	3
Sistema de Incidencias SIT	Sistemas	2	3	1	2
Utilitario Microsoft	Jefe Departamento	2	3	2	2
Sistema Email	Ingeniería	3	2	4	3
Sistema Mensajeria Instantanea	Jefe Departamento	1	1	3	2
Sistema OOB	Ingeniería	3	2	4	3
Router NOC	NOC	1	3	3	2
Líneas telefónicas externas	Ingeniería	1	1	4	2
Minibodega	NOC	1	1	1	1
Sistema GPRS	NOC	3	2	3	3
Personal Standby	NOC	3	2	4	3
Equipos de monitoreo (PC)	NOC	1	1	2	1
Bases celulares	Jefe Departamento	1	1	4	2
Diagramas	Jefe Departamento	1	4	3	3

Sisetma Base Datos Whats,up	Ingeniería	1	2	3	2
Sistema de llaves nodos	NOC	1	2	3	2
Lista de escalamientos	NOC	1	3	3	2
Informes SLA	NOC	1	2	2	2
Internet	Ingeniería	1	2	2	2
Respaldos de documentos	Jefe Departamento	1	2	2	2
Servidor acceso (.21/iserver)	Ingeniería	1	1	3	2
CACTI	Ingeniería	1	1	5	2
Sistemas DNS	Ingeniería	1	1	3	2
Notificaciones	NOC	1	3	3	2
Reportes de monitoreos	NOC	1	2	3	2
Telepuerto kennedy	NOC	1	4	4	3
Telepuertos Bellavista	Telepuerto	1	4	5	3
Telepuerto Gosseal	NOC UIO	1	4	5	3
Telepuerto Muros	NOC UIO	1	4	4	3
sistema eléctrico Telepuertos	DPTO. ELECTRICO	1	1	5	2
Momitores del NOC	NOC	1	1	2	1
Control de Acceso(Fisico)	SEC	3	1	1	2
Asterisk	Ingeniería	2	2	4	3
UPS del NOC	NOC	1	2	4	2

Cuadro 1.- Tasación de Activos.

La tasación también se la realiza para los activos de los otros 3 procesos: control de cambio, aprovisionamiento y mantenimiento. Como resultado tenemos el listado de los activos importantes para la compañía.

ACTIVOS IMPORTANTES			
Mantenimiento	Monitoreo	Control de Cambios	Aprovisionamiento
Herramientas de fusión y medición	Sistema What´s up	Servicio Project (Web Access)	Instalaciones
Movilización	Sistema ORION	Sistema email	Contrato con clientes
Personal de Standby	Sistema Incidencias SIT	Sistema OOB	Ing. VIP
Sistema Eléctrico	Router NOC	Sistema OG	PCs de Técnicos
Personal del NOC	Lineas Telefónicas externas	Script Server Producción	Personal de Ventas
Instructivos	PCs del NOC	Equipos de Laboratorio	Proxy
Sistema Celular	Sistema GPRS	Simuladores	Bodega GYE
Telepuertos Gye - Uio	Servidor de acceso	Sistema de Base de Datos	Asterisk UIO
Fibra óptica Nodos		SMOPs	
Fibra óptica Backbone		Notificaciones de trabajo	
Nodos backbone		Diagramas de Red	
Nodos edge		Sistema DNS	
		SAN	
Sistema de llaves		Sistema de monitoreo y control SDH	
Enlaces de radio de backbone		Sistema NOF	
		Equipos de backbone SDH	

Cuadro 2. Activos Importantes.

1.1.4 Metodologías del análisis y evaluación del riesgo.

De igual manera que en los pasos previos, el análisis y evaluación del riesgo se lo lleva a cabo en un taller multidisciplinario de la organización. Para el análisis y evaluación del riesgo, nos podemos acoger a cualquier metodología conocida, pero la exigencia de la norma es que dicha metodología arroje resultados comparables y reproducibles, esto quiere decir que el producto debe ser similar si la evaluación la hace otro grupo taller multidisciplinario o si lo hace el grupo taller inicial en otro momento.

La recomendación es usar un método cualitativo para el cálculo del riesgo, puesto que puede abarcar todos los activos con mayor facilidad. El método cuantitativo exigiría que todo sea llevado a valor monetario y en la mayoría de los casos esta tarea es complicada y/o tarda demasiado, puesto que no sólo implica el valor comercial de los activos sino también de la afectación que pueden tener su entorno.

Nuestra metodología consiste que para cada activo debemos identificar todas las amenazas existentes, la posibilidad de ocurrencia de estas amenazas, las vulnerabilidades que pueden hacer que dicha amenaza se materialice y la

posibilidad que dicha amenaza penetre tal vulnerabilidad. El valor del riesgo está dado por el producto matemático del valor del activo, encontrado en la tasación, por el valor de la mayor de posibilidad de amenaza.

La escala para calcular las posibilidades es de 1 al 5, siendo 5 mayor. De la misma forma como en la tasación de activos se puede descartar las de menor valor para enfocarnos en las verdaderamente importantes, el valor del umbral es decisión del grupo taller. A continuación se presenta el análisis y evaluación del riesgo para un grupo de activos, del proceso monitoreo.

Activos de información	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en Riesgo	Posibilidad de ocurrencia de amenaza	Total RIESGO
Sistema What´s up	A. Falla de la base Datos B. Virus C. Falla Hardware D. Falla del Sistema E. ~~Mal Funcionamiento~~	2 4 2 2 1	A.1 No tener backup B.1 Falta de mantenimiento y políticas B.2 Falta de control de acceso C.1 Falta de mantenimiento C.2 Equipos sin redundancia C.3 Falta de control de manipulación D..1 Equipos sin redundancia D.2 Instalación no controlada de software	2 4 3 3 3 1 2 3	**2**	**4**	**8**
Sistema ORION	A. Falla de la base Datos B. Virus C. Falla Hardware D. Falla del Sistema E. ~~Mal Funcionamiento~~	2 4 2 2 1	A.1 No tener backup B.1 Falta de mantenimiento y políticas B.2 Falta de control de acceso C.1 Falta de mantenimiento C.2 Equipos sin redundancia C.3 ~~Falta de control de manipulación~~ D..1 Equipos sin redundancia D.2 Instalación no controlada de software	2 4 3 3 3 1 2 3	**2**	**4**	**8**
Sistema Incidencias SIT	A. Falla de base datos B. Falla de hardware C. Ingreso información errónea D. Perdida de acceso	2 2 3 3	A.1 No tener redundancia B.1 Falta de Mantenimiento B.2 Falta de redundancia C.1 Falta de control de procedimiento C.2 Personal novato en producción D.1 Falta comunicación en trabajos de mantenimiento	3 2 3 2 2 3	**2**	**3**	**6**

Activos de información	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en riesgo	Posibilidad de ocurrencia de amenaza	Total RIESGO
Router NOC	A. Fallo de hardware B. Fallo de software C. ~~Fallo de red~~ D. Hackeo o DoS	2 2 1 2	A.1 Falta de equipo redundante A.2 Uso de equipo no modular B.1 ~~Bugs del IOS de CISCO~~ B.2 Falta de monitoreo B.3 ~~Errores configuración~~ D.1 Falta de buenas prácticas de seguridad	4 2 1 2 1 2	**2**	**2**	**4**
Lineas Telefónicas externas	A. Falta de servicio B. ~~Escuchas Electrónicas~~	2 1	A.1 Falta de pago A.2 Congestionamiento A.3 Falta proveedor alterno	2 3 2	**2**	**2**	**4**
PCs del NOC	A. Falla hardware B. Virus C. Falla de software D. ~~Perdida o Robo~~ E. Multa por software sin licencia	2 3 2 1 2	A.1 Falta de mantenimiento A.2 Falta de equipo de respaldo B.1 Falta de buenas prácticas B.2 Falta de sistema de antivirus confiable C.1 ~~Falta de sistema de almacenamiento de información~~ E.1 Uso de software sin licencia	3 3 2 2 1 3	**1**	**3**	**3**

Activos de información	Amenazas	Posibilidad de ocurrencia de la amenaza	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos en riesgo	Posibilidad de ocurrencia de amenaza	Total RIESGO
Sistema GPRS	A. Falla en la red del proveedor B. Daño o deterioro del equipo GPRS	3 3	A.1 Falta de contingencia B.1 Escasez de equipos B.2 Falta de mantenimiento	2 4 3	**3**	**3**	**9**
Servidor de acceso	A. Fallo de software B. Fallo de hardware C. Hackeo	2 2 3	A.1 Falta de control de actualización de software A.2 Bugs del S.O. B.1 Falta de servidor de respaldo B.2 Falta de respaldo de interfaces C.1 Falta de análisis de vulnerabilidades C.2 Falta de firewall local C.3 Falta de monitoreo de logs C.4 Falta de control de claves	2 2 3 2 3 3 3 3	**2**	**3**	**6**

Cuadro 3. Análisis y Evaluación del riesgo**.**

NOTA.- Se tachan aquellas amenazas y vulnerabilidades despreciables.

1.1.5 Tratamiento del riesgo.

El análisis y evaluación riesgo nos permitió valorizar el riesgo y conocer cuáles son los activos de información que tienen mayor exposición por lo tanto saber a dónde enfocar los recursos de la organización.

El riesgo tiene 4 opciones de tratamiento que son:

- *Reducir el riesgo*, con la aplicación de contramedidas o salvaguardas especificadas controles del Anexo A de la norma.
- *Evitar el riesgo*, dejando de realizar la actividad que produce el riesgo.
- *Transferir el riesgo*, a un tercero como por ejemplo una aseguradora o una tercerización de servicios.
- *Aceptar el riego*, que consiste en asumir la responsabilidad de correr dicho riesgo.

La opción de aceptación de un riesgo deber ser aprobada formalmente por la dirección de la compañía, en la mayoría de casos se presenta esta situación cuando el control necesario de implantar tiene un valor económico mayor que el mismo activo.

En nuestro caso la única opción de tratamiento que se usó fue la de reducción del riesgo.

1.1.6 Selección de controles.

Los controles son las contramedidas o salvaguardas especificadas en el Anexo A de la Norma ISO 27001:2005, enfocados a los 11 dominios de cobertura de la norma, como son:

- A.5 Política de seguridad.
- A.6 Organización de la seguridad de la información.
- A.7 Gestión de activos.
- A.8 Seguridad de los recursos humanos.
- A.9 Seguridad física y ambiental.
- A.10 Gestión de las comunicaciones y operaciones.
- A.11 Control de acceso.
- A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información.
- A.13 Gestión de incidentes en seguridad de la información.

- A.14 Gestión de la continuidad del negocio.
- A.15 Cumplimiento.

La selección de los controles que la organización debe implementar se lo hace por 3 fuentes:

- Del tratamiento del riesgo, orientados a eliminar vulnerabilidades o minimizar el impactos.
- Los requerimientos legales (implementación no es discutible).
- Producto de las operaciones en el negocio de la compañía.

Si se requiere una mayor ampliación de las prácticas para implementar los controles se puede referenciar a la ISO 17799:2005. También existe la posibilidad de que la organización cree sus propios controles puesto que los que se describen en la norma no se adapta a nuestras necesidades. En nuestro caso creamos un control con la nomenclatura T1 que se refiere a tener un equipo de contingencia.

Análisis y Evaluación del Riesgo									Opciones de Tratamiento del riesgo		
Activos de información	Dueño de Activo	Amenazas	Posibilidad de ocurrencia	Vulnerabilidades	Posibilidad que la amenaza penetre la vulnerabilidad	Valor de activos de Riesgo	Posibilidad de ocurrencia de amenaza	Total de cálculo del Riesgo	**Opción de tratami-ento de riesgo**	**Objetivos de control**	**Controles de la norma ISO 27001**
Servicio Project (Web Access)	Ingeniería	A. Daño del software B: Falla de Hardware C. Hacking D. ~~Fallas de red~~ E. Virus F. Fallos eléctrico	3 3 2 1 2 2	A.1 Falta de capacitación B.1 ~~Equipo tipo clon no confiable~~ B.2 ~~Falta de recursos (memoria,hw)~~ B.3 Falta de respaldo C.1 Sistema sin revocación claves C.2 Vulnerabilidades del Windows E.1 Malware DIA ZERO F.1 Falta de fuente redundante G.1 Falta de control de datos de salida	4 1 1 3 2 2 2 2 2	**1**	**3**	**3**	**Reducción del riesgo**	**A.11.2 Gestión de acceso a usuarios** **A.12.5 Control de Acceso al S.O.** **A.12.6 Vulnerabilidades Técnicas** **T.1 Asegurar la disponibilidad del equipo con sistemas de respaldo**	**Control(Vulnerabilidad)** **A.11.2.3 (C.1)** **A.12.5.2 (C.2)** **A.12.6.1 (E.1)** **T.1 (A.1,B1, B2, B3, F.1)**

Sistema email	Ingeniería	A. Daños de software B. Falla o falta de hardware C. Hacking D. Ataques remotos (DoS,Spam) E. ~~Virus~~ F. ~~Fallo Eléctrico~~ G. ~~Falla de red~~	2 2 4 4 1 1 1	A.1 ~~Bugs del sistema~~ A.2 Error de configuración A.3 ~~Desactualización~~ A.4 Daño no intencionado por personal interno B.1 Falta de balanceador de carga automática C.1 Acceso Publico C.2 desactualización C.3 bug del sistema C.4 Malware día Zero C.5 ~~Daño intencionado por personal interno~~ C.6 Falta de protección de sandvine D.1 Falta de protección IDS/IPS D.2 Acceso publico D.3 Falta de políticas locales D.4 ~~Falla de antivirus , antispam~~	1 2 1 2 3 2 2 2 2 1 3 3 2 2 1	**3**	**4**	**12**	**Reducción del riesgo**	**A.9.2 Seguridad de equipos** **A.10.1 Procedimiento y responsables de la operación** **A.12.6 Vulnerabilidades Técnicas** **A.10.3 Planificación y Aceptación del Sistema** **A10.6 Gestión de la seguridad de la red** **A.11.6 Control de acceso a a aplicaciones** **A.11.4 Control de acceso a la red**	**Control (Vulnerabilidad)** **A.9.2.4 (C.2)** **A.10.1.2 (A.2)(A.4)** **A.12.6.1(C.4)(C.3)** **A.10.3.1(B.1)** **A.10.6.1(D.2)** **A.11.2.3 (C.1)** **A.11.6.1 (D.3)**

Cuadro 4. Selección de controles.

Uno de los requerimientos de la norma ISO 27001:2005 es que la organización cuente con una DECLARACION DE LA APLICABILIDAD, que consiste en un documento que comprometa e identifique los controles del anexo A de la Norma que se implementarán y la justificación en caso de que no proceda. Esto significa que por defecto todos los controles de la norma son aplicables a la organización y cualquier excepción debe ser justificada.

La declaración de aplicabilidad debe ser aprobada y revisada por la alta dirección de la empresa (Gerencia General).

Objetivo de Control	Control	Aplica SI/NO	Justificación

Cuadro 5. Encabezado de la Declaración de la Aplicabilidad.

1.1.7 Medición de efectividad de los controles.

Una vez que los controles han sido implantados es necesario revisarlos constantemente que estén cumpliendo su objetivo. La medición de los controles se lo puede hacer mediante indicadores de efectividad, por ejemplo, si luego del análisis y evaluación de riesgo sobre el activo “Nodos Edge”, salta a la luz que

debemos implementar u optimizar el control A.9.2.2 de la Norma ISO 27001:2005 (Anexo A) cuyo objetivo de control son los servicios público y nos indica que los equipos deben ser protegido de fallas de energía y otras interrupciones por fallas de los servicios públicos. Los indicadores pueden ser de tipo seguimiento o de rendimiento, un indicador de seguimiento aplicado al control A.9.2.2 es el porcentaje de “Nodos Edges” por cada ciudad que pierde conectividad durante un apagón nacional.

Un indicador de rendimiento o performance puede ser el Tiempo de Supervivencia Real de un Nodo Edge durante un apagón / sobre el Tiempo Estimado de respaldo, este indicador nos mostraría que tan acertados han sido los trabajos de mantenimiento.

El indicador más significativo para un proveedor de servicio de telecomunicaciones es el llamado Acuerdo de Nivel de Servicios o SLA (*Service Level Agreement) por sus siglas en inglés,* establecido en los contratos, medido en porcentaje de disponibilidad del servicio. En términos generales consiste en calcular el tiempo de disponibilidad de un enlace dividido sobre el tiempo transcurrido. En implementaciones más sofisticadas el SLA también se puede

ver afectado por variables o sub-indicadores como son el porcentaje de paquetes perdidos, jitter y/o delays.

Cada organización debe escoger los indicadores que económica y operativamente sean factibles implementar y llevar a cabo su medición. Pero sobre todas las cosas estas mediciones deben agregar valor a los objetivos del negocio de la compañía.

Algunos indicadores de tecnología son: porcentaje de falsos positivos de un IDS/IPS, porcentaje de disponibilidad de un Servidor WEB, porcentaje de solución de Incidentes que se extiende más de un tiempo X, Número de casos de Phishing presentados en el mes por ciudad, Número de Clientes que caen en listas negras de SPAM por Ciudad, Número de empleados infectados con virus por mes por ciudad.

La recomendación es que la medición de los indicadores debe institucionalizarse dentro de las operaciones del SGSI y conforme se optimice el sistema, dichas mediciones deben automatizarse.

1.1.8 Riesgos residuales.

El riesgo residual como su nombre lo indica, son aquellos riesgos remanentes aún cuando se haya implementado todos los controles necesarios. Los riesgos residuales deben ser conocidos, revisados y aprobados por la dirección de organización.

Conforme se optimiza el sistema estos riesgos residuales tienden a disminuir. Los riesgos residuales por lo general siempre están presentes puesto que llegar a riesgo cero es casi imposible ya sea porque el costo de un mayor control es muy alto o porque su posibilidad de ocurrencia es muy remota pero no cero. Por ejemplo , A pesar de implementar el control A.8.1.2 que nos indica que debemos contar con un proceso formal de selección de personal que incluyan test sicológicos, la verificación de antecedentes , siempre puede existir la posibilidad que un empleado descontento sabotee algún sistema.

Otros riesgos residuales comunes son: bugs de hardware o software desconocidos incluso por el fabricante, ataques que aprovechen vulnerabilidades de día cero, amenazas ambientales como tormentas eléctricas,

derrumbes , que un empleado aún capacitado y evaluado contra ataques de ingeniería social sea vulnerado, etc.

1.2 Requisitos documentales.

En toda implementación de sistemas de gestión, un factor a superar es el sistema documental exigidos por la norma, entre los principales motivos podemos mencionar:

- Se percibe como una carga operativa que no se quiere asumir.
- Rechazo al cambio.
- Informalidad muy institucionalizada.

Para poder obtener una certificación, hay que superarlo y utilizar mecanismos tecnológicos que faciliten la institucionalización del sistema documental. La recomendación es implementar un sistema intranet que pudiera usar protocolo HTTP y/o FTP para la gestión de documentos. Dicho sistema debe manejar perfiles y roles así como también características del modelo AAA (Authentication, Authorization, Accounting).

La ISO 27001 tiene exigencias documentales que se indican en la cláusula 4.3 de dicha norma y son:

- Enunciado de la política de seguridad y los objetivos.
- El alcance del SGSI.
- Procedimientos y controles de soporte del SGSI.
- Una descripción de la metodología de evaluación del riesgo.
- Reporte de la evaluación del riesgo.
- Plan de tratamiento del riesgo.
- Enunciado o declaración de aplicabilidad.
- Procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles.
- Registros requeridos por este estándar internacional.

Los procedimientos documentados son:

- Debe existir un procedimiento documentados que especifique el manejo de documentos como es la creación, nomenclatura, aprobación, obsolescencia, cambios, etc.

- Debe existir un procedimiento documentado para el manejo de las auditorías, reporte de resultados y mantenimiento de registros.
- Debe existir un procedimiento documentado para el manejo de acciones correctivas.
- Debe existir un procedimiento documentado para el manejo de acciones preventivas.

Se deben mantener registros de:

- Auditorías realizadas.
- Resultados de las revisiones por la gerencia.
- Registros de capacitación, competencias, capacidades, experiencias y calificaciones.
- Y todos aquellos registros que otorguen evidencia objetiva del cumplimiento con la norma.

Una buena práctica es identificar textualmente todos los “debes” dentro de la redacción de la norma para así poder identificar las exigencias explícitas.

1.3 Factores de éxito

Existen factores que son claves para una implantación exitosa del sistema de gestión de seguridad de la información. Entre ellos podemos mencionar:

- Compromiso de la dirección con el SGSI.
- Objetivos del SGSI deben estar alineados con el negocio de la compañía.
- Liderazgo de la gerencia del proyecto.
- Motivación del personal.
- Concientización de toda la organización para con la seguridad.
- Embeber en todos los procesos del negocio el ciclo PLAN-DO-CHECK-ACT e institucionalizar la mejora continua.
- Establecer claramente las responsabilidades y obligaciones de cada persona dentro del SGSI.

2. Mejoramiento Continuo del SGSI.

Cuando una organización decide implementar un SGSI y certificarlo significa que ha tomado la decisión de encaminar sus operaciones en base a las mejores prácticas recomendadas por la Norma ISO27001:2005. Pero el verdadero éxito está en la sofisticación del sistema para ellos es necesario el mejoramiento continuo. El mejoramiento continuo está intrínseco en el modelo PLAN-DO-CHECK-ACT o Ciclo de Deming sobre el cual se basa los sistemas de gestión.

2.1 Mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información.

La norma nos exige que el SGSI debe ser monitoreado y revisado, lo mismo que viene dado por los siguientes puntos:

- Medir la efectividad de los controles.
- Realizar auditorías interna.
- Realizar auditorías externas.
- Revisión por la dirección de todo el SGSI (cumplimiento de objetivos y resultados).

- Reuniones gerenciales para revisar acciones correcticas, acciones preventivas, oportunidades de mejoras.
- Correcta ejecución del procedimiento para reportar y tratar incidentes.
- Reevaluación de los riesgos cuando las condiciones de negocio o entorno cambien.
- Revisar los riesgos residuales.
- Sofisticación de los mecanismos de medición.

2.2 Metodología.

La metodología que la organización escoja para el mejoramiento continuo es flexible a la realidad tecnológica, operativa y económica de la organización. Pueden considerarse métricas de mejoramiento como son : número de proyectos de mejoras implantadas por un área en particular, la efectividad de una acción correctiva o preventiva, la disminución de tal o cual incidente, el ajuste de los controles a través del tiempo, la reducción de los riesgos residuales. La premisa de la metodología debe ser que no es necesario esperar una auditoría para emprender acciones correctivas, preventivas o proyectos de mejora.

Es importante tener claro el procedimiento de mejora continua, para saber cuándo abrir o cerrar una acción correctiva, preventiva u oportunidad de mejora.

Una ***acción correctiva (AC)***, se levanta ante algún incidente presentado o cuando alguna no conformidad con la norma haya sido detectada. Esta acción es cerrada únicamente cuando se puede comprobar la efectividad de la misma es decir cuando el incidente no vuelva a ocurrir.

Una ***acción preventiva (AP),*** se levanta para garantizar que un evento presentado no se convierta en un incidente.

Una ***oportunidad de mejora***, como su nombre lo indique son aquellas actividades que se realizan sin necesidad de la presencia de un incidente o un evento, por lo general contribuyen directamente a la sofisticación del SGSI.

También se puede usar una acción curativa o inmediata, que consiste en aquella que permite cubrir el incidente hasta poder encaminar una acción correctiva. Para nuestro caso real, del proveedor de servicio de telecomunicaciones, el objetivo fue concientizar a la gente respecto al mejoramiento continuo e institucionalizar el correcto uso del formato y/o

procedimiento. En una compañía como la nuestra las reuniones de planificación gerencial son continuas por lo cual nos enfocamos en adoptar formatos y medios tecnológicos de mejora continua en dichas reuniones y así no duplicar procedimientos ni documentación. Por ejemplo para cualquier actividad a realizarse durante la semana debe especificarse cual es su origen es decir debemos indicar si es una acción correctiva, acción preventiva u oportunidad de mejora. Cabe recalcar que el registro, operación y el cierre de dicha actividad ya estaban manejados por nuestros procedimientos operacionales.

A continuación se presenta un formato usado para la gestión del mejoramiento continuo.

GESTIÓN DE MEJORAMIENTO CONTINUO

AÑO: 2008

No.	Ciudad	Apertura	TIPO	Origen	Área	Hallazgo	Identificado por:	Responsable	Controlado por:	Solución Inmediata o curativa	Causa Raíz	Acciones Correctivas	Acciones Preventivas	Plazo de AC/AP	Cumplimiento de la AC/AP	Comentarios	Verificacion de Eficacia	Fecha de Verificacion de Eficacia	Estado de la AC/AP
90	Guayaquil	17-nov-08	AC	Incidencia	Seguridad	Los equipos Observer para el análisis de la red no facilitan la trazabilidad de los incidentes	NOC	Cert	CERT	Levantar el servicio del observer que se encontraba inhibido	La topología actual del sistema observer ya no abastece los requerimientos de la red	Rediseño e implementación de un nuevo sistema de servidores observers		22-dic-08	Pendiente	Se verificará la eficacia simulando un analisis de tráfico por parte de los técnicos de soporte	Simulación	01-ene-09	ABIERTA

Figura 5. Formato para la gestión del mejoramiento continuo.

2.3 Factores de éxito.

Un factor clave para el establecimiento del mejoramiento continuo es que existan políticas claras establecidas y un impulso jerárquico desde la dirección. Entre los factores importantes podemos mencionar:

- Gerencias de área debe asumir tareas de seguimiento.
- Adaptar procesos actuales al ciclo PDCA.
- Tratar las tareas o provectos como acciones correctivas, preventivas u oportunidades de mejora.
- Proveer herramientas tecnológicas que disminuyen gasto operativo.
- Establecer formatos adecuados y que estén adaptados a los objetivos del negocio (cosas que agreguen valor).
- Revisión del sistema de gestión o parte de él cuando un cambio del entorno del negocio se produzca.
- Establecer indicadores de rendimiento, revisarlos y actualizarlos. Es buena práctica revisar dichos indicadores cada mes.
- Todas las tareas de revisión y mejoras del SGSI deben ser reconocidas como aumento de responsabilidades y estar descritas en las funciones de cada empleado, por el departamento de recursos humanos.

- Establecer métricas de evaluación del personal basadas en el aporte al SGSI de la organización.

3. Plan de Continuidad del Negocio BCP.

Por definición el Plan de continuidad del Negocio o BCP es la creación, validación y práctica de un plan logístico que permita restaurar o recuperar de manera parcial o completa los procesos críticos del negocio de la compañía. La normativa de este plan es la BS-25999 pero también lo exige la norma ISO27001:2005 en el dominio A.10 del Anexo de dicho documento.

En el medio, existen enfoques relacionados como Plan de Contingencia (orientado a tecnología), Plan de Evacuación (Personas), Plan de Recuperación de Desastres (Instalaciones y TI). El éxito de la adopción de un BCP es que cubre todos esos aspectos de manera intrínseca y no se orienta sólo a la tecnología, personas o instalaciones sino a los procesos críticos del negocio por lo cual despierta gran interés de la dirección de la compañía.

La implementación de un BCP convierte a la organización en un proveedor confiable, en el caso de un proveedor de servicio de telecomunicaciones, esta

característica es buscada o exigida por los clientes. En nuestro medio el Estado exige a las organizaciones financieras cumplir con la resolución de la Junta bancaria JB-834, que se refiere al tratamiento del riesgo operativo y continuidad del negocio, quienes a su vez les exigen a sus proveedores contar con este tipo de plan. Creando así un efecto cadena.

3.1 Análisis del Impacto del Negocio BIA.

Bajo la premisa que ninguna organización tiene recursos ilimitados, lo primero que se debe hacer es enfocar esfuerzos en lo que realmente es importante para la organización. Para esto debemos identificar cuáles son los procesos, que si estuvieran detenidos, provocarían un mayor impacto negativo en la organización.

3.1.1 Identificación de procesos críticos.

El primer paso del Análisis del Impacto del Negocio BIA es identificar los procesos críticos y para ello es necesario conocer cuáles son los procesos de la organización. Nuevamente salta a la luz que una correcta Identificación e ingeniería de procesos agregaría gran valor a nuestro proceso de

implementación. Por lo general es muy notorio el proceso principal de la organización pero existen otros igual de importantes que son necesarios identificarlos y priorizarlos. Para nuestro caso el proceso principal es el de CONEXIÓN.

Para la identificación de los procesos críticos se puede usar la metodología que mejor se adapte a la organización y la recomendación es hacerlo mediante talleres multidisciplinarios. Los procesos críticos se los escoge como producto del análisis del impacto financiero y del impacto operacional.

Una vez identificados los procesos del negocio calculamos primero el impacto financiero de cada proceso y le asignamos una escala de impacto según la pérdida económica por un día de estar parado dicho proceso y así podemos priorizarlos.

. A continuación se presenta la metodología usada en el BIA para un proveedor de servicio de telecomunicaciones.

.

Análisis del impacto financiero de los procesos de negocio

Procesos de Negocio	Valor	Severidad	Escala
Función de negocio: ADMINISTRATIVA			NO impacto-1
Almacenamiento y Despacho	$ 97.500	3	Menor-2
Gestión de recursos Financieros	$ 0	1	Intermedio-3
Compras	$ 0	1	Mayor-4
Pago de Nóminas	$ 0	1	
Gestión de Recursos Humanos	$ 0	1	
Proceso contable	$ 0	1	
Facturación	$ 500	2	
Cobranzas	$ 475	2	
Legalizaciones	$ 0	1	
Gestión de proveedores de Internet	$ 0	1	
Función de negocio: TÉCNICA			
Monitoreo	$ 100	2	
Instalaciones	$ 3.310	2	
Mantenimiento Preventivo	$ 0	1	
Mantenimiento Correctivo Fisico	$ 450.000	4	
Administración de Red	$ 50.000	4	
Soporte Técnico	$ 500	2	
Control de Cambios	$ 0	1	
Investigación/Desarrollo	$ 0	1	
Incidencias Seg. Lógica	$ 0	1	
Conexión	$ 500.000	4	
Función de negocio: VENTAS			
Comercialización	$ 0	1	
Servicio al cliente	$ 0	1	
Desarrollo de Productos nuevos	$ 0	1	

Cuadro 6.- Calculo del impacto financiero de los procesos del negocio.

Los impactos operacionales se calculan en base a métricas que por lo general no pueden ser cuantificados fácilmente como son el impacto al Flujo de Caja, Imagen, Posicionamiento en mercado, cumplimiento legal, etc. Para estimar el impacto usaremos una escala de ninguno, bajo, medio, alto y altísimo.

A continuación presentamos el análisis del impacto operativo.

Análisis del impacto operacional de los procesos de negocio

Procesos de Negocio	Flujo de Caja	Participación de Mercado	Competitividad	Satisfacción cliente	Imagen	Ambiente Laboral	Cumplimiento Legal
Función de negocio: ADMINISTRATIVA							
Almacenamiento y Despacho	Ninguno	Medio	Bajo	Medio	Medio	Medio	Bajo
Gestión de recursos Financieros	Alto	Alto	Medio	Ninguno	Medio	Medio	Alto
Compras	Ninguno	Medio	Medio	Ninguno	Bajo	Bajo	Bajo
Pago de Nóminas	Ninguno	Ninguno	Bajo	Ninguno	Bajo	Altisimo	Alto
Gestión de Recursos Humanos	Ninguno	Ninguno	Bajo	Ninguno	Bajo	Altisimo	Bajo
Proceso contable	Ninguno	Ninguno	Bajo	Ninguno	Bajo	Ninguno	Alto
Facturación	Alto	Ninguno	Bajo	Alto	Alto	Ninguno	Bajo
Cobranzas	Altisimo	Ninguno	Bajo	Alto	Alto	Ninguno	Bajo
Legalizaciones	Ninguno	Alto	Alto	Bajo	Alto	Ninguno	Altisimo
Gestión de proveedores de Internet	Ninguno	Alto	Alto	Altisimo	Alto	Alto	Medio
Función de negocio: TÉCNICA							
Monitoreo	Ninguno	Alto	Altisimo	Altisimo	Altisimo	Alto	Alto
Instalaciones	Bajo	Alto	Altisimo	Altisimo	Altisimo	Medio	Bajo
Mantenimiento Preventivo	Bajo	Alto	Altisimo	Bajo	Alto	Bajo	Ninguno
Mantenimiento Correctivo	Medio	Alto	Altisimo	Altisimo	Altisimo	Alto	Ninguno
Administración de Red	Ninguno	Alto	Alto	Medio	Alto	Alto	Ninguno
Soporte Técnico	Ninguno	Altisimo	Altisimo	Altisimo	Altisimo	Alto	Alto
Control de Cambios	Ninguno	Alto	Alto	Alto	Alto	Alto	Ninguno
Investigación/Desarrollo	Ninguno	Alto	Alto	Alto	Alto	Bajo	Ninguno
Incidencias Seg. Lógica	Ninguno	Medio	Altisimo	Alto	Alto	Bajo	Alto
Conexión	Alto	Altisimo	Altisimo	Altisimo	Altisimo	Alto	Alto
Función de negocio: VENTAS							
Comercialización	Medio	Alto	Alto	Alto	Altisimo	Alto	Ninguno
Servicio al cliente	Bajo	Alto	Alto	Altisimo	Altisimo	Medio	NInguno
Desarrollo de Productos nuevos	Ninguno	Alto	Alto	Alto	Alto	Medio	Ninguno

Cuadro 7. Cálculo del impacto operativo de los procesos del Negocio.

Una vez hecho el análisis de los impactos económicos y operativos, se consideraron procesos críticos si cumplen con cualquiera de los siguientes puntos:

- Tiene una severidad 3 ó 4 en los impactos financieros.
- Una clasificación de alta se asigna por lo menos a tres de sus impactos operacionales.
- Una clasificación de alta se asigna al menos a dos y una clasificación de altísima se asigna a uno de sus aspectos operacionales.
- Una clasificación de altísima se asigna por lo menos a dos de sus impactos operaciones.
- Aquel proceso que bajo circunstancia extremas sería vital para sus empleados, como por ejemplo el pago de nómina.

Los proceso críticos identificados para el proveedor de servició de telecomunicaciones son:

- Almacenamiento y despacho
- Gestión de recursos financieros
- Pago de nóminas

- Facturación
- Cobranzas
- Legalizaciones
- Gestión de proveedores de Internet
- Monitoreo
- Instalaciones
- Mantenimiento preventivo
- Mantenimiento correctivo
- Administración de red (mantenimiento lógico)
- Soporte técnico
- Control de cambios
- Investigación/Desarrollo
- Conexión
- Comercialización
- Servicio al cliente

Ahora debemos calcular la prioridad de recuperación de los procesos críticos, la misma que depende del máximo tiempo tolerable de estar abajo, MTD (Maximum Tolerable Downtime) por sus siglas en inglés.

3.1.2 Descripción y cálculo de los Tiempos de recuperación

MTD (Maximum Tolerable Downtime). Este tiempo representa el periodo máximo de tiempo de inactividad que puede tolerar una organización, sin entrar en un colapso financiero y operacional.

RTO (Recovery Time Objective). Indica el tiempo disponible para recuperar sistemas y/o recursos que han sufrido alteración. Comúnmente también se lo representa como el tiempo necesario para levantar los procesos a medias, quizás con actividades manuales.

RPO (Recovery Point Objetive). Se refiere a la magnitud de la pérdida de datos, medida en términos de un periodo de tiempo que un negocio de procesos puede tolerar.

WRT (Work recovery Time). Es el tiempo disponible para recuperar datos perdidos una vez que los sistemas están reparados, dentro del MTD. Comúnmente se lo representa como el tiempo después del RTO que se necesito para recuperar todas las funciones perdidas.

La suma de los tiempos RTO y WRT deben ser iguales o menores que el MTD. Jamás pueden ser mayores.

Continuando con nuestro BIA calculamos el MTD para los procesos críticos, preguntándonos ¿Cuál es el máximo tiempo que puede estar parado dicho proceso sin causar un colapso financiero u operacional a la compañía? y según el MTD calculamos la prioridad de recuperación.

Análisis de MTD y prioridad de recuperación

Procesos de negocio	MTD (días)	Prioridad de recuperación
Función de negocio: ADMINISTRATIVA		
Almacenamiento y Despacho	3	1d
Gestión de recursos Financieros	30	2
Pago de Nóminas	90	4
Facturación	60	3
Cobranzas	60	3
Legalizaciones	360	5
Gestión de proveedores de Internet	360	5
Función de negocio: TÉCNICA		
Monitoreo	3	1e
Instalaciones	360	5
Mantenimiento Preventivo	60	3
Mantenimiento Correctivo	3	1b
Administración de Red	3	1c
Soporte Técnico	30	2
Control de Cambios	360	5
Investigación/Desarrollo	360	5
Incidencias Seg. Lógica	360	5
Conexión	3	1a
Función de negocio: VENTAS		
Comercialización	360	5
Servicio al cliente	360	5

Cuadro 8. Cálculo de la prioridad de recuperación de los procesos críticos.

El último paso del BIA es el cálculo de los tiempos RTO, RPO y WRT de los procesos críticos, para ello es necesario conocer todos los recursos de IT (Sistemas) y de no IT (Herramientas, materiales, materia prima, etc.) que cada proceso necesita. Esta información nos servirá cuando se planten las estrategias de recuperación puesto que son valores con los cuales nos debemos dirigir.

Procesos de Negocio	RECURSOS IT	RECURSOS NO IT		TIEMPOS RECUPERACION		
ıción de negocio: ADMINISTRATI	SISTEMAS CRITICOS Y APLICACIONES	TIPO DE RECURSOS	DETALLE DE RECURSOS	RTO	WTR	RPO
Almacenamiento y Despacho	Sistema Mag, Sistema Email	Personal	Ayudante de embalaje	12 horas	12 horas	1días
Gestión recursos Financieros	Sistema NAF, Sistema Email	Monetario	Saldos y créditos Disponibles	4 horas	20 horas	5días
Pago de Nóminas	Sistema NAF	Materia Impresa	Chequera para pago	4 horas	20 horas	5días
Facturación	Sistema OG, Sistema Email, Sistema Telefónico	Materia Prima	Facturas	15 min	1hora	12horas
Cobranzas	Sistema OG, Sistema Email, Sistema Telefónico	Personal	Mensajeros, Asistentes de cobro	15 min	1hora	12horas
Legalizaciones	Sistema OG, Sistema Email	Personal	Mensajeros	15 min	1hora	12horas
Gestión de proveedores int	Sistema Whatsup, Sistema Email	Personal	Standby NOC, CTO	15 min	1hora	3horas
Función de negocio: TÉCNICA						
Monitoreo	Sistema Whats,up, ORION, Admin,Email, Telefónico	Equipos	PCs,Telefonos,Pantallas	15 min	1hora	1horas
Instalaciones	Sistema Email,Sistema OG, Sistema admin	Materia Prima/Personal	FO,Trasnceiver,Puertos Switch/Standby de instal	15 min	1hora	12horas
Mantenimiento Preventivo	Sistema Whatsup	Equipamiento/Materiales/Persona	OTDR, Fusionadora /FO/Standby de reparacione	15 min	1hora	1horas
Mantenimiento Correctivo	Sistema Whatsup	Equipamiento/Materiales/Persona	OTDR, Fusionadora /FO/Standby de reparaciones	15 min	1hora	1horas
Administración de Red	Sistema AAAA,Sistema OOB	Personal	Standby turno	15 min	1hora	1horas
Soporte Técnico	Sistema Whats,up, ORION, Admin,Email, Telefónico,Tacas	Personal	Standby turno	15 min	1hora	1horas
Control de Cambios	Sistema Whats,up, ORION, Admin,Email, Telefónico,Tacas	Personal	Standby turno	15 min	1hora	1horas
Investigación/Desarrollo	Sistema Whats,up, ORION, Admn,Email, Telefónico,Tacas	Personal	Standby turno	15 min	1hora	1horas
Incidencias Seg. Lógica	AAAA,email,Telefonico,	Personal	Standby turno	15 min	1hora	1horas
Conexión	Protocolos TCP/IP , I1-L7	Equipos/Materiales	Routers , Switch,Servidores,Radios/FO,Tarjetas,Ir	3 min	17,28 min	N/A
Función de negocio: VENTAS						
Comercialización	OG,email,Telefónico	Personal	Personal operativo	15 min	1hora	1horas
Servicio al cliente	OG,email,Telefónico	Personal	Personal operativo	15 min	1hora	1horas

Figura 6. Identificación de recurso y tiempos de recuperación de procesos (RTO, WTR, RPO) críticos.

3.1.2 Análisis y evaluación de riesgos de los procesos críticos.

Al igual que se lo hizo con los activos de información es necesario un análisis y evaluación de los riesgos para los procesos críticos. Para la metodología a presentar necesitamos identificar amenazas, severidad de amenazas y porcentaje de cobertura. La representación numérica del riesgo se la obtiene multiplicando el valor de la severidad de la amenaza (0, 10, 50,100) por el porcentaje de NO cobertura (100% - porcentaje de cobertura). Una vez que se calcula el valor del riesgo y lo priorizamos, sabremos en cual proceso debemos enfocar nuestros recursos para protegerlo o mejorar sus contramedidas.

Nuevamente es necesario implementar los controles adecuado, del Anexo A de la Norma ISO 27001, para aumentar el porcentaje de cobertura ante de las amenazas en los procesos críticos. A continuación se presenta una muestra de la metodología usada.

Cálculo de exposición al Riesgo de los procesos críticos													
Exposición al riesgo: Nivel de Severidad x (100% - %Cobertura) - {Max: 10000 Min: 0}			Severidad				Cobertura						Exposicion del riesgo
Proceso	**Potenciales Amenazas**		N/A	B(10)	M(50	A(100)	0-19%	20-39%	40-59%	60-79%	80-99%	100%	
Conexión	A. Cortes de Fibra				**50**						**85**		**750**
	B. Falla sist electrico interno					**100**					**90**		**1000**
	C. Corte de energia					**100**				**60**			**4000**
	D. Faño de hardware de red Cat 6500, 7200, ADM10Gb					**100**					**95**		**500**
	E. Interferencia de radio enlace				**50**						**90**		**500**
	~~F. Falla Humana~~												**0**
	G. Caidas de rayos				**50**						**95**		**250**
	H. Incencios					**100**		**30**					**7000**
	I. Inundaciones			**10**							**95**		**50**
	J. Deslaves					**100**					**85**		**1500**
	K. Ataques informaticos				**50**						**80**		**1000**
	L. Falla de software					**100**					**95**		**500**
	M. Sabotaje				**50**						**80**		**1000**
Servicio al cliente	A. Falta de movilizacion			**10**							**95**		**50**
	B. Falta de Personal			**10**							**95**		**50**
	C. Instalaciones Fallidas			**10**							**90**		**100**
	D. Falta de acceso al sistema (OG)				**50**						**95**		**250**
	E. Errores humanos				**50**						**95**		**250**
	F. Daño en los equipos de trabajo (PC)			**10**							**95**		**50**
	~~G. Dificultad para retiro de equipos~~												**0**
	H. Daño del sistema telefónico					**100**					**80**		**2000**
													0

Figura 7. Metodología para el análisis y evaluación del riesgo de los procesos.

3.2 Escenarios de amenazas.

Una vez que se implementan los controles, necesarios para minimizar los riesgos de los procesos críticos, el siguiente paso del BCP es redactar los posibles escenarios de amenazas que puede sufrir la organización.

Los escenarios de amenazas pueden tener diferentes niveles según los procesos que paralicen su materialización, a continuación una definición de un texto de referencia:

Amenaza nivel 1. Aquí se identifica una amenaza para la continuación de una o más funciones organizacionales en la empresa. Esta amenaza se debe a la pérdida de un recurso único pero crítico en una de las instalaciones de la organización (energía, sistemas de computación, archivos electrónicos, personal clave).

Amenaza nivel 2. En este escenario se identifica una amenaza para la continuidad de muchas funciones organizacionales, debido a un evento que impide el acceso a una de las instalaciones de la organización, pero no daña ningún recurso crítico.

Amenaza nivel 3. Una amenaza para la continuidad de varias funciones organizacionales, debido a un evento que daña o destruye un número de recursos críticos en una de las instalaciones de la organización. Este escenario es una combinación de los niveles 1 y 2.

Amenaza nivel 4. Una amenaza para la continuidad de varias funciones organizacionales en la empresa, debido a un evento que destruye totalmente una de las instalaciones de la organización y sus respectivos recursos críticos. Estos podrían ser imprevistos, tales como incendios o explosiones.

Amenaza nivel 5. Una amenaza para la continuidad de muchas funciones organizacionales e instalaciones múltiples, debido a pérdida de instalaciones críticas compartidas (energía, telecomunicaciones, sistemas centralizados). El evento causa daño y/o acceso restringido a más de una instalación en la organización (sismo o terremoto, huracán, incidente ambiental) Se puede generar pérdida del grupo gerencial (accidente aéreo, bomba, terrorismo biológico).

La redacción de los escenarios y sus consecuencias se lo hace en un taller multidisciplinario.

N	Escenario de Amenaza	NIVEL				
		1	2	3	4	5
1	Daño catalyst 6509 en NODO San Eduardo, afecta conexiones a switches de la red de Guayaquil routers tales como: GYE1 , GYE-LOJA, conexión de la primera Fibra enlace Guayaquil-Ibarra y otras provincias y SDH Guayaquil-Ibarra, Fibra Óptica entre Guayaquil-Manta			X		
2	Daño catalyst 6509 Nodo Pascuales, afecta conexiones a switches de red Guayaquil routerurales; La segunda fibra Óptica que da comunicación Guayaquil-Ibarra y varias provincias			x		
3	Daño catalyst 6509 en Quito Norte , afecta conexiones a switches de la red de Quito(conexión de la primera fibra que comunica Guayaquil-Ibarra y otras provincias y SDH Guayaquil-Ibarra,			x		
4	Daño catalyst 6500 en Aloag, afecta conexiones a switches de la metro de Aloag routers tales como: roxds3; la segunda Fibra óptica que da comunicación Guayaquil-Ibarra y varias provincias.			x		
5	Daño del equipo principal GYE1, perdemos Internet y Datos de las ciudades para tráfico MPLS están Guayaquil, Quevedo, Babahoyo, Cuenca; para tráfico IP están: Manta, salinas, Milagro, Salinas, Progreso, Montecristi.			x		
6	Daño del equipo principal UIO, perdemos Internet y Datos de las ciudades: Quito, Ibarra, Esmeraldas			x		
7	Cortes simultáneos de fibra Inter Urbano por sabotaje o caso fortuito			x		
8	Robo o sabotaje de un nodo	X				
9	Incendio de un nodo	X				

Cuadro 9. Escenarios de amenazas y niveles.

3.3 Estrategias de recuperación

La estrategia de recuperación es el plan de acción a seguir para recuperar los procesos críticos, en caso de la materialización de algún escenario de amenaza. Para ellos se debe tener identificado todos los recursos necesarios de IT y no IT que se necesitan.

La estrategia de recuperación debe cumplir con las factibilidades económicas de la compañía y también con los tiempos de recuperación previamente definidos (MTD, RTO, RPO, WRT).

N	Escenario de Amenaz	NIVEL 1	2	3	4	5	Controles	RESPONSABLE	Identificación: Requerimientos de recuperación	Opciones de Recuperación	Disponibilidad tiempo (RTO)	Costo Capacidad Recuperación	Estrategia de recuperacion
0	AMENAZA						Controles que minimizar el impacto y a minimizar el riesgo	Encargado de dar seguimiento a los entregables del BCP	Software, Hardware, Conexiones eléctricas, Datos, Hdráulicos, movilización, personal,	Plantear las posibles opciones de recuperación	Tiempo necesario para ejecutar la opción de recuperación	$ recursos	
1	Robo o sabotaje de un NODO	x					A.9.1.2 A.9.1.3 A.9.1.4 A.9.2.1	Gerencia Operaciones	2 Switch 3560 48Puertos, 60 Transceiver, 2UPS 1KVA, 2 ATS, 2 Tarjeta Monitoreo UPS, 60 Patch cord UTP , 20 patch cord FO SC, 4 Patch FO SC-LC, 4 SFP LX, 1 GPRS, Cable de puesta a tierra #2 Cu(30m), 5 fuentes Canopy, Cable RG8 30 m , 2 conectores BNC, 1 Red Lines, listado de clientes del Nodo (NOC), Diagrama NODOS (NOC- de donde viene y a donde va), Respaldo de configuración de switch (Proyectos), Listado de los radios (Radios), Inventario de Conexiones de FO (Fibra), Reestablecer Seguridad(Puertas, candados, chapas entre otros), 6 Personas FO, 1 otdr, 1 medidor de potencia, tubos de fusión (150-200 tubos), 4 Extensiones polarizadas de 30m, 1 caja de exteriores para equipos, 1 caja de exteriores para ups, 2 fusionadoras operativas, 1 Standby PROY ,NOC, 2 Electricos, 1 Operaciones, 2 Radios. De ser Necesario Generador,	1a) Tener parte de este material en la minibodega y lo restante en la bodega general. 1b) Tener todo el material en bodega central 1c) Tener todo el material en cada minibodega	1a) RTO=8 horas urbano (12 horas rural) WRT=4horas urbano. (4 horas rural) RTO (80 % de los clientes levantados)	1a) $17,575.60	PROC BCP Robo Nodo

Figura 8. Estrategia de recuperación para un escenario de amenaza.

Las estrategias de recuperación deben ser redactadas para cada uno de los escenarios de la amenaza.

3.4 Ensayos.

El principal fin de los ensayos del BCP es identificar falencias en la logística y la medición de los tiempos de recuperación, para así poder hacer los ajustes necesarios a la estrategia de recuperación. Uno de los objetivos de revisión del BCP, dentro de la ISO 27001:2005, es constatar la evidencia de su efectividad y cuando un escenario no se ha materializado, lo adecuado es presentar los informes de la ejecución de ensayos.

Simular completamente un escenario de amenaza suele ser disruptivo, en especial para un proveedor de servicios de telecomunicaciones, pero aún así se sebe tratar de realizar ensayos controlados, es decir segmentar el escenario de amenaza y simularlo por partes. La frecuencia de los ensayos está definida por cambios en el entorno, pero es recomendable simular todos los escenario de amenazas por lo menos una vez en el año.

4. Certificación ISO 27001:2005.

Una vez que se ha cumplido el ciclo PLAN-DO-CHECK-ACT del SGSI bajo todos los exigibles de la Norma ISO 27001:2005. Podemos optar por una certificación formal de nuestro sistema, para ello es necesario contratar los servicios de una empresa certificadora autorizada.

4.1 Proceso de certificación.

El proceso de certificación empieza con la elección de la empresa certificadora, en nuestro medio es posible contar con tres compañías: BSI, BVQI, SGS. A la empresa certificadora debemos entregarles información que les permita estimar la duración de las fases de certificación, como puede ser: el alcance número de empleados en el SGSI, cantidad de activos, ubicaciones geográficas, si ya cuenta con otro sistema de gestión (ej. ISO 9001).

Algunas organizaciones optan por contratar una pre-auditoria con el fin de diagnóstico, antes de contratar la auditoría formal.

La certificación del SGSI bajo la norma ISO 27001:2005 consta de dos fases:

FASE I: Aquí se verifica el cumplimiento documental del sistema y se puede detectar fallas medulares en la implementación. En esta fase el Auditor Externo debe emitir un informe favorable para continuar o no con la Auditoría de FASE II. Por lo general entre FASE I y FASE II no pude exceder más de 30 días, pero es el cliente quien propone las fechas exactas para llevar a cabo cada una de las FASES de la Auditoría.

FASE II: El objetivo de esta fase, es que la certificadora verifique objetivamente la implantación correcta del SGSI bajo todas las exigencias de la norma. El equipo de auditores mediante muestreo verificará el cumplimiento de todas o la mayoría de áreas dentro del alcance del SGSI.

Como auditado es necesario mantener a la mano todos los procedimientos, registros, formatos y acceso a sistemas que sirvan como evidencia del cumplimiento. El último día de la auditoría se lleva a cabo la reunión de cierre donde el Auditor Líder presenta el informe donde se especifica los hallazgos y se recomienda o no para la certificación.

Si el informe es favorable, la empresa certificadora debe enviarlo a la Empresa Acreditara quien es la que nos emite el certificado una vez que aprueba el informe. En nuestro medio las acreditadoras usadas por las certificadoras, son UKAS y ANAB.

4.2 Auditorías internas

Las auditorías internas es el proceso interno de revisión del SGSI en conformidad con la NORMA ISO 27001:2005.

La premisa de todas las auditorías, por consiguiente de todo auditor, es buscar conformidades más no no-conformidades. La ISO 27001:2005 exigen que la organización haya llevado a cabo auditorías internas y los resultados de las mismas sean revisados por la dirección. Por lo general las auditorías internas se las lleva a cabo antes de la auditoría externa y esta última se recomienda mínimo una vez al año. En nuestra implementación se las lleva a cabo cada semestre.

Mientras más exigente y formales sean las auditorías internas mayor valor agregarán a la preparación de la organización. Estas auditorías pueden ser

ejecutadas por personal interno de la compañía con formación como auditores internos o en su defecto puede ser llevado a cabo por personal externo como ejemplo una empresa consultora. Lo recomendación es que sea personal interno quien realice las auditoría de una forma cruzada entre los diferente áreas de la organización, o sea que nadie puede auditar su propia área.

Las organizaciones deben manejar programas de auditoría (cronograma general o anual), planes de auditorías (objetivos, horarios y secuencia de auditorías) y listas de chequeo (preguntas puntuales por área). Son herramientas que ayudan a las planificar, ejecutar y reportar las auditorías internas.

A continuación mostramos un formato de Plan de Auditoría usado en el Proveedor de servicio de Telecomunicaciones

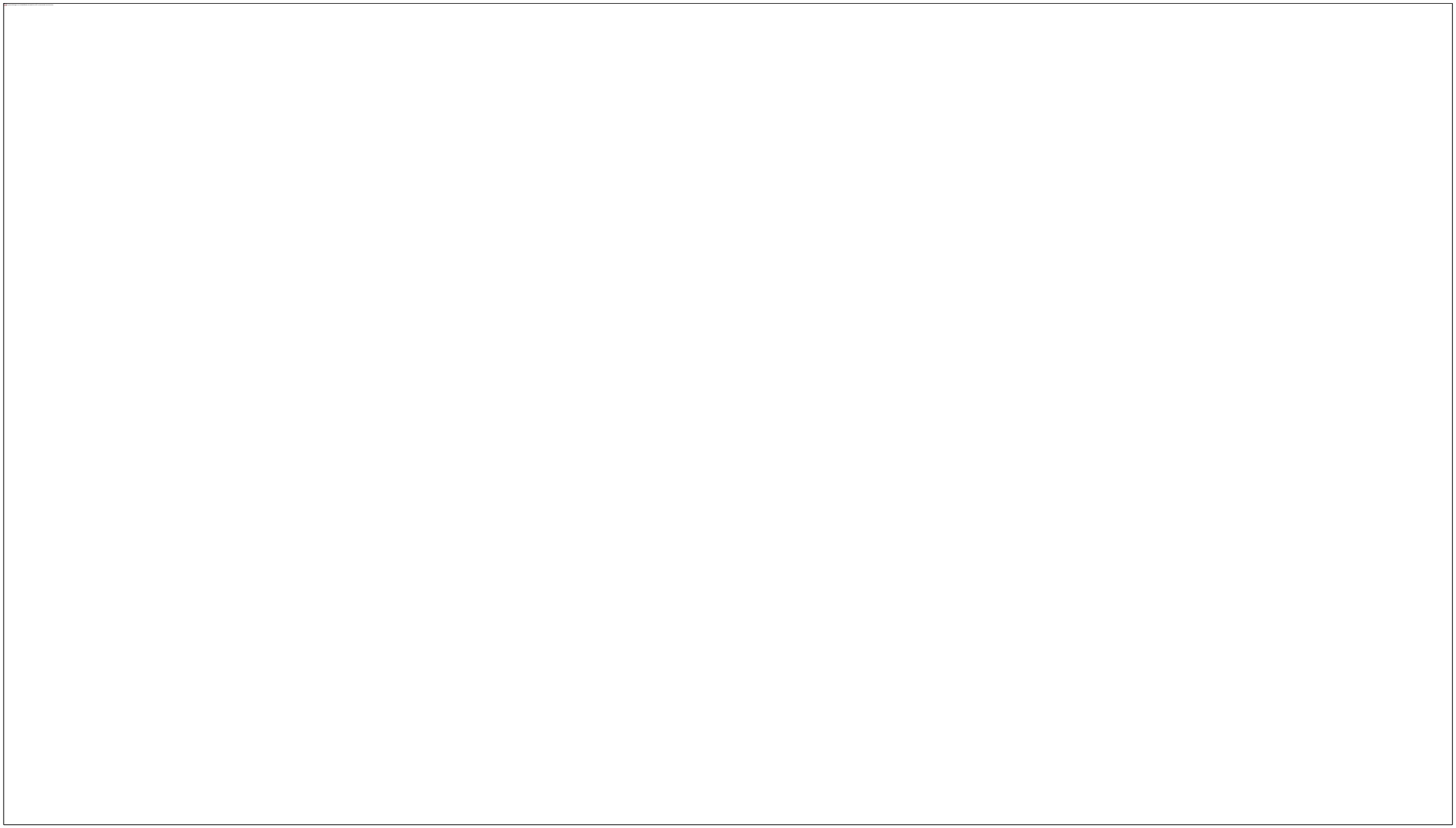


Figura 9. Plan de Auditoría Interna ISO 27001:2005.

Dentro del informe de auditoría se debe especificar las conformidades generales o fortalezas, no conformidades, observaciones y oportunidades de mejora. La definición de cada una de ellos es la siguiente:

Las ***no conformidades*** son aquellas oposiciones a la norma que se pueden redactar con el lenguaje natural de la misma. Es decir contrario a todos los DEBES textuales de la redacción.

Las ***observaciones*** son situaciones que a pesar de no ser no-conformidades pueden transformarse en ellas, sino se les da el tratamiento debido.

Las ***oportunidades de mejora*** son los puntos en que se puede sofisticar el sistema.

4.3 Auditorías de Terceras partes.

Las auditorías de terceras parte dentro de nuestro contexto se refieren a las auditorías externas que pueden ser llevadas a cabo por una entidad certificadora, empresa consultora, clientes . Cada uno con sus fines específicos.

Dependiendo del tamaño de la organización la auditoría externa puede ser llevada a cabo por un equipo de auditores dirigidos por un auditor líder.

Es responsabilidad de la empresa certificadora enviar el plan de auditoría especificando los horarios por área a ser auditada. Como empresa auditada debemos prever disponibilidad de un representante del área para ser auditado en el horario establecido, pero esto no impide que el auditor entreviste a cualquier miembro del departamento consultándole aspectos generales y fundamentales como son la política general, los objetivos del SGSI de la empresa o el procedimiento para reportar incidentes.

La auditoría externa inicia con una reunión de apertura con los directivos de la organización, aquí se validará el alcance de la auditoría y se expondrá cualquier inconveniente logístico de último momento. Al final de cada día es buena práctica, por el auditor, exponer los hallazgos para que la directiva de la organización esté consciente del avance de la auditoría.

Al final del último día el auditor líder expondrá el informe de auditoría donde se incluirán todos los hallazgos encontrados, conformidades o fortalezas a resaltar, no-conformidades mayores, no-conformidades menores, observaciones y

oportunidades de mejora. Dicho informe será enviado a la empresa certificadora y de ser favorable al organismo acreditador.

La organización debe evitar a toda costa las no-conformidades MAYORES, puesto que la presencia de una de ellas es un impedimento de recomendación de certificación. Se identifican como ***NO-CONFORMIDADES MAYORES***, cuando se presentan las siguientes situaciones:

- No cumplimiento de la norma ISO 27001:2005 que afecte el núcleo del SGSI en cualquier punto del ciclo PLAN-DO-CHECK-ACT. Es decir una situación que puede afectar las bases del SGSI y por ende todo su funcionamiento.
- La múltiple repetición de una misma no-conformidad menor en muchas áreas de la organización también produce una MAYOR.
- Un área de la organización con muchas no-conformidades menores también produce una no-conformidad MAYOR.

Desde el rol de auditor la premisa es que si se duda que una no-conformidad es mayor o menor entonces es menor.

Algunas no conformidades mayores son: la metodología errónea para el análisis y evaluación de riesgo, no haber hecho auditorías internas, no existir la revisión por la dirección.

5. Recursos necesarios

Esta norma está pensada para que cualquier empresa pueda implementarla independientemente al poder económico que ella posea.

En realidad, una mayor cantidad de recursos económicos, pueden ser diferenciadores en lo que respecta a la cantidad de tareas automatizadas que se pueden adoptar, por consiguiente la carga operativa en planear, implementar, monitorear y mejorar el SGSI es menor y más llevadero para toda la organización, a diferencia de procedimientos manuales y documentos impresos.

5.1 Puntos claves de Inversión.

Se recomienda que la organización enfoque la inversión en los siguientes puntos:

- Capacitación del personal clave: manager del proyecto, miembros del equipo de trabajo.
- Mecanismos de concientización de todo el personal.
- Formación de un equipo de auditores internos.
- Formación de Auditor Líder certificado ISO 27001:2005 por IRCA.
- Pre-auditoría de diagnóstico.
- Automatización y/o elaboración de herramientas de apoyen la medición de los controles, mejoramiento continuo.
- Crear un ambiente favorable en los talleres multidisciplinario.

5.2 Estimación de Costos del proceso.

En lo que respecta a costos de la certificación, estos varían de una organización a otra dependiendo del tamaño, ubicación geográfica, alcance del SGSI. A continuación presentaremos un desglose de los valores DIRECTOS invertidos en el proyecto para implantar el SGSI certificado ISO 27001:2005 en nuestro proveedor de servicios de telecomunicaciones en el mercado ecuatoriano.

Todo proceso duró aproximadamente un año y cuatro meses.

ITEM	VALOR
Contratación de pre-auditoría (5 días) a empresa Certificadora con Auditor Internacional	$8500
Curso de Auditor Líder ISO 27001:2005 certificado IRCA	$2500
Curso de Formación de auditores internos para 30 personas	$6200
Auditoría de FASE I por empresa Certificadora (3 días) con auditor internacional	$6000
Auditoría de FASE II por empresa Certificadora (3 días) con auditor internacional	$6000
Como valor indirecto , Tiempo aprox. Invertido 450 horas hombre	$5400
TOTAL	$34600

Cuadro 10. Costos del proyecto.

CONCLUSIONES Y RECOMENDACIONES.

1. La norma ISO 27001:2005 está orientada al tratamiento de la seguridad de la información mediante la gestión del riesgo, tanto para sus activos como para sus procesos. Esto garantiza que ante recursos limitados las inversiones sean bien focalizadas.

2. Hay decisiones respecto al cumplimiento de políticas dentro SGSI que deben ser de carácter jerárquico, impulsado por el director de la organización, siendo este el primer paso para adaptarse a todo cambio coyuntural dentro de la empresa.

3. Para poder tener una implantación exitosa del SGSI, los objetivos del mismo deben estar alineados al negocio de la compañía, caso contrario el valor que agrega no sería muy tangible.

4. La concientización de la compañía es un pilar fundamental de esta norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados. Existen mecanismos

como bonos, viajes, cenas o reconocimientos públicos que siempre despiertan interés.

5. Las organizaciones deben tratar de hacer lo más llevadero posible las tareas operativas del sistema SGSI, para lo cual necesitan la ayuda de herramientas tecnológicas que automaticen ciertas tareas.

6. Contar con personal clave dentro de la empresa y con las competencias exigidas por la Norma ISO 27001:2005 evitan la contratación de consultorías externas cuyo costo suele ser alto.

7. Un SGSI no puede ser implantado por moda sino siempre buscando objetivos claros que agreguen valor a la organización. Toda nueva implementación en pro de mejoras en la seguridad de la información debe ir acompañado de políticas funcionales que direccionen los esfuerzos hacia los objetivos del SGSI

8. El tener implantado un SGSI certificado bajo la norma ISO 27001:2005 no significar contar con seguridad máxima en la información de la organización sino que esto significa que la empresa cumple con los

requerimientos y mejores prácticas establecidas en dicha norma para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la sofisticación.

9. El eslabón más débil de la cadena son las personas, por lo tanto dentro del análisis y evaluación del riesgo del SGSI se debe dar el énfasis necesario para considerar este tipo de amenazas. Siempre aplicando en los perfiles el principio del mínimo conocimiento.

BIBLIOGRAFIA y REFERENCIAS.

1. International Standard Organization, Norma ISO/IEC FDIS 27001:2005(E).
2. Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad , Editorial Alfaomega, Colombia, 2007
3. British Standard Institute , Website www.bsi.com ,

ANEXO A

Carta de constancia de Certificación del SGSI bajo la norma ISO 27001:2007.

Guayaquil, 12 de Diciembre de 2008
EC/UIO 2008035

Señores:
TELCONET S.A.
Av. Luis Orrantia mz. 109 solar # 21 y Av. Victor Hugo Sicouret (Kennedy Norte)
Guayaquil

Atención:
Ing. Alfonso Aranda
Jefe Nacional de Seguridad Informatica

Referencia: Recomendación de Certificación ISO 27001:2005

Estimado Ing. Alfonso Aranda

Nos complace informar a ustedes que en cumplimiento con el proceso formal de auditoria de certificación del Sistema de Gestión de la Seguridad de la Información ISO 27001 de **TELCONET S.A.** efectuada los días 9, 10 y 11 de Diciembre del año en curso, el equipo auditor de SGS SSC decidió **RECOMENDAR LA CERTIFICACIÓN Y REGISTRO** de dicho sistema, conforme a los requisitos de la Norma ISO 27001:2005 y de acuerdo al alcance de certificación delineado en nuestro formato de solicitud de certificación.

Dicha recomendación se efectuó de acuerdo con los lineamientos establecidos por la **Entidad de Acreditación United Kingdom Accreditation Service UKAS** y a través de nuestra Oficina Acreditada **SGS Yarsley International Certification Services, Ltd.**

En relación directa con el procedimiento de certificación y registro observamos a ustedes que actualmente se está procesando el correspondiente certificado de auditoria a fin de cumplir con el proceso formal requerido para estos efectos.

Aprovechamos la presente para extender nuestras más sinceras felicitaciones por el logro alcanzado, en el conocimiento pleno de que este objetivo es tan sólo uno más en el camino de la excelencia que se ha marcado **TELCONET S.A.**

Atentamente.

Mauricio Rodriguez
Sector Manager
Systems & Services Certification
SGS Del Ecuador S.A