UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE CUENCA

FACULTAD DE INGENIERÍAS

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del

Título de: Ingeniero de Sistemas

TÍTULO

"DISEÑO DE UNA POLÍTICA DE SEGURIDAD PARA LA EMPRESA DE TELECOMUNICACIONES PUNTONET EN LA CIUDAD DE CUENCA, EN BASE A LAS NORMAS DE SEGURIDAD ISO 27001 Y 27011 COMO LÍNEAS BASE PARA LAS BUENAS PRÁCTICAS DE TRATAMIENTO Y SEGURIDAD DE LA INFORMACIÓN"

AUTORAS:

Jessica Maricela Avilés Armijos

María Elisa Uyaguari Guartatanga

DIRECTOR:

Ing. Byron Carrión Ramírez

Cuenca, Mayo 2012

AGRADECIMIENTO

Agradezco a Dios por haberme permitido llegar hasta dónde estoy por ser la principal guía en mi camino y haberme ayudado a superar y vencer todos mis obstáculos.

Quiero agradecer a mis padres Juan e Irene quienes permanentemente me han sabido apoyar para que continúe y han sido mi ejemplo y fuente de inspiración para luchar por lo que quiero.

A mi hermana y confidente Fernanda por su amor incondicional y por estar ahí en las buenas y en las malas a mi hermano Juan Carlos que siempre me saca una sonrisa y me da aliento y a ese ángel que llego a dar luz a mi vida Camila mi sobrina.

Un agradecimiento especial a mi amiga y compañera de tesis Elisa porque ha sabido comprenderme y apoyarme durante este trabajo.

A mis amigos y compañeros de la universidad Karina, Remigio, Javier, Paúl , José, Vero por su amistad incondicional, por estar siempre ahí y hacer mejores y más alegres mis días de estudiante.

Al Ing. Patricio León Jefe Técnico de la empresa Puntonet por habernos contribuido con su ayuda para la elaboración de esta tesis.

Y un sincero agradecimiento a nuestro director de tesis Ing. Byron Carrión quien nos ha brindado su ayuda y guía para la realización del presente trabajo.

DEDICATORIA

Dedico este esfuerzo y trabajo a Dios por su infinito amor hacia a mí y haberme acompañado todo este tiempo en mi camino.

A mi papá por su apoyo por su ejemplo de perseverancia y de lucha por lo que uno quiera.

A mi mamá por ser esa luz en mi vida que con su amor, enseñanzas y consejos ha sabido hacer de mí la persona que soy.

"La gran victoria que hoy parece fácil fue el resultado de pequeñas victorias que pasaron desapercibidas." -Paulo Coehlo-

Jessica Maricela Avilés Armijos

AGRADECIMIENTO

La realización de este proyecto agradezco primeramente a Dios por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño tan anhelado, por estar conmigo en cada momento.

A mi padre Julio por ser quien a estado en cada momento apoyandome desde mi infancia, ayudando en mis estudios y enseñandome a luchar cada día por ser alguien mejor.

A mi madre Lucia el pilar fundamental que me ha brindado apoyo incondicional y consejos cuando los he requerido, a ella le dedico todo el esfuerzo dado para lograr lo que hoy soy.

A mis hermanos Andrés, Francisco, Paulette por estar en momentos difíciles, alegrandome de alguna manera y animándome para continuar.

A ti Juan, que desde un principio hasta el día hoy sigues dándome ánimo para terminar este proceso.

A mis amigos Jessica, Vero, Kari, Remigio, Javier, Paúl, José con los que he compartido momentos agradables durante esta etapa.

A la Universidad Politécnica Salesiana por darme la oportunidad de estudiar y obtener nuevos conocimientos.

A nuestro director de tesis, Ing. Byron Carrión por la guía brindada, quien con sus conocimientos, su experiencia, y su motivación ha logrado que pueda terminar con éxito este proyecto.

Son muchas las personas que han formado parte de mi vida a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida.

DEDICATORIA

La realización de este proyecto está dedicada a Dios porque ha estado conmigo guiándome en cada momento, dándome la fortaleza para continuar hasta llegar a la finalización de este proyecto.

A mis padres, pilares fundamentales en mi vida, quienes han sido un ejemplo a seguir y han depositado toda su confianza en cada reto que se me ha presentado. A mis familiares y amigos por el apoyo.

María Elisa Uyaguari
Guartatanga

CERTIFICACIÓN

Certifico haber dirigido y revisado el proyecto de Tesis "DISEÑO DE UNA POLÍTICA DE SEGURIDAD PARA LA EMPRESA DE TELECOMUNICACIONES PUNTONET EN LA CIUDAD DE CUENCA, EN BASE A LAS NORMAS DE SEGURIDAD ISO 27001 Y 27011 COMO LÍNEAS BASE PARA LAS BUENAS PRÁCTICAS DE TRATAMIENTO Y SEGURIDAD DE LA INFORMACIÓN", realizado por las señoritas Jessica Maricela Avilés Armijos y María Elisa Uyaguari Guartatanga.....

Cuenca, 27 de mayo de 2012

DECLARACIÓN DE RESPONSABILIDAD

Los conceptos desarrollados, análisis realizados y conclusiones expuestas en el presente trabajo, son de exclusiva responsabilidad de las autoras. Y autorizo a la Universidad Politécnica Salesiana usar la misma con fines académicos.

Jéssica Avilés

Elisa Uyaguari

RESUMEN

Un adecuado diseño de políticas de seguridad debe estar basado en normas internacionales para que puedan ser sustentables, en este proyecto se ha tomado en cuenta las normas ISO 27001 y 27011 la primera que trata de controles enfocados a una correcta gestión de la información y la segunda que establece controles orientados a las empresas de telecomunicaciones.

Es necesario establecer una metodología que defina las etapas que permitan llevar a cabo un correcto análisis y gestión de riesgos utilizando las ISO mencionadas, para el desarrollo del proyecto se tomó como guías la metodología MAGERIT y se hizo uso de su software PILAR debido a que el análisis estará fundamentado y se hará un aproximación metódica a la situación real.

Para realizar un diseño de las políticas de seguridad es imprescindible definir los activos y el valor que tienen para la empresa y posteriormente desarrollar una serie de tareas que ayuden a determinar que amenazas pueden afectar estos activos, de esta forma identificar las salvaguardas que son aplicables según el grado de impacto y riesgo con el fin de mitigar toda clase de amenazas que pudieran poner en peligro la función del negocio.

Con los datos obtenidos del análisis de riesgos se continúa con la etapa de gestión de riesgos dónde se considera el diseño de nuevas políticas de seguridad en base a los requerimientos generados mediante este estudio, con el principal objetivo de disminuir el riesgo y mantener las dimensiones de seguridad tomando en cuenta las recomendaciones de las normas ISO definidas anteriormente.

ÍNDICE GENERAL

1 ESTÁNDAR ISO 27001 1
- 1.1 POLITICAS DE SEGURIDAD 1
  - 1.1.1 Documento de Política de Seguridad de la Información 2
  - 1.1.2 Revisión de la Política de Seguridad de la Información 2
- 1.2 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN 2
  - 1.2.1 Organización Interna 2
  - 1.2.2 Organización Externa 4
  - 1.2.3 Abordaje de la Seguridad en los Acuerdos con Terceras Partes 6
- 1.3 ADMINISTRACIÓN DE RECURSOS 6
  - 1.3.1 Responsabilidad sobre los Activos 6
  - 1.3.2 Clasificación de la Información 7
- 1.4 SEGURIDAD DE LOS RECURSOS HUMANOS 7
  - 1.4.1 Antes de la Contratación Laboral 7
- 1.5 SEGURIDAD FISICA Y DEL ENTORNO 10
  - 1.5.1 Áreas Seguras 10
  - 1.5.2 Seguridad de los Equipos 11
- 1.6 ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES 12
  - 1.6.1 Procedimientos Operacionales y Responsabilidades 12
  - 1.6.2 Gestión de la Prestación del Servicio por Terceras Partes 12
  - 1.6.3 Planificación y Aceptación del Sistema 12
  - 1.6.4 Protección contra Códigos Maliciosos y Móviles. 12
  - 1.6.5 Respaldo 13
  - 1.6.6 Gestión de la Seguridad de Redes 13
  - 1.6.7 Manejo de los Medios 13
  - 1.6.8 Intercambio de la Información 13
  - 1.6.9 Servicios de Comercio Electrónico 13
  - 1.6.10 Monitoreo 13
- 1.7 CONTROL DE ACCESOS 13
  - 1.7.1 Requisitos de Negocio para el Control de Accesos. 14
  - 1.7.2 Gestión de Acceso de Usuario. 14
  - 1.7.3 Responsabilidades del Usuario. 14
  - 1.7.4 Control de Acceso en Red. 15
  - 1.7.5 Control de Acceso al Sistema Operativo. 16
  - 1.7.6 Control de Acceso a las Aplicaciones. 18
  - 1.7.7 Informática Móvil y Tele Trabajo. 18
- 1.8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN. 19
  - 1.8.1 Requisitos de Seguridad de los Sistemas de Información 19
  - 1.8.2 Procesamiento Correcto en las Aplicaciones 19
  - 1.8.3 Controles Criptográficos 19

1.8.4 Seguridad de los Archivos del Sistema 20
1.8.5 Seguridad en los Procesos de Desarrollo y Soporte 21
1.9 ADMINISTRACIÓN DE LOS INCIDENTES DE SEGURIDAD 21
1.9.1 Comunicación de Eventos y Debilidades en la Seguridad de la Información. 22
1.9.2 Gestión de Incidentes y Mejoras en la Seguridad de la Información. 22
1.10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 23
1.10.1 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio 23
1.10.2 Inclusión de la Seguridad de la Información en el Proceso de Gestión de la Continuidad del Negocio 23
1.11 CUMPLIMIENTO (LEGALES,DE ESTÁNDARES,TÉCNICAS Y AUDITORÍAS) 24
1.11.1 Conformidad con los Requisitos Legales. 24
1.11.2 Revisiones de la Política de Seguridad y de la Conformidad Técnica. 25
1.11.3 Consideraciones Sobre la Auditoria de Sistemas. 25
2 ESTÁNDAR ISO 27011 27
2.1 ARQUITECTURA DE SEGURIDAD PARA INTERCONEXION DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT 27
2.1.1 Alcance y Campo de Aplicación 27
2.1.2 Ubicación de los Servicios y Mecanismos de Seguridad 28
2.2 ARQUITECTURA DE SEGURIDAD PARA SISTEMAS DE EXTREMO A EXTREMO DE LAS COMUNICACIONES 34
2.2.1 Dimensiones de Seguridad 34
2.2.2 Capas de Seguridad 35
2.2.3 Planes de Seguridad 35
2.3 SISTEMAS DE GESTIÓN DE CALIDAD 36
2.3.1 Requisitos de un Sistema de Gestión de Calidad 36
2.3.2 Compromiso con la Calidad 37
2.3.3 Enfoque al Cliente 37
2.3.4 Política de la Calidad 38
2.4 SISTEMAS DE GESTIÓN AMBIENTAL 38
2.4.1 Política Ambiental 38
2.4.2 Planificación 39
2.5 TECNOLOGÍA DE LA INFORMACIÓN 39
2.6 GESTIÓN DE RIESGOS 40
2.6.1 La Interpretación de los Valores de Impacto y Riesgo Residuales 40
2.6.2 Selección de Salvaguardas 41
2.6.3 Pérdidas y Ganancias 42
2.6.4 La Actitud de la Dirección 42
2.6.5 Revisión del Paso 1: Activos 43
2.7 SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACIÓN 43
2.7.1 Utilidad de un SGSI 43

2.7.2 Implementación de un SGSI 43
2.7.3 Do: Implementar y Utilizar el SGSI 44
2.7.4 Check: Monitorizar y Revisar el SGSI 44
2.7.5 Act: Mantener y Mejorar el SGSI 45
3 SITUACIÓN ACTÚAL DE LA EMPRESA 47
3.1 DELIMITACIÓN DEL ALCANCE 47
3.1.1 Misión 47
3.1.2 Visión 47
3.1.3 Características del Negocio 47
3.1.4 Servicios que Ofrece 47
3.1.5 Diagrama Organizacional 50
3.1.6 Grado de Penetración Nacional 50
3.1.7 Ubicación y Area de Cobertura 50
3.1.8 Procesos 50
3.1.9 Activos 53
3.2 DECLARACIÓN DE APLICABILIDAD 59
3.3 POLÍTICAS Y PROCEDIMIENTOS 61
3.4 PLAN DIRECTOR DE SEGURIDAD 61
3.5 PLAN DE CONTINUIDAD DE NEGOCIO 61
3.6 PLAN DE FORMACIÓN 61
3.7 GESTIÓN DE INCIDENTES 62
3.8 AUDITORIA INTERNA 62
4 ANÁLISIS DE RIESGOS 63
4.1 IDENTIFICACIÓN DE PROCESOS REALIZADOS EN LA ORGANIZACIÓN 63
4.2 ESTUDIO DE LAS ACTIVIDADES QUE SE REALIZA PARA CADA UNO DE LOS PROCESOS 65
4.3 ANÁLISIS DE RIESGOS 72
4.3.1 Caracterización de los Activos 72
4.3.2 Caracterización de las Amenazas 78
4.3.3 Caracterización de las Salvaguardas 80
4.3.4 Estimación del Estado de Riesgo 91
4.4 EVALUACIÓN DEL RIESGO 94
4.5 ANÁLISIS DEL IMPACTO Y EL FACTOR DE RIESGO 98
4.6 EFECTOS DEL IMPACTO 99
4.7 GESTIÓN DE RIESGOS 100
5 DESARROLLO DE LA POLÍTICA DE SEGURIDAD 101
5.1 PLANIFICACION DE LA POLITICA 101
5.2 CREACION DE LA POLITICA 101
5.2.1 Políticas Eegún el Estándar ISO 27001 101
5.2.2 Políticas Según el Estándar ISO 27011 113
5.3 REVISION DE LA POLITICA 120
5.4 APROBACION DE LA POLITICA 121
5.5 DESARROLLO DEL SGSI 121
6 CONCLUSIONES Y RECOMENDACIONES 123

BIBLIOGRAPHY 125
7 ANEXOS 127
7.1 ANEXO A: CATÁLOGO DE IDENTIFICACIÓN DE ACTIVOS 127
7.2 ANEXO B: CRITERIOS DE VALORACIÓN ADICIONALES 128
7.3 ANEXO C: CATÁLOGO DE AMENAZAS 132

7.4 ANEXO 1: METODOLOGÍA DE ANÁLISIS DE RIESGOS 136
7.5 ANEXO 2: VALORACIÓN DE LOS ACTIVOS 140
7.6 ANEXO 3: SOLICITUD LICENCIA PILAR 141

ÍNDICE DE FIGURAS

Figura 1 Pérdicas y Ganancias 42
Figura 2 Diagrama Organizacional Fuente: PUNTONET 51
Figura 3 Ubicación y Area de Cobertura Fuente: PUNTONET 52
Figura 4 Sistema Netplus - Departamento Técnico Fuente: PUNTONET 56
Figura 5 Sistema Netplus - Requerimientos Fuente: PUNTONET 56
Figura 6 Sistema Syscorp Fuente: PUNTONET 57
Figura 7 Software de Monitoreo Cacti Fuente: PUNTONET 57
Figura 8 Actividades para el proceso Registro de Clientes 66
Figura 9 Actividades para el proceso de Post Venta Fuente: Puntonet 66
Figura 10 Actividades para el proceso de Facturación Fuente: Puntonet 67
Figura 11 Actividades para el proceso de Atención al Cliente Fuente: Puntonet 67
Figura 12 Actividades para el proceso de Comercialización Fuente: Puntonet 68
Figura 13 Actividades para el proceso de Instalación Fuente: Puntonet 68
Figura 14 Actividades para el proceso de Monitoreo Fuente: Puntonet 69
Figura 15 Actividades para el proceso de Mantenimiento Fuente: Puntonet 70
Figura 16 Actividades para el proceso de Administracion de Red Fuente: Puntonet 70
Figura 17 Actividades para el proceso de Soporte Técnico Fuente: Puntonet 71
Figura 18 Tarea Identificación de Activos Fuente:PILAR 74
Figura 19 Tarea Dependencia entre activos Fuente: PILAR 76
Figura 20 Tarea Valoración de Activos Fuente: PILAR 78
Figura 21 Tarea Identificación de las Amenazas Fuente: PILAR 79
Figura 22 Tarea Valoración de las Amenazas Fuente: PILAR 80
Figura 23 Tarea Identificación de Salvaguardas. Fuente PILAR 85
Figura 24 Tarea Valoración de las Salvaguardas. Fuente PILAR 87
Figura 25 Niveles de Criticidad Fuente: MAGERIT 91
Figura 26 Impacto Residual 92
Figura 27 Riesgo Residual 92
Figura 28 Frecuencia Residual 92
Figura 29 Impacto Acumulado 93
Figura 30 Impacto Repercutido 93

Figura 31 Riesgo Residual Repercutido. Fuente: PILAR 96
Figura 32 Riesgo Residual Acumulado. Fuente: PILAR 97
Figura 33 Impacto Residual Repercutido. Fuente: PILAR 98
Figura 34 Impacto Residual Acumulado. Fuente: PILAR 99
Figura 35 Efectos del impacto. Fuente: PILAR 100
Figura 36 Matriz de políticas. Fuente: Autoras 102
Figure 37 Proceso del Análisis de Riesgos 137
Figure 38 Solicitud licencia PILAR 142

ÍNDICE DE CUADROS

Cuadro 1 Función del negocio: Administrativo Fuente: PUNTONET 52
Cuadro 2 Función del negocio: Ventas Fuente: PUNTONET 53
Cuadro 3 Función del negocio: Técnico Fuente: PUNTONET 53
Cuadro 4 Principales activos Fuente: PUNTONET 54
Cuadro 5 Criterios de valoración de activos Fuente: MAGERIT 59
Cuadro 6 Valoración de los Activos Fuente: PUNTONET 60
Cuadro 7 Identificación de los activos en las diferentes subcapas Fuente: LAS AUTORAS 73
Cuadro 8 Identificación de Dependencia entre activos Fuente: Puntonet 75
Cuadro 9 Escala de criterios de valoración Fuente: MAGERIT 75
Cuadro 10 Criterios de valoración adicionales Fuente: MAGERIT 77
Cuadro 11 Estimación de la frecuencia Fuente: MAGERIT 79
Cuadro 12 Estimación de la degradación Fuente: MAGERIT 79
Cuadro 13 Niveles de madurez de las salvaguardas. Fuente: MAGERIT 86
Table 14 Criterios de valoración de activos Fuente: MAGERIT 140

Cuenca, 26 de mayo de 2012

A petición verbal de la parte interesada, Ing. Patricio León, JEFE TECNICO DE LA EMPRESA PUNTONET-CUENCA,

CERTIFICA

Que, la tesis realizada en nuestras instalaciones por las Señoritas Jéssica Maricela Avilés Armijos con CI. 010442764-6 y María Elisa Uyaguari Guartatanga con CI. 010451582-0, cumple con los objetivos planteados para llevar a cabo el tema titulado "DISEÑO DE UNA POLITICA DE SEGURIDAD PARA LA EMPRESA DE TELECOMUNICACIONES PUNTONET EN LA CIUDAD DE CUENCA, EN BASE A LAS NORMAS DE SEGURIDAD ISO 27001 Y 27011 COMO LINEAS BASE PARA LAS BUENAS PRACTICAS DE TRATAMIENTO Y SEGURIDAD DE LA INFORMACION", el que mismo fue desarrollado en la empresa Puntonet y cuenta con todo nuestro respaldo y aprobación.

Es todo cuanto se puede certificar en honor a la verdad y se autoriza a las interesadas hacer uso del presente documento como lo creyeren conveniente.

Atentamente

Ing. Patricio León

Jefe Técnico

Puntonet-Cuenca

1 ESTÁNDAR ISO 27001

La información es parte esencial de las actividades diarias de una organización, para gestionarla y protegerla en todo momento es necesario disponer de un grupo de reglas o políticas especificadas en la ISO/IEC 27001.

ISO/IEC 27001 define los requisitos para "Sistemas de Gestión de la Seguridad de la Información (SGSI)", ya que permite la selección de controles acorde a las necesidades de seguridad de la organización. Esta norma presenta una guía por procesos para establecer, implantar, operar, revisar, mantener y mejorar un SGSI, con el objetivo de brindar protección a información sensible y en algunos casos crítica, siendo esta relativa a finanzas, tecnología de la información, datos de clientes, etc.

1.1 POLITICAS DE SEGURIDAD

La información es el recurso más importante de cualquier compañía, por lo tanto debe estar protegido mediante la creación de varias políticas de seguridad para proveer los elementos claves de seguridad ya mencionados: Integridad, Disponibilidad, Confidencialidad, Autenticidad y Trazabilidad, para:

- Garantizar la confidencialidad de los datos gestionados en los diferentes procesos de la empresa.
- Garantizar la disponibilidad de servicios ofrecidos a clientes, de igual manera a los servicios y procesos internos de la empresa.
- Garantizar el funcionamiento de servicios en lapsos de tiempo cortos, tras ocurrir situaciones de emergencia.
- Prevenir que la información sea modificada sin ninguna autorización.
- Concientizar y brindar formación permanente sobre seguridad de la información.

Una política de seguridad está formada de normas, reglamentos y protocolos a seguir de acuerdo con los objetivos, requisitos del negocio y leyes previamente establecidas, donde se definen las medidas a tomar para proteger a la información de amenazas, permitiendo así la continuidad del negocio, de igual manera minimizar los efectos de posibles daños y maximizar el rendimiento de las herramientas empleadas para proteger la información.

La Política de Seguridad tiene dos propósitos centrales: Informar a todos los usuarios sobre las obligaciones que deben asumir respecto a la seguridad asociada a los recursos de tecnología de Información y dar las guías para actuar ante posibles amenazas y problemas presentados. [1]

1 CEVALLOS, P. (2007). *Políticas de Seguridad. Obtenido el 11 de octubre de 2011, de http://www.repositorio.utn.edu.ec*

1.1.1 *Documento de Política de Seguridad de la Información*

El personal asignado por parte de la organización, es el encargado de comunicar a los empleados sobre la política que ha sido creada. Ellos son quienes deben aprobar y posteriormente publicar el documento de la política de seguridad de la información.

Dentro del documento se debe especificar lo siguiente:

- Objetivos de la organización, el alcance y una descripción de la seguridad de la información.
- Valoración y manejo de los riesgos existentes así como detallar los objetivos de los controles.
- Una descripción de las políticas y normas de conformidad más importantes para la organización.

1.1.2 *Revisión de la Política de Seguridad de la Información*

En la revisión de la política de seguridad de la información es necesario indicar los cambios más significativos que repercuten a la primera evaluación de los riesgos presentes en activos de la organización, así como cambios de gran importancia en otros aspectos. Esta revisión se debe realizar con cierta frecuencia o en tiempos planificados.

1.2 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Mediante este control se identifican los puntos para realizar una gestión de la información en la organización.

El objetivo de este dominio es el de implementación de las guias para administrar y mantener la seguridad de la información, así como las normativas y polìticas de seguridad que deben ser aplicados al personal ya sean estos interno y externo, que se vea involucrado directa o indirectamente con la información.

1.2.1 *Organización Interna*

Lo primero que se debe hacer es realizar una estructura de cómo se va a iniciar y controlar la implementación de políticas de seguridad dentro de la organización, se debería aprobar la política de seguridad, así como asignar al personal que va a ser el responsable de manejar la seguridad.

Compromiso de la Dirección con la Seguridad de la Información.

Es muy importante que la dirección apoye activamente la seguridad dentro de la organización. Las responsabilidades se podrían manejar a través de un comité de dirección, deberían ser coordinadas por los representantes de todas las áreas de la organización.

Asignación de Responsabilidades para la Seguridad de la Información

Se deben definir claramente las responsabilidades para la protección de activos. Las personas con responsabilidades de seguridad son las

encargadas de verificar la correcta ejecución de las tareas asignadas.

Proceso de Autorización para los Servicios de Procesamiento de Información

Según la norma ISO 27001[2], se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

- Los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado.
- Cuando sea necesario, tanto hardware como software deberían ser verificados para asegurar que son compatibles con otros componentes del sistema
- Se deberían identificar e implementar controles necesarios contra posibles vulnerabilidades introducidas por equipos personales.

Acuerdos sobre Confidencialidad

Según la norma[3] deberían considerar los siguientes elementos para establecer los requisitos:

- Definir la información que se ha de proteger
- Tiempo de duración esperada del acuerdo
- Acciones requeridas cuando se termina un acuerdo
- Responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información
- Propiedad de la información, secretos comerciales y propiedad intelectual
- Derecho de auditar y monitorear las actividades que involucran a la información confidencial
- Proceso para el reporte de divulgación no autorizada o violación de la información confidencial.
- Términos para la devolución o la destrucción de la información al terminar el acuerdo.
- Acciones esperadas a tomar en caso de incumplimiento de este acuerdo

2 POSSO, R.(2009). Desarrollo de políticas de seguridad informática e implementación de tres dominios en base a la norma 27002 para el área de hardware en la empresa Uniplex S.A en Quito. Obtenido el 04 de octubre de 2011.

3 POSSO, R.(2009). Desarrollo de políticas de seguridad informática e implementación de tres dominios en base a la norma 27002 para el área de hardware en la empresa Uniplex S.A en Quito. Obtenido el 04 de octubre de 2011

Contacto con las Autoridades

La empresas debería contar con los procedimientos que especifiquen cuándo, cómo y a través de qué autoridades se debería contactar para reportar de forma oportuna los incidentes identificados de la Seguridad de la Información, o la sospecha de incumplimiento de la ley. Esto también implica relación con organismos de regulación.

Contactos con Grupos de Intereses Especiales

De igual forma la norma 27011 establece que la pertenencia a foros o grupos de intereses especiales se debería considerar un medio para :

- Renovar el conocimiento sobre la información referente a la seguridad.
- Garantizar que la comprensión del entorno de Seguridad de la Información es actual y completa.
- Recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.
- Obtener acceso a asesoría especializada sobre Seguridad de la Información.
- Compartir información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Suministrar puntos adecuados de enlace cuando se trata de incidentes de Seguridad de la Información.

Revisión Independiente de la Seguridad de la Información

Esta revisión debe ser hecha por una persona que no pertenezaca al área que esta siendo sometida a revisión; así se puede conseguir eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la Seguridad de la Información.

1.2.2 *Organización Externa*

Las normas de seguridad de la información no solo deben aplicarse para el personal interno, sino que también debe involucrar al personal externo a la empresa o a un tercero de la organización, que esté implicado por medio de un contrato, alianza o convenio, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información de la Organización.

Identificación de los Riesgos Relacionados con las Partes Externas

Cuando es necesario conceder la autorización para el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, se debería llevar a cabo una evaluación de riesgos, así se pueden identificar los controles necesarios. Según la ISO[3] se debería considerar:

- Los servicios de procesamiento de información a los cuales requiere acceso la parte externa.

- El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información (físico, lógico o conexión de red).
- El valor y la sensibilidad de la información involucrada.
- Los controles necesarios para que información no autorizada no esté disponible para la parte externa.
- La forma en que se puede identificar al personal autorizado a tener acceso, la manera de verificar la autorización, y la forma de confirmar esta verificación.
- Los medios y controles utilizados por la parte externa para almacenar, procesar, comunicar, compartir e intercambiar la información.
- El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a información engañosa.
- Los procedimientos para tratar los incidentes de Seguridad de la Información, los daños potenciales y las condiciones para la continuación del acceso de la parte externa.
- Los requisitos legales y otras obligaciones contractuales pertinentes a la parte externa que se debería tener en cuenta.

Abordaje de la Seguridad cuando se Trata con los clientes

Segùn el estándar los siguientes términos se deberían considerar para abordar la seguridad antes de dar acceso a los clientes a cualquiera de los activos de la organización:

- Protección de activos.
- Descripción del producto o servicio que se va a proveer.
- Las diversas razones, requisitos y beneficios del acceso del cliente.
- Política del control de acceso (uso de identificadores, contraseñas, privilegios, o revocar derechos).
- Convenios para el reporte, la notificación y la investigación de las inexactitudes de la información (por ejemplo de detalles personales), incidentes y violaciones de la seguridad de información.
- Descripción de cada servicio que va a estar disponible.
- El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.
- Las respectivas responsabilidades civiles de la organización y del cliente.
- Derechos de propiedad intelectual y asignación de derechos de copia y la protección de cualquier trabajo en colaboración.

1.2.3 *Abordaje de la Seguridad en los Acuerdos con Terceras Partes*

Se debería también garantizar que no existen malos entendidos entre la organización y la tercera parte. Según recomiendaciones de la ISO 27001 se debe tener en cuenta los siguientes puntos:

- La política de Seguridad de la Información y los controles para asegurar la protección del activo.
- Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información.
- Responsabilidades relacionadas con la instalación y el mantenimiento del software y el hardware.
- La estructura clara y los formatos acordados para la presentación de los informes.
- La política de control del acceso.
- Disposiciones para la notificación y la investigación de incidentes, incumplimientos y violaciones de los requisitos establecidos en el acuerdo.
- La descripción de cada servicio que va a estar disponible y los objetivos del servicio.
- El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización.
- El derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorías sean realizadas por una tercera parte y a enumerar los derechos estatutarios de los auditores.
- El establecimiento de un proceso de escalada para la solución de problemas.

1.3 ADMINISTRACIÓN DE RECURSOS

Este dominio indica que tan importante es llevar un inventario de activos, controlar que su uso sea el adecuado y clasificarlos, además de asignar responsabilidades al personal que labora en la organización, que es el encargado del tratamiento de la información. Logrando así proveer de adecuadas medidas de seguridad para proteger a los activos de una manera efectiva. Es necesario inventariar todos los activos ya que de lo contrario se puede considerar como una brecha de seguridad del sistema que maneja la organización.

1.3.1 *Responsabilidad sobre los Activos*

A cada activo se le asigna un responsable para que le brinde protección y mantenimiento adecuado a los controles.

Inventario de Activos

Se debe identificar los principales activos de la organización, así como el responsable o propietario, su importancia, valor, ubicación, y por último los niveles de protección que se desee proporcionar al activo.

Una vez realizado algún cambio o modificación en lo mencionado, se debe registrar y actualizar esa información en el inventario.

Propiedad de los Recursos

Todos los activos que maneja la organización deben ser propiedad del personal desigando, para asegurar que los activos sean correctamente clasificados bajo las restricciones de clasificación y acceso, teniendo en consideración las políticas de control de acceso.

Uso aceptable de los Activos

Es necesario identificar reglas sobre el uso aceptable de los recursos del tratamiento de la información y activos para luego ser documentados e implementados.

1.3.2 *Clasificación de la Información*

No toda la información tiene el mismo valor, ni grado de sensibilidad, algunos recursos tal vez podrían necesitar de grados adicionales de protección, por ello es necesario clasificarla en base a niveles apropiados de protección para garantizar la confidencialidad, integridad y disponibilidad de la información en todo momento.

Guías de Clasificación

Las guías de clasificación orientan en el proceso de clasificación de la información de acuerdo a su valor, sensibilidad, criticidad con el objetivo de protegerla y manejarla adecuadamente. Estás guías tras un cierto tiempo pueden dejar de tener la misma importancia o criticidad.

Etiquetado y Tratamiento de la Información

La organización se encarga de definir el procedimiento del etiquetado (puede ser físico o lógico) y tratamiento de la información, para luego desarrollarlo e implementarlo.

1.4 SEGURIDAD DE LOS RECURSOS HUMANOS

1.4.1 *Antes de la Contratación Laboral*

Antes de la contratación de nuevo personal se debere definir las responsabilidades de seguridad a los que va a estar ligado el nuevo empleado, esto debería definirse en el contrato en los términos y condiciones del mismo. El personal se debería seleccionar adecuadamente, y más cuando se trata de trabajos de mayor importancia.

Roles y Responsabilidades

Es conveniente definir las responsabilidades de la dirección para garantizar que se aplica la seguridad durante todo el contrato laboral de una persona dentro de la organización. Se debería brindar concientización, educación y formación en los procedimientos de seguridad y el uso correcto de los servicios de procesamiento de información a todos los usuarios.

Selección

Según la norma ISO para seguridad en la selección del personal se debería considerar, siempre y cuando se autorice en la legislación, lo siguiente:

- Referencias de comportamiento satisfactorio.
- Verificación de la hoja de vida del candidato.
- Verificación de las calificaciones profesionales y académicas declaradas.
- Verificación de la identidad.
- Verificación de los detalles adicionales tales como créditos o antecedentes criminales.

Términos y Condiciones Laborales

Para los términos y condiciones laborales se debería reflejar la política de seguridad de la organización, algunas recomendaciones de la 27001, debería tener en cuenta elementos como:

- Todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a información sensible deberían firmar un acuerdo de confidencialidad antes de tener acceso a la información.
- Responsabilidades para la clasificación de la información y la gestión de los activos de información manejados por el empleado, el contratista o el usuario de tercera parte.
- Responsabilidades del empleado, el contratista o el usuario de tercera parte para el manejo de la información recibida de otras empresas o de partes externas.
- Responsabilidades de la organización para el manejo de toda la información personal, durante el contrato laboral con la organización.
- Acciones a tomar si el empleado, el contratista o el usuario de tercera parte hace caso omiso de requisitos de seguridad de la organización.

Durante la Vigencia del Contrato Laboral

Se debe garantizar que todos los empleados, contratistas y usuarios de terceras partes están conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y deberes, y que sobre todo estén dispuestos a apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

Responsabilidades de la Dirección

Las responsabilidades de la dirección deben incluir el garantizar que los empleados, los contratistas y los usuarios de terceras partes las recomendaciondes de la norma ISO son:

- Estén adecuadamente informados sobre las funciones y responsabilidades respecto a la Seguridad de la Información antes de que se les otorgue acceso a la información.
- Tengan las directrices para establecer las expectativas de seguridad de sus funciones dentro de la organización.
- Estén motivados para cumplir las políticas de seguridad de la organización.
- Logren un grado de concientización sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización.
- Estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen la política de Seguridad.

Educación y Concientización sobre la Seguridad de la Información

A través de reuniones o foros se debería empezar con un proceso de instrucción, en el cual se presenten las políticas de seguridad de la organización y las expectativas, esto debería ser antes de otorgar el acceso a la información. En esta introducción se deberían incluir puntos como requisitos de seguridad, controles, sanciones al no cumplir estas normas.

Proceso Disciplinario

Si un empleado no cumple con las normas establecidas, se debería aplicar sanciones conforme a la mala conducta que se ha presentado y verificar si es reiterado.

Terminación o Cambio de la Contratación Laboral

Se deberían establecer responsabilidades para asegurar la gestión de la salida de los empleados, contratistas o usuarios de terceras partes de la organización y que se complete la devolución de todo el equipo y la cancelación de todos los derechos de acceso.

Responsabilidades en la Terminación

La comunicación de las responsabilidades en la terminación debería incluir las responsabilidades legales y las responsabilidades contenidas en cualquier acuerdo de confidencialidad, los términos y condiciones laborales deberían continuar durante un período definido después de terminar la contratación laboral del empleado.

Devolución de Activos

Cuando un empleado da por terminado su contrato laboral, es necesario un proceso de terminación para incluir la devolución del software previamente publicado, los documentos corporativos, manuales y los

equipos.

Retiro de los Derechos de Acceso

Después de la terminación del convenio con un empleado, se deberían considerar los derechos de acceso de la persona a los activos asociados con la información y de ser necesario retirarlos.

1.5 SEGURIDAD FISICA Y DEL ENTORNO

Dentro de esta política se considera los sistemas de información como: instalaciones, equipamiento, cableado, medios de almacenamiento.

El personal encargado de cumplir con los objetivos de este control debe:

- Definir medidas de seguridad física y del entorno.
- Controlar que se realice mantenimiento en los equipos informáticos.

1.5.1 *Áreas Seguras*

Este dominio se centra básicamente en el Centro de Procesamiento de Datos de toda la organización, en donde también podemos encontrar armarios de cableado, archivos entre otros, cada uno con su nivel de importancia. Siendo su principal objetivo evitar el acceso no autorizado a las instalaciones como a la información que maneja la organización, mediante diferentes medidas de seguridad previamente establecidas.

Perímetro de Seguridad Física

Para proteger áreas en donde se procese la información, se debe contar con puertas de acceso, paredes, dispositivos de autenticación, oficina de recepción, es decir cualquier medio que no permita el acceso a terceros.

Controles Físicos de Entrada

La organización debe proteger las áreas seguras mediante controles de acceso físico, tecnologías de autenticación, cámaras de vigilancia, monitoreo para evitar acceso de personal no autorizado.

Seguridad de Oficinas, Despachos y Recursos

Se debe evitar posibles daños causados por desastres industriales (explosión), desastres naturales (incendio, inundación) o agitación civil en la seguridad de oficinas, despachos y recursos.

Protección contra Amenazas Externas y del Entorno

Se consideran los posibles daños mencionados en la seguridad de oficinas, despachos y recursos con el fin de proteger el equipamiento.

Trabajo en Áreas Seguras

En las áreas seguras se efectúan actividades de terceros, por ello es necesario reforzar la seguridad mediante el diseño y aplicación de una

protección física.

Áreas Aisladas de Carga y Descarga

Para evitar el acceso no autorizado a lugares de tratamiento de información se debe aislar y controlar las áreas de cargar y descarga

1.5.2 *Seguridad de los Equipos*

Se debe tener cuidado contra amenazas que puedan afectar la normal operación del sistema.

Se debe disponer de controles para minimizar el riesgo potencial de:

- Robo
- Daño
- Pérdida
- Fuego
- Explosivos
- Humo
- Inundación o falta de suministro
- Interferencia Eléctrica y/o Radiación electromagnética
- Puesta en peligro de los activos
- Interrupción de las actividades de la organización

Instalación y Protección de los Equipos

Los equipos de procesamiento y tratamiento de información deben estar ubicados en lugares donde se los proteja y no puedan sufrir daños del entorno, así como evitar el acceso no autorizado, tanto durante el horario normal de trabajo como en horas no laborables.

Suministro Eléctrico

Es necesario proteger al equipamiento de problemas eléctrico, así como de fallas en el suministro de energía.

Seguridad del Cableado

Tanto el cableado de energía eléctrica como el de comunicaciones deben estar colocados bajo normas de seguridad que establezcan la protección que se debe brindarles, para prevenir interceptaciones o daños.

Mantenimiento de Equipos

El mantenimiento del equipamiento de tratamiento de la información debe ser frecuente para garantizar que la mayor parte del tiempo este íntegro y disponible.

Seguridad de los Equipos fuera de los Locales de la Organización

La seguridad de los equipos fuera de los locales de la organización debe ser la misma que la protección suministrada dentro de las instalaciones de la organización, tomando en consideración los riesgos de trabajar fuera de ella.

Seguridad en la Reutilización o Eliminación de Equipos

La información de los equipos que ya no vayan a ser de uso exclusivo de la organización deben ser eliminados por completo ya que la información puede verse comprometida por la reutilización inapropiada de los equipos.

Traslado de Activos

El personal encargado de esta tarea es el responsable de que el equipamiento y la información sean retirados con la respectiva autorización de la organización.

1.6 ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES

1.6.1 *Procedimientos Operacionales y Responsabilidades*

Establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

1.6.2 *Gestión de la Prestación del Servicio por Terceras Partes*

Su objetivo es implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceros. La organización debería verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

1.6.3 *Planificación y Aceptación del Sistema*

Con este control lo que se busca es minimizar el riesgo de fallas en los sistemas. Se requieren planificación y preparación avanzadas para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema. Es necesario hacer proyecciones de la capacidad futura para reducir el riesgo de sobrecarga del sistema.

1.6.4 *Protección contra Códigos Maliciosos y Móviles.*

El objetivo de este control es proteger la integridad del software y de la información. Se requieren precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos.

1.6.5 *Respaldo*

Se deberían establecer procedimientos de diarios para implementar la política y la estrategia de respaldo acordada para hacer copias de seguridad de los datos y probar sus tiempos de restauración.

1.6.6 *Gestión de la Seguridad de Redes*

Su objetivo es asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y la protección.

1.6.7 *Manejo de los Medios*

El objetivo es evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio. Estos medios se deberían controlar y proteger de forma física. Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador, datos de entrada, salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

1.6.8 *Intercambio de la Información*

Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito.

1.6.9 *Servicios de Comercio Electrónico*

Se debería garantizar la seguridad de los servicios de comercio electrónico y su utilización segura. Es necesario considerar las implicaciones de seguridad asociadas al uso de servicios de comercio electrónico. Incluyendo las transacciones en línea y los requisitos para los controles.

1.6.10 *Monitoreo*

Una parte esencial debería ser el monitoreo de los sistemas y llevar un registro de los eventos de seguridad de la información. Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de Información. Según la norma ISO 27001 es recomendable emplear el monitoreo del sistema para verificar la eficacia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

1.7 CONTROL DE ACCESOS

El principal objetivo de este dominio es dar a conocer la importancia del control de acceso a la red y a los recursos del sistema como medida de prevención de abusos tanto internos como externos. De igual manera trata de impedir el acceso no autorizado a los diferentes sistemas de información y servicios, implementar técnicas de autenticación y autorización, concientizar al personal que labora en la empresa sobre el uso adecuado de contraseñas y equipos de trabajo, garantizar que la conexión entre diferentes puntos sea segura, así como asegurar la

computación móvil e instalaciones de trabajo remoto.

1.7.1 *Requisitos de Negocio para el Control de Accesos.*

La organización debe establecer los requisitos de seguridad y del negocio para controlar el acceso a la información, a los procesos y servicios.

Política de Control de Accesos.

Es necesario documentar una política de control de acceso que incluya las necesidades de seguridad y de control acceso de la organización. Este documento debe ser revisado tras un periodo de tiempo.

1.7.2 *Gestión de Acceso de Usuario.*

Es importante crear un procedimiento que contenga todas las fases del acceso de los usuarios, desde el momento que inicia el registro hasta la fase final de su ingreso, con este procedimiento se trata de asegurar el acceso a usuarios autorizados a los sistemas de información. Otro procedimiento necesario sería para controlar la asignación de los derechos de acceso a los sistemas y servicios.

Registro de Usuario.

Se debe definir un procedimiento para registro de usuarios que especifique los pasos para otorgar y revocar permisos de acceso a los sistemas y servicios de la organización.

Gestión de Privilegios.

Es necesario controlar y gestionar la asignación de privilegios a los usuarios de los sistemas, ya que si se les da un uso inadecuado a los privilegios podría perjudicar a las actividades de la empresa.

Gestión de Contraseñas de Usuario.

Las contraseñas deben estar almacenadas en un sistema informático protegido mediante tecnologías diferentes a las utilizadas para la identificación y autenticación de usuarios y controladas mediante un proceso de gestión formal.

Revisión de los Derechos de Acceso de los Usuarios.

Esta revisión se la debe realizar mensualmente, para mantener un control efectivo del acceso a datos y servicios de información de la organización.

1.7.3 *Responsabilidades del Usuario.*

El principal objetivo es evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de Información.

Se debería concientizar a los usuarios sobre sus responsabilidades para el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

Uso de Contraseña.

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Equipo Informático de Usuario Desatendido.

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente como por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Políticas para Escritorios y Monitores sin Información.

Deberían adoptarse políticas de limpieza de escritorio para evitar papeles y unidades extraíbles que contengan información que requiera protección.

1.7.4 *Control de Acceso en Red.*

Evita el acceso no autorizado a los servicios en red, mediante control de acceso de los usuarios a los servicios. El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que existen interfaces apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones y las redes públicas aplican mecanismos adecuados de autenticación para los usuarios y los equipos.

Política de Uso de los Servicios de Red.

Se controlará el acceso a los servicios de red tanto internos como externos. El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red.

Autenticación de Usuario para Conexiones Externas.

El responsable de Seguridad Informática, conjuntamente con el propietario de la información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

Autenticación de Nodos de la Red.

La autenticación de nodos puede ser una alternativa a la autenticación de grupos de usuarios remotos, cuando éstos estén conectados a un sistema compartido seguro.

Protección a Puertos de Diagnóstico Remoto.

Los puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado. En muchos computadores y sistemas de comunicación se instala un servicio de conexión dialup para que los ingenieros de mantenimiento puedan realizar diagnósticos remotos.

Segregación en las Redes.

Se definirán y documentarán los perímetros de seguridad que sean convenientes, que se implementarán mediante la instalación de gateways con funcionalidades de firewall o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

Control de Conexión a las Redes.

Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto. Dichos controles se podrán implementar en los gateways que separan los diferentes dominios de la red.

Control de Encaminamiento en la Red.

Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la política de accesos a la red. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.

1.7.5 *Control de Acceso al Sistema Operativo.*

Evita el acceso no autorizado a los sistemas operativos. Se deben utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

- Autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;
- Registrar intentos exitosos y fallidos de autenticación del sistema;
- Emitir alarmas cuando se violan las políticas de seguridad del sistema;
- Suministrar medios adecuados para la autenticación: cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

Procedimientos de Conexión de Terminales.

El responsable de Seguridad Informática realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Identificación y Autenticación de Usuario.

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único solamente para su uso personal exclusivo.

Sistema de Gestión de Contraseñas.

El sistema de administración de contraseñas debe:

- Imponer el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Imponer una selección de contraseñas de calidad.
- Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas.
- Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware.
- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

Uso de los Servicios del Sistema.

Es fundamental que se restrinja el uso de sistemas o aplicaciones y se mantenga fuertemente controlado el acceso a las mismas. Los controles siguientes deberían ser considerados:

- Usar procedimientos de autenticación para las facilidades del sistema;
- Separar las facilidades del sistema de las aplicaciones de software;
- Limitar el uso de las facilidades del sistema al mínimo número de usuarios autorizados y fiables;
- Autorizar el uso de las facilidades con un propósito concreto (ad hoc);
- Limitar la disponibilidad de las facilidades del sistema;
- Registrar todo uso de las facilidades del sistema;
- Definir y documentar los niveles de autorización para las facilidades del sistema;
- Desactivar todas las facilidades basadas en software y el software de sistemas que no sean necesarios.

- No dar disponibilidad de las facilidades del sistema a usuarios que tienen acceso a aplicaciones en sistemas donde utilizan separación de tareas.

Desconexión Automática de Terminales.

El responsable de Seguridad Informática, junto con los propietarios de la información de que se trate definirán cuáles se consideran terminales de alto riesgo o que sirven a sistemas de alto riesgo. Las mismas se deben apagar después de un periodo definido de inactividad, por un lapso que responderá a los riesgos de seguridad del área y de la información que maneje la terminal. Para las PC's, se implementa la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Limitación del Tiempo de Conexión.

Para aplicaciones informáticas sensibles se debe limitar el tiempo de conexión, sobre todo de terminales instaladas en zonas de alto riesgo.

1.7.6 *Control de Acceso a las Aplicaciones.*

Es necesario usar medios de seguridad para restringir el acceso a los sistemas de aplicación y dentro de ellos.

Restricción de Acceso a la Información.

Los usuarios acceden a la información delegada por parte de la organización de acuerdo con lo estipulado en la política de control de acceso definida.

Aislamiento de Sistemas Sensibles.

Aislar sistemas sensibles que solo deben compartir recursos con los sistemas de aplicación confiables.

1.7.7 *Informática Móvil y Tele Trabajo.*

Garantiza la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

Informática Móvil.

Con el uso de dispositivos de computación móvil, como portátiles, agendas y teléfonos móviles, se debe establecer una política que tenga presente los riesgos de trabajar con estos dispositivos, especialmente en entornos desprotegidos.

Trabajo Remoto.

El trabajo remoto debe ser autorizado por el responsable de la organización, al cual pertenezca el usuario que solicita el trabajo remoto. La organización debería aplicar protección en el sitio del trabajo remoto y garantizar que se han establecido las disposiciones adecuadas para esta forma de trabajo.

1.8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

En caso de que la organización cuente con un equipo de desarrollo de software, el objetivo de este control es el de garantizar que la seguridad es parte integral de los sistemas de información, estos incluyen sistemas operativos, infraestructura, aplicaciones del negocio, servicios y aplicaciones desarrolladas para usuarios.

1.8.1 *Requisitos de Seguridad de los Sistemas de Información*

Se deberían identificar los requisitos de seguridad antes del desarrollo y/o la implementación de los sistemas de información.

Análisis y Especificación de los Requisitos de Seguridad

En las especificaciones para los requisitos de control se debe considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de manuales de apoyo.

1.8.2 *Procesamiento Correcto en las Aplicaciones*

Diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto. Estos controles deberían incluir la validación de los datos de entrada y de salida del procesamiento interno.

Validación de los Datos de Entrada

Se deben realizar validaciones de los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.

Control de Procesamiento Interno

Se deben incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información. El diseño y la implementación de las aplicaciones garantizan que se minimizan los riesgos de falla en el procesamiento, los cuales originan pérdida de la integridad.

Integridad del Mensaje

Identificar los requisitos para asegurar la autenticidad y proteger la integridad en las aplicaciones, así como identificar e implementar los controles adecuados.

Validación de los Datos de Salida

Se deberían validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.

1.8.3 *Controles Criptográficos*

Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos. Es necesario desarrollar una política sobre el uso de los controles criptográficos y establecer una gestión de

claves para dar soporte al empleo de técnicas criptográficas.

Política Sobre el Uso de Controles Criptográficos

Se debería implementar una política sobre el uso de controles criptográficos para la protección de la información. Se recomienda según la ISO[4], tomar en consideración los siguientes aspectos al desarrollar una política criptográfica:

- El enfoque de la dirección para el uso de controles criptográficos en la organización, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio.
- Uso de encriptación para la protección de la información transportada por medios móviles o removibles, por dispositivos o a través de líneas de comunicación.
- Funciones y responsabilidades, es decir, quien es encargado de la implementación de la política y de la gestión de claves.

Gestión de Claves

Se recomienda que todas las claves criptográficas deberían tener protección contra modificación, pérdida o destrucción. Un sistema de gestión de claves se debería basar en un conjunto acordado de normas, procedimientos y método seguros.

1.8.4 *Seguridad de los Archivos del Sistema*

Los accesos a los archivos del sistema y al código fuente del programa deberían estar protegidos, y los proyectos de tecnología de la información y las actividades de soporte se deberían efectuar de forma segura.

Control del Software Operativo

Se deben establecer procedimientos para controlar la instalación de software en los sistemas operativos.

Protección de los Datos de Prueba del Sistema

Evitar el uso de bases de datos operativos que contiene información sensible con propósitos de prueba. Si se utiliza información sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso.

Control de Acceso al Código Fuente de los Programas

Como se describe en la ISO el acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios.

4 POSSO, R.(2009). Desarrollo de políticas de seguridad informática e implementación de tres dominios en base a la norma 27002 para el área de hardware en la empresa Uniplex S.A en Quito. Obtenido el 04 de octubre de 2011

1.8.5 *Seguridad en los Procesos de Desarrollo y Soporte*

Los entornos de soporte y de desarrollo deberían estar estrictamente controlados. Como en uno de los controles anteriores este será necesario si la empresa cuenta con un equipo de desarrolladores.

Procedimientos de Control de Cambios

Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios como bitácoras o logs. Los procedimientos se deberían documentar y hacer cumplir.

Revisión Técnica de las Aplicaciones Después de los Cambios en el Sistema Operativo

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay un mal impacto en las operaciones ni en la seguridad de la organización.

Restricciones en los Cambios a los Paquetes de Software

Según la norma ISO se debería minimizar y controlar la realización de modificaciones a los paquetes de software, limitarlas a cambios necesarios. Los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones.

Fuga de Información

Se deberían evitar las oportunidades para que se produzca fuga de información, por ello se debería considerar los siguientes aspectos que indica la ISO 27001:

- Exploración de los medios y comunicaciones de salida para determinar la información oculta.
- Utilización de sistemas y software que se consideran con alta integridad (productos evaluados).
- Monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes.

Desarrollo de Software Contratado Externamente

Se debería supervisar y monitorear el desarrollo de software cuando este no es ejecutado por un equipo interno de la organización.

1.9 ADMINISTRACIÓN DE LOS INCIDENTES DE SEGURIDAD

Dentro de este dominio se define a la incidencia de seguridad como un suceso de eventos de seguridad no deseados o no esperados que tienen una alta probabilidad de interrumpir las operaciones de la organización o comprometer la seguridad de la información. Un evento de seguridad es un suceso que indique que posiblemente las políticas de seguridad fueron violadas en uno de los sistemas, servicios o redes y que puedan ser relevantes para la seguridad de la información.

1.9.1 *Comunicación de Eventos y Debilidades en la Seguridad de la Información.*

Su objetivo es asegurar que los eventos y las debilidades de la seguridad de la información relativa con los sistemas de información sean comunicados para que permitan a los responsables de esta tarea, tomar las acciones correctivas. Todos los empleados y deben tener conocimiento sobre los procedimientos para dar a conocer los diferentes tipos de eventos y las debilidades que puedan tener impacto en la seguridad de los activos de la organización.

Comunicación de Eventos en Seguridad.

Es necesario comunicar los eventos en la seguridad de información en el tiempo más corto posible mediante canales proporcionados por la organización, para ello es recomendable definir un punto de contacto que debe ser conocido por todos los empleados. Este punto de contacto puede ser una dirección de email, una aplicación web, un número de teléfono o cualquier otro canal de comunicación que la organización de a conocer, la misma que debe estar siempre disponible.

Comunicación de Debilidades en Seguridad.

Requiere que empleados de los sistemas de información, sean quienes notifiquen eventos de seguridad. Es necesario informar que los usuarios nunca deben tratar de verificar vulnerabilidades identificadas o que sospechen que existen, por que estas actuaciones de los usuarios pueden ser tomadas como un ataque no intencionado o una violación de la política de seguridad. Para la comunicación de debilidades de seguridad es necesario disponer de un sistema de feedback.

1.9.2 *Gestión de Incidentes y Mejoras en la Seguridad de la Información.*

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera eficaz una vez se han reportado, para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

Identificación de Responsabilidades y Procedimientos.

Las responsabilidades y los procedimientos de la parte encargada de manejar esas notificaciones, se deben establecer para asegurar una respuesta rápida, eficaz, y ordenada a los incidentes de la seguridad de la información. [5]

Evaluación de Incidentes en Seguridad.

Se debe contar con mecanismos para cuantificar y supervisar incidentes de seguridad que afecten al procesamiento de la información. Estos incidentes deben ser evaluados para evitar que se repitan en otras ocasiones.

5 Alvarez Zurita F M & García Guzman P A. (2007). Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud. Obtenido el 23 de octubre de 2011, de http://www.bibdigital.epn.edu.ec/bitstream/15000/565/1/CD-1077.pdf

Recogida de Pruebas.

Para recoger las pruebas necesarias y presentar las evidencias se deben establecer procedimientos internos, con la finalidad de aplicar acciones disciplinarias.

1.10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

El objetivo de este control es el de adoptar todas las medidas para minimizar en lo posible la interrupción del servicio o actividad de la empresa.

1.10.1 *Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio*

Es neceario identificar los proceso críticos de la organización para integrarlos con los de la gestión de la seguridad, esto con el fin de minimizar el impacto y la pérdida de activos de información en la organización.

1.10.2 *Inclusión de la Seguridad de la Información en el Proceso de Gestión de la Continuidad del Negocio*

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trae los requisitos de Seguridad de la Información necesarios para la continuidad del negocio dentro de la organización.

Continuidad del Negocio y Evaluación de los Riesgos

Se debe identificar los eventos que pueden causar interrupciones en los procesos del negocio luego de esto realizar una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación. Según las ISO, estas evaluaciones deben considerar todos los procesos del negocio para identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización.

Desarrollo e Implementación de Planes de Continuidad que Incluyan la Seguridad de la Información

Según como lo indica la documentación de las ISO, se deberían desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.

Estructura para la Planificación de la Continuidad del Negocio

Es necesario mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la Seguridad de la Información así como identificar las prioridades para pruebas y mantenimiento.

Cada plan debería especificar las condiciones para su activación, así como las personas responsables encargados de llevar a cabo cada componente del plan. Como lo define la norma ISO 27001 una estructura para la planificación de la continuidad del negocio debería considerar los siguientes aspectos:

- Los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio.
- Los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos.
- Los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración.
- Los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad.
- Una programación de mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del plan.
- Actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.
- Las responsabilidades de las personas, que describan quién es responsable de la ejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes.
- Los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

Pruebas, Mantenimiento y Reevaluación de los Planes de Continuidad del Negocio

Se deben ejecutar las pruebas necesarias del plan de continuidad del negocio, y de esta forma asegurar que todos los miembros del equipo de recuperación son conscientes de los planes y sus responsabilidades para la continuidad del negocio y la Seguridad de la Información. Se deben aplicar técnicas para garantizar que los planes funcionen en condiciones reales.

1.11 CUMPLIMIENTO (LEGALES,DE ESTÁNDARES,TÉCNICAS Y AUDITORÍAS)

Este dominio pretende asegurar el cumplimiento de leyes reglamentarias, contractuales o de seguridad, así como verificar que los sistemas cumplan con las normas y políticas de seguridad de la organización, con la finalidad de minimizar amenazas tanto interna como externa de la organización.

1.11.1 *Conformidad con los Requisitos Legales.*

Este control pretende evitar incumplimientos de ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad.

Identificación de la Legislación Aplicable.

Todos los sistemas de información tienen requisitos normativos y contractuales que deben ser definidos y documentados.

Derechos de Propiedad Intelectual.

Procedimientos para uso del material protegido por derechos de propiedad intelectual, mediante restricciones legales.

Salvaguarda de los Registros de la Organización.

Para cumplir con los requisitos legales o regulatorios, se debe proteger los registros de la organización para evitar su pérdida, destrucción y falsificación.

Protección de Datos de Carácter Personal y de la Intimidad de las Personas.

Se debe brindar formación a los empleados para que tengan un conocimiento claro sobre la protección de la información que manipulan en las diferentes actividades.

Evitar Mal Uso de los Dispositivos de Tratamiento de la Información.

Con la finalidad de evitar que el acceso que se les brinda a los diferentes recursos sea inadecuado y se concienticen del correcto uso de los dispositivos de tratamiento de información.

Reglamentación de los Controles de Cifrados.

Controles criptográficos conforme a leyes y reglamentos de cada país.

1.11.2 *Revisiones de la Política de Seguridad y de la Conformidad Técnica.*

Se deben hacer revisiones regulares de la seguridad de los sistemas de información para asegurar la conformidad de los sistemas en base a políticas de seguridad apropiadas y normas apropiadas. Una vez realizada la auditoria se determina si el cumplimiento de los estándares es el adecuado.

Conformidad con la Política de Seguridad.

El personal encargado debe verificar la correcta implementación y cumplimiento de procedimientos de seguridad, dentro de su área asignada.

Comprobación de la Conformidad Técnica.

El personal encargado verificará que los sistemas de información cumplan con los procedimientos de seguridad, que incluyen controles de hardware y software correctamente implementados.

1.11.3 *Consideraciones Sobre la Auditoria de Sistemas.*

Con este control se busca maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema; estableciendo la necesidad de controles para salvaguardar los sistemas operativos y las

herramientas de auditoría durante las auditorias del sistema.[6]

Controles de Auditoría de Sistemas.

Es necesario llevar a cabo procedimientos en los que se indique las actividades de auditoría para combrobaciones de sistemas operativos, con la finalidad de minimizar riesgos de interrupción de los procesos esenciales de la organización.

Protección de las Herramientas de Auditoría de Sistemas.

Proteger herramientas de auditorías de sistemas como: software o archivos de datos, para evitar un posible mal uso, pérdida de información comprometida.

6 Alvarez Zurita F M & García Guzman P A. (2007). Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud. Obtenido el 23 de octubre de 2011, de http://www.bibdigital.epn.edu.ec/bitstream/15000/565/1/CD-1077.pdf

2 ESTÁNDAR ISO 27011

La ISO 27011 es un desarrollo del marco de controles de otras ISO, reúne varias recomendaciones de las ISO como la ISO 9001 (Gestión Ambiental), ISO 9001:2000(sistema de gestión de la calidad) ISO 27001 (Gestión de riesgos) entre otras.

Esta ISO es una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU que está especialmente creada para los organismos de telecomunicaciones, instalaciones de telecomunicaciones, redes y líneas y para los que éstos suponen importantes activos empresariales.

Esta ISO permite establecer políticas, procedimientos y controles que tienen que ver con los objetivos de negocio de la organización en este caso la de brindar servicios de telecomunicaciones, su principal meta es minimizar riesgos propios de la organización. Se a visto necesario la implementación de está ISO debido a que la gestión de la seguridad de la información es sumamente necesaria con el fin de que los organismos de telecomunicaciones puedan gestionar adecuadamente estos activos de la empresa y continuar con éxito sus actividades.

2.1 ARQUITECTURA DE SEGURIDAD PARA INTERCONEXION DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT

Toma el modelo de referencia OSI para la interconexión de sistemas abiertos. Establece un marco para coordinar el desarrollo de recomendaciones existentes y futuras para la interconexión de sistemas.

El objetivo de este control es el permitir la interconexión de sistemas de computador heterogéneos para de esta forma lograr comunicaciones màs eficientes. En distintos momentos, deben establecerse controles de seguridad para proteger la información intercambiada entre los procesos de aplicación.

2.1.1 *Alcance y Campo de Aplicación*

Según la recomentación X.800
[1] de la norma ISO 27011 :

- Da una descripción general de los servicios de seguridad y mecanismos conexos, que pueden ser proporcionados por el modelo de referencia; y
- Define las posiciones, dentro del modelo de referencia, en que pueden proporcionarse los servicios y mecanismos.

1 UNIÓN NACIONAL DE TELECOMUNICACIONES, Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT, Recomendación X.800. Tomado el 10 de noviembre de 2011

2.1.2 *Ubicación de los Servicios y Mecanismos de Seguridad*

Se definen los servicios de seguridad que han de proporcionarse en el marco del modelo de referencia OSI y se describe de forma breve la manera en la cual han de realizarse.

Según la recomendación X.800 de la norma ISO 27011 son varias las definiciones que son aplicables en misma pero podemos resaltar los más importantes como control de acceso, imputabilidad, auditoría, autenticación, confidencialidad, credenciales, criptoanálisis, valor de comprobación criptográfico, política de seguridad, servicio de seguridad, etc.

Capa Física

Servicios

1. Confidencialidad en modo con conexión, y
2. Confidencialidad del flujo de tráfico.

El servicio de confidencialidad del flujo de tráfico adopta dos formas:

1. Confidencialidad total del flujo de tráfico, que puede proporcionarse solamente en ciertas circunstancias, por ejemplo, transmisión bidireccional simultánea, síncrona, punto a punto, y
2. Confidencialidad limitada del flujo de tráfico, que se puede proporcionar para otros tipos de transmisión, por ejemplo, transmisión asíncrona.

Mecanismos

Una de las formas de cifrado, aplicable únicamente en la capa física, es la seguridad de transmisión (es decir, una seguridad de espectro ensanchado). La protección de la capa física es suministrada por medio de un dispositivo de cifrado que funciona de manera transparente. El objetivo de la protección de la capa física es proteger todo el tren binario de datos del servicio físico y suministrar la confidencialidad del flujo de tráfico.

Capa de Enlace de Datos

Servicios

1. Confidencialidad en modo con conexión, y
2. Confidencialidad en modo sin conexión.

Mecanismos

El mecanismo de cifrado se utiliza para proporcionar los servicios de seguridad en la capa de enlace de datos. La funcionalidad adicional

de protección de seguridad de la capa de enlace de datos se realiza antes de las funciones normales de capa para la transmisión y después de estas funciones para la recepción. Los mecanismos de cifrado de la capa de enlace de datos son sensibles al protocolo de la capa de enlace de datos

Capa de Red

La capa de red está organizada internamente para proporcionar protocolos que realizan las siguientes operaciones:

- Acceso a subred;
- Convergencia dependiente de la subred;
- Convergencia independiente de la subred; y
- Relevo y encaminamiento.

Servicios

1. Autenticación del origen de los datos;
2. Servicio de control de acceso;
3. Confidencialidad en modo con conexión;
4. Confidencialidad en modo sin conexión;
5. Confidencialidad del flujo de tráfico;
6. Integridad en modo con conexión sin recuperación; y
7. Integridad en modo sin conexión.

Estos servicios de seguridad pueden prestarse individualmente o combinados

Mecanismos

El encaminamiento se efectúa en esta capa y, por tanto, el control de encaminamiento está situado en esta capa.

1. El servicio de autenticación de entidad par se proporciona por una combinación adecuada de intercambios de autenticación, mecanismos de intercambio de contraseñas protegidos y mecanismos de firma;
2. El servicio de autenticación del origen de los datos puede proporcionarse mediante mecanismos de cifrado o de firma;
3. El servicio de control de acceso se proporciona mediante el uso apropiado de mecanismos específicos de control de acceso;
4. El servicio de confidencialidad en modo con conexión se proporciona mediante un mecanismo de cifrado y/o control de encaminamiento;

5. El servicio de confidencialidad en modo sin conexión se proporciona mediante un mecanismo de cifrado y/o control de encaminamiento;
6. El servicio de confidencialidad del flujo de tráfico se presta mediante un mecanismo de relleno de tráfico, combinado con un servicio de confidencialidad en la capa de red o debajo de ésta y/o control de encaminamiento;
7. El servicio de integridad en modo con conexión sin recuperación se proporciona utilizando un mecanismo de integridad de los datos, y
8. El servicio de integridad en modo sin conexión se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado.

Capa de Transporte

Servicios

Los servicios de seguridad que pueden prestarse, individualmente o combinados, en la capa de transporte son:

- Autenticación de entidad par;
- Autenticación del origen de los datos;
- Servicio de control de acceso;
- Confidencialidad en modo con conexión;
- Confidencialidad en modo sin conexión;
- Integridad en modo con conexión con recuperación;
- Integridad en modo con conexión sin recuperación;
- Integridad en modo sin conexión.

Mecanismos

1. El servicio de autenticación de entidad par es proporcionado por una combinación apropiada de intercambios de autenticación o protegidos, mecanismos de intercambio derivados criptográficamente o protegidos, o por mecanismos protegidos de intercambio de contraseñas y firmas;
2. El servicio de autenticación de origen de los datos puede proporcionarse por mecanismos de cifrado o de firma;
3. El servicio de control de acceso se proporciona mediante el uso apropiado de mecanismos específicos de control de acceso;
4. El servicio de confidencialidad en modo con conexión se proporciona mediante un mecanismo de cifrado;

5. El servicio de confidencialidad en modo sin conexión se proporciona mediante un mecanismo de cifrado;
6. El servicio de integridad en modo con conexión con recuperación se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado;
7. El servicio de integridad en modo con conexión y recuperación se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado; y
8. El servicio de integridad en modo sin conexión se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado.

Capa de Sesión

Servicios

En la capa de sesión no se proporcionan servicios de seguridad.

Capa de Presentación

Servicios

La capa de presentación proporcionará facilidades para el soporte de la prestación de los siguientes servicios de seguridad por la capa de aplicación al proceso de aplicación:

1. Confidencialidad en modo con conexión;
2. Confidencialidad en modo sin conexión; y
3. Confidencialidad de campos seleccionados.
4. Confidencialidad del flujo de tráfico;
5. Autenticación de entidad par;
6. Autenticación de origen de los datos;
7. Integridad en modo con conexión con recuperación;
8. Integridad en modo con conexión sin recuperación;
9. Integridad en modo con conexión de campos seleccionados;
10. Integridad en modo sin conexión;
11. Integridad en modo sin conexión de campos seleccionados;
12. No repudio

Mecanismos

Pueden utilizarse junto con mecanismos de seguridad de la capa de aplicación para proporcionar servicios de seguridad de la capa de aplicación:

1. El servicio de autenticación de entidad par puede ser soportado por mecanismos de transformación sintáctica (por ejemplo, el cifrado)
2. El servicio de autenticación del origen de los datos puede ser soportado por mecanismos de cifrado o de firma;
3. El servicio de confidencialidad en modo con conexión puede ser soportado por un mecanismo de cifrado;
4. El servicio de confidencialidad en modo sin conexión puede ser soportado por un mecanismo de cifrado;
5. El servicio de confidencialidad de campos seleccionados puede ser soportado por un mecanismo de cifrado;
6. El servicio de confidencialidad de flujo de tráfico puede ser soportado por un mecanismo de cifrado.
7. El servicio de integridad en modo con conexión con recuperación puede ser soportado por un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado;
8. El servicio de integridad en modo con conexión sin recuperación puede ser soportado por un mecanismo de integridad de datos, algunas veces combinado con un mecanismo de cifrado;
9. El servicio de integridad en modo con conexión de campos seleccionados puede ser soportado por un mecanismo de integridad de datos, algunas veces combinado con un mecanismo de cifrado.
10. El servicio de integridad en modo sin conexión puede ser soportado por un mecanismo de integridad de datos, algunas veces combinado con un mecanismo de cifrado.
11. El servicio de integridad en modo sin conexión de campos seleccionados puede ser soportado por un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado;
12. El servicio de no repudio con prueba del origen puede ser soportado por una combinación apropiada de mecanismos de integridad de datos, de firma y de notarización, y;
13. El servicio de no repudio con prueba de la entrega puede ser soportado por una combinación apropiada de mecanismos de integridad de datos, de firma y de notarización.

Capa de Aplicación

Servicios

La capa de aplicación puede proporcionar uno o más de los siguientes servicios de seguridad básicos individualmente o combinados:

- Autenticación de entidad par;
- Autenticación del origen de los datos;
- Servicio de control de acceso;
- Confidencialidad en modo con conexión;
- Confidencialidad en modo sin conexión;
- Confidencialidad de campos seleccionados;
- Confidencialidad del flujo de tráfico
- Integridad en modo con conexión con recuperación;
- Integridad en modo con conexión sin recuperación;
- Integridad en modo con conexión de campos seleccionados;
- Integridad en modo sin conexión;
- Integridad en modo sin conexión de campos seleccionados;
- No repudio con prueba del origen y;
- No repudio con prueba de la entrega.

La autenticación de los partícipes previstos en la comunicación facilita los controles de acceso a recursos y distintos por ejemplo, ficheros, logical (software, terminales, impresoras) en sistemas abiertos reales. La determinación de requisitos específicos de seguridad en una instancia de comunicación, incluidas la confidencialidad, la integridad y la autenticación de los datos

Mecanismos

Los servicios de seguridad de la capa de aplicación se proporcionan mediante los siguientes mecanismos:

1. El servicio de autenticación de entidad par puede proporcionarse utilizando la información de autenticación transferida entre entidades de aplicación, protegida por mecanismos de cifrado de la capa de presentación o de capas más bajas;
2. El servicio de autenticación del origen de los datos puede proporcionarse utilizando mecanismos de firma o mecanismos de cifrado de capas más bajas;
3. El servicio de control de acceso para estos aspectos de un sistema abierto real que son pertinentes a ISA, tales como la capacidad de comunicar con sistemas específicos o entidades de aplicación distantes, puede ser proporcionado por una combinación de mecanismos de control de acceso en la capa de aplicación y en capas inferiores;

4. El servicio de confidencialidad en modo con conexión puede proporcionarse utilizando un mecanismo de cifrado de capas inferiores;

2.2 ARQUITECTURA DE SEGURIDAD PARA SISTEMAS DE EXTREMO A EXTREMO DE LAS COMUNICACIONES

Esta arquitectura pretende asegurar la red de extremo a extremo, conforme a exigencias de seguridad por parte de proveedores, clientes y la organización. Para brindar esta seguridad a la red, se la divide lógicamente de acuerdo a características de seguridad, en componentes de arquitectura, con la finalidad de evaluar la seguridad de la red y en caso de existir falencias planificar procedimientos para la pronta recuperación de la red.

Es válida para redes de voz, datos y convergentes de tecnología inalámbrica, óptica o de cable. Esta segmentación permite considerar la seguridad de extremo a extremo de forma sistemática, lo que permite planificar nuevas soluciones de seguridad y evaluar la seguridad de las redes actuales. [2]

Los componentes a estudiar dentro de esta arquitectura son:

- Dimensiones de Seguridad
- Capas de Seguridad
- Planos de Seguridad

2.2.1 *Dimensiones de Seguridad*

Control de Acceso:
Garantizar que el personal y dispositivos autorizados accedan a los recursos de red.

Confidencialidad:
Garantizar que los datos no sean interpretados u obtenidos por entidades no autorizadas.

Integridad:
Garantizar que los datos en el proceso de transmisión del emisor al receptor sean correctos, es decir no estén expuestos a modificaciones.

Privacidad:
Evita dar a conocer información de las actividades de red (direcciones IP).

Autenticación:
Garantizar que no se ha usurpado la entidad en el proceso de comunicación, así como verificar la procedencia de la información.

Disponibilidad:
Garantizar que todos los recursos y servicios de la red estén disponibles en todo momento.

2 Ruiz, B. A. P. (2011). Académica cursos libres Web site. Obtenido el 07 de noviembre de 2011, de http://cursoslibres.academica.mx/computacion/seguridad-en-redes/1-principios-de-seguridad-en-redes-de-datos/arquitectura-de-seguridad-en-redes

No repudio:
Garantizar que no se pueda negar la realización de alguna actividad en la red.

Seguridad de la Información:
Garantizar que la información únicamente se establece entre los extremos autorizados.

2.2.2 *Capas de Seguridad*

El diseño de capas brinda seguridad en cada una de las capas de extremo a extremos, siendo establecidas las siguientes capas:

Seguridad de las Aplicaciones

La capa de seguridad aplicaciones proporciona seguridad en las aplicaciones, tanto de la red como a las que acceden los clientes. Aquí tenemos aplicaciones de correo electrónico, FTP, HTTP, mensajería instantánea, etc.

Seguridad de los Servicios

La capa de seguridad de servicios, tiene que ver con la seguridad de los servicios que los proveedores prestan a sus clientes como son: servicios básicos de transporte y conectividad, plataformas auxiliares para el acceso a Internet, mensajería instantánea, etc.[3]

Seguridad de la Infraestructura

La capa de seguridad de infraestructura, abarca todos los elementos que conforman la red de datos así como los dispositivos de transmisión. Esta capa es parte esencial de las redes, servicios y aplicaciones. Dentro de estos elementos tenemos: enrutadores, servidores, enlaces de comunicación, entre otros.

2.2.3 *Planes de Seguridad*

Gestión

Este plano tiene que ver con la protección de las funciones de:

- Operaciones
- Administración
- Gestión
- Aprovisionamiento de la red

Los protocoles que trabajan aquí son:

- SNMP, Telnet, FTP, HTTP

Control

Este plano tiene que ver con la protección de las actividades que permiten:

- Actualización de routers / tablas de conmutación

3 Ruiz, B. A. P. (2011). Académica cursos libres Web site. Obtenido el 07 de noviembre de 2011, de http://cursoslibres.academica.mx/computacion/seguridad-en-redes/1-principios-de-seguridad-en-redes-de-datos/arquitectura-de-seguridad-en-redes

- Servicio de la iniciación, control y desmontaje
- Aplicación de control

Los protocoles que trabajan aquí son:

- BGP, OSPF, IS-IS, RIP, PIM, SIP, RSVP, H.323, SS7, IKE, ICMP, PKI, DNS, DHCP, SMTP

Usuario Final

Este plano se encarga de la seguridad cuando los clientes acceden y utilizan la red del proveedor de servicio. Dentro de las actividades de esta capa tenemos:

- Transferencia de datos de usuario final
- Interacción de aplicaciones de usuario final

Los protocoles que trabajan aquí son:

- HTTP, RTP, POP, IMAP, TCP, UDP, FTP, IPsec, TLS

2.3 SISTEMAS DE GESTIÓN DE CALIDAD

Es la nueva norma basada en el estándar ISO 9000 que fue desarrollado específicamente para la industria de las telecomunicaciones.

Las metas que persigue este estándar son:

- Confiabilidad y costos asociados
- Establecer y mantener requerimientos para funciones de Servicio especializadas
- Establecer requerimientos para tratar continuos problemas de comunicación en la cadena de abastecimiento
- Reforzar las relaciones entre el cliente y el proveedor

2.3.1 *Requisitos de un Sistema de Gestión de Calidad*

Según las recomendaciones de esta normar la organización debe establecer, documentar, implementar y mantener un SGC y mejorar continuamente su eficacia. Las etapas lógicas que esto supone incluyen:

1. Determinar las necesidades y expectativas de los clientes;
2. Establecer la política y objetivos de la calidad de la organización;
3. Determinar los procesos y las responsabilidades necesarias para el logro de los objetivos de la calidad;

4. Determinar y proporcionar los recursos necesarios para el logro de los objetivos de la calidad;
5. Establecer los métodos para medir la eficacia de cada proceso y aplicar las medidas correspondientes;
6. Determinar los medios para prevenir no conformidades y eliminar sus causas;
7. Establecer y aplicar un proceso para la mejora continua del SGC.

2.3.2 *Compromiso con la Calidad*

La Dirección de la organización debería garantizar que el personal se encuentre completamente involucrado.

Las actividades que la dirección debería planificar son:

- Establecer y mantener una política de calidad y asegurarse que se definen los objetivos de calidad de la organización, mesurable y coherente con dicha política.
- Comunicar la política y los objetivos de calidad en el seno de la organización para aumentar la concienciación, la motivación y la participación del personal.
- Asegurarse de que la organización está plenamente orientada a satisfacer tanto los requisitos del cliente como los legales y reglamentarios.
- Asegurarse de que se identifican y desarrollan todos los procesos necesarios para cumplir con estos requisitos y para alcanzar los objetivos de calidad definidos.
- Asegurarse de que se ha establecido, implantado y mantenido un SGC eficaz para alcanzar los objetivos de calidad definidos.
- Asegurarse de la disponibilidad de recursos necesarios.
- Revisar periódicamente el SGC.
- Decidir sobre las acciones en relación con la política y con los objetivos de calidad y sobre las acciones de mejora.

2.3.3 *Enfoque al Cliente*

Esta norma revela la importancia que tiene el cliente para la organización, por esta razón,este requisito está bajo la responsabilidad de la Dirección. Para hacerlo con éxito, debería procurar llegar a un acuerdo con su cliente acerca de qué servicios ha de suministrarle.

Para llevar a cabo esto es necesario seguir un conjunto de especificaciones descritos en la norma:

- Hablar con los clientes.
- Realizar estudios de mercado o de la clientela.
- Tener acceso a informes del sector.

- Identificar oportunidades de comercialización especializada.

2.3.4 *Política de la Calidad*

La Dirección debe asumir esta responsabilidad, de los que la calidad significa para la organización y para sus clientes.

Según las recomendaciones de la ISO, la Dirección debe asegurarse de que la política de la calidad:

1. Es adecuada al propósito de la organización.
2. Incluye un compromiso de cumplir con los requisitos y de mejorar continuamente la eficacia del SGC.
3. Proporciona un marco de referencia para establecer y revisar los objetivos de la calidad.
4. Es comunicada y entendida dentro de la organización.
5. Es revisada para su continua adecuación.

La política de la calidad también necesita ser revisada periódicamente, a fin de determinar si los objetivos siguen siendo los más apropiados para la organización. Esto debería llevarse a cabo en la revisión del sistema por la Dirección.

2.4 SISTEMAS DE GESTIÓN AMBIENTAL

Las normas ISO 14000[4] son utilizadas como parte de un sistema de gestión medioambiental que puede ser aplicado tanto a productos y servicios, como a los procesos de producción y administración de la empresa.

Estas normas de gestión medioambiental son aplicables en organizaciones que desean:

- Implementar, mantener y perfeccionar un sistema de gestión medioambiental.
- Asegurar que la empresa cumpla con la política medioambiental que exige el país.
- Conseguir la certificación y registro del sistema de gestión medioambiental por parte de una organización externa.

2.4.1 *Política Ambiental*

Dentro de la política ambiental se define la misión, la visión ambiental de la organización, objetivos y metas y como punto principal está la declaración que hace la empresa para garantizar su compromiso con la conservación del ambiente.

4 Cordero P & Salas S. (2002). Sistemas de Gestión Medio Ambiental: Las Normas ISO 14000. Obtenido el 13 de noviembre de 2011, de http://www.bvsde.paho.org/bvsaia/fulltext/ct21.pdf

2.4.2 *Planificación*

La planificación consta de las siguientes etapas:

- Aspectos ambientales y sus impactos
- Requerimientos legales y otros
- Objetivos y Metas
- Programa(s) de Gestión Ambiental

Aspectos Ambientales

Dentro de los aspectos ambientales es necesario reconocer los aspectos que la organización podría controlar o en los que influye de alguna manera como podría ser el consumo de energía y demás actividades que podrían tener grandes impactos en el medio ambiente.

Requerimientos Legales y Otros

Para esta debe crearse un proceso por medio del cual se identifiquen cuáles son los requerimientos legales: requerimientos nacionales, locales, permisos, normas internacionales, y otras reglas que deba adoptar la empresa, como son: códigos específicos de la empresa, requerimientos del proveedor, requerimientos de la compañía aseguradora, normas en locales donde se venden sus productos y servicios, etc.

Objetivos y Metas

Los objetivos y metas pueden variar dependiendo de las necesidades establecidas por la organización, entre los principales objetivos están la capacitación a los empleados y mejorar la educación con respecto al medio ambiente. Las metas ambientales son tradicionalmente más específicas, como reducir el consumo de energía en un 10 % en un año, o la reducción de generación de desechos peligrosos en un 3 % en un período de tres años, por ejemplo.[4]

Programa(s) de Gestión Ambiental

El Programa de Gestión Ambiental (PGA) es un plan de acción para lograr los objetivos y metas del sistema de gestión ambiental. Se desarrolla priorizando acciones en relación con los procesos, productos, servicios y proyectos que se relacionen con los aspectos ambientales significativos establecidos, objetivos y metas, y la política ambiental de la empresa. El programa debe ser documentado, para poder ser sujeto a revisión posteriormente. [4]

2.5 TECNOLOGÍA DE LA INFORMACIÓN

Al seguir los lineamientos de una norma ISO[5], proporciona a las organizaciones un planteamiento estructurado para desarrollar servicios de tecnología de la información fiables. Es un reto, pero también es una oportunidad que tienen las empresas para salvaguardar sus sistemas de gestión de tecnología de la información.

Se concentra en la gestión de problemas de tecnología de la información mediante el uso de un planteamiento de servicio de asistencia, los problemas se clasifican, lo que ayuda a identificar problemas continuados o interrelaciones.

5 ATTEST. ISO 20000 e ISO 27000. Obtenido 20 noviembre de 2011, de http://www.attest.es/

Avala la calidad y apoya los diferentes servicios de soporte. La gestión de servicios de TI brinda un marco de mejores prácticas para ayudar a las organizaciones a mejorar su provisión de servicios de TI.

La Norma define los requisitos que debe cumplir un proveedor de servicios en tecnología de la información (TI) para la prestación de servicios gestionados de calidad aceptable para sus clientes. Sus puntos clave consisten en:

- Gestión del nivel de servicios.
- Informes de servicios.
- Gestión de la continuidad y disponibilidad de servicios.
- Presupuesto y contabilidad de servicios de TI.
- Gestión de la capacidad.
- Gestión de la seguridad de la información.
- Gestión de la relación del negocio.
- Gestión de los proveedores.

Ventajas:

Mediante la implementación de un Sistema de Gestión de Servicios de TI, se consigue:

- Optimizar costos a través de estructuras transparentes y gestión de servicios profesional.
- Focalizar en servicios de una punta a otra (end-to-end).
- Gestionar riesgos sistemáticamente.
- Mejorar la escala de servicios
- Reaccionar efectivamente ante posibles problemas.

2.6 GESTIÓN DE RIESGOS

Para el estudio de la gestión de riesgos, se a tomado como referencia lo expuesto en la metodología MAGERIT.[6]

2.6.1 *La Interpretación de los Valores de Impacto y Riesgo Residuales*

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores despreciables. Son pues una métrica de carencias. Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer. Si el valor residual es despreciable, ya está. Esto no quiere

6 López Crespo F, Amutio Gómez M A, Candau J, Mañas J A. (2006). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información I - Método. Obtenido el 13 de noviembre de 2011, de http://www.seap.minhap.gob.es/dms/.../Magerit-v2-I-metodo.pdf

decir descuidar la guardia; pero si afrontar el día con cierta confianza. Mientras el valor residual sea más que despreciable, hay una cierta exposición. Es importante entender que un valor residual es sólo un número.

2.6.2 *Selección de Salvaguardas*

Las amenazas hay que conjurarlas, por principio y mientras no se justifique lo contrario. Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades). Toda amenaza debe ser conjurada profesionalmente, lo que quiere decir que hay que:

- Establecer una política de la Organización al respecto; o sea, unas directrices generales de quién es responsable de cada cosa
- Establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada
- Establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer
- Desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas
- Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto.

Tipos de Salvaguardas

Un sistema debe considerar prioritariamente las salvaguardas de tipo preventivo que buscan que la amenaza no ocurra o su daño sea despreciable. Es decir, impedir incidentes o ataques. En la práctica, no todo es previsible, ni todo lo previsible es económicamente razonable atajarlo en sus orígenes. Tanto para enfrentar lo desconocido como para protegerse de aquello a lo que se permanece expuesto, es necesario disponer de elementos que detecten el inicio de un incidente y permitan reaccionar con presteza impidiendo que se convierta en un desastre. Tanto las medidas preventivas como las de emergencia admiten una cierta degradación de los activos por lo que habrá que disponer por último de medidas de recuperación que devuelvan el valor perdido por los activos. Es de sentido común intentar actuar de forma preventiva para que las cosas no puedan ocurrir o no puedan causar mucho daño; pero no siempre es posible y hay que estar preparados para que ocurran. Lo que no debe ser de ninguna manera es que un ataque pase inadvertido: hay que detectarlo, registrarlo y reaccionar primero con un plan de emergencia (que pare y limite el incidente) y después con un plan de continuidad y recuperación para regresar a donde se debe estar. Por último, sin ánimo de saturar al lector, hay que recordar que conviene llegar a un cierto equilibrio entre:

- **Salvaguardas técnicas:** en aplicaciones, equipos y comunicaciones
- **Salvaguardas físicas:** protegiendo el entorno de trabajo de las personas y los equipos

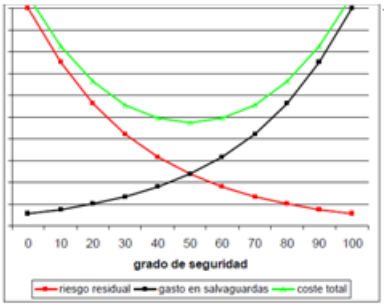


Figura 1: Pérdicas y Ganancias

- **Medidas de organización:** de prevención y gestión de las incidencias
- **Política de personal:** que, a fin de cuentas, es el eslabón imprescindible y más delicado: política de contratación, formación permanente, Organización de reporte de incidencias, plan de reacción y medidas disciplinarias.

2.6.3 *Pérdidas y Ganancias*

Es de sentido común que no se puede invertir en salvaguardas más allá del valor de los propios activos a proteger. Aparecen en la práctica gráficos como el siguiente que ponen uno frente al otro el coste de la inseguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas.

Este tipo de gráficas intentan reflejar cómo al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100 %, el coste de la inseguridad (el riesgo) disminuye, mientras que el coste de la inversión en salvaguardas aumenta. Es intencionado el hecho de que el riesgo caiga fuertemente con pequeñas inversiones y que el coste de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100 %. La curva central suma el coste para la Organización, bien derivado del riesgo (baja seguridad), bien derivado de la inversión en protección. De alguna forma existe un punto de equilibrio entre lo que se arriesga y lo que se inverte en defensa, punto al que hay que tender si la única consideración es económica.

2.6.4 *La Actitud de la Dirección*

La dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, ...) Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección 225. Si el impacto y/o el riesgo están por encima de lo aceptable, se puede: 1. eliminar el activo; suena muy fuerte, pero a veces hay activos que, simplemente, no vale la pena mantener26 2. introducir nuevas salvaguardas o mejorar la eficacia de las presentes .

2.6.5 *Revisión del Paso 1: Activos*

Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento que se convierte a su vez en un activo del sistema. Estos activos soportan parte del valor del sistema y están a su vez sujetos a amenazas que pueden perjudicar a los activos de valor. Hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la Organización.

2.7 SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

Esta norma fue especialmente creada para los organismos de telecomunicaciones, instalaciones de telecomunicaciones y redes. El Sistema de Gestión de la Seguridad de la Información ayuda a establecer políticas, procedimientos y controles que tienen que ver con los objetivos de negocio de la organización, su objetivo es minimizar riesgos propios de la organización. [7]

2.7.1 *Utilidad de un SGSI*

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

2.7.2 *Implementación de un SGSI*

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, es necesario definirse un modelo a seguir el más utilizado es la PDCA. Las fases de esta metodología son: Plan (planificar): establecer el SGSI. Do (hacer): implementar y utilizar el SGSI. Check (verificar): monitorizar y revisar el SGSI. Act (actuar): mantener y mejorar el SGSI.

Plan: Establecer el SGSI

Se debe definir el alcance del SGSI según las necesidades del negocio, la organización, su localización, activos y tecnologías.

Definir una política de seguridad

Según la metodología es necesario definir los siguientes lineamientos:

• Incluir el marco general y los objetivos de seguridad de la información de la organización;

• Considerar requerimientos legales o contractuales relativos a la seguridad de la información;

• Alinear con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;

• Establecer los criterios con los que se va a evaluar el riesgo;

• Que se apruebe por la dirección.

• Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.

Identificar los riesgos

La identificación requiere:

7 ISO27000.es.Sistema de Gestión de la Seguridad de la Información. Obtenido 20 noviembre de 2011, de http://www.iso27000.es/sgsi.html

• Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
• Identificar las amenazas en relación a los activos;
• Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
• Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

Analizar y evaluar los riesgos

Se necesita:

• Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
• Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
• Estimar los niveles de riesgo;
• Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
• Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
• Aplicar controles adecuados;
• Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
• Evitar el riesgo,
• Transferir el riesgo a terceros.

2.7.3 *Do: Implementar y Utilizar el SGSI*

De acuerdo a las recomendaciones de la metodología PDCA se debería tomar en cuenta los siguientes aspectos:

• Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
• Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
• Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
• Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
• Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
• Gestionar las operaciones del SGSI.
• Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
• Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

2.7.4 *Check: Monitorizar y Revisar el SGSI* [8]

La organización deberá:

Ejecutar procedimientos de monitorización y revisión para:

• Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
• Identificar brechas e incidentes de seguridad;

8 ISO27000.es.Sistema de Gestión de la Seguridad de la Información. Obtenido 20 noviembre de 2011, de http://www.iso27000.es/sgsi.html

• Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;

• Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;

• Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

• Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

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

• Realizar periódicamente auditorías internas del SGSI en intervalos planificados. • Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

• Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

• Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

2.7.5 *Act: Mantener y Mejorar el SGSI*

Según la metodología, la organización deberá regularmente:

• Implantar en el SGSI las mejoras identificadas.

• Realizar las acciones preventivas y correctivas adecuadas en relación a la claúsula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.

• Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.

• Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

Compromiso de la Dirección:

La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

• Establecer una política de seguridad de la información.

• Asegurarse de que se establecen objetivos y planes del SGSI.

• Establecer roles y responsabilidades de seguridad de la información.

• Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.

• Asignar suficientes recursos al SGSI en todas sus fases.

• Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.

• Asegurar que se realizan auditorías internas.

• Realizar revisiones del SGSI, como se detalla más adelante.

Asignación de Recursos

Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignan los suficientes para:

• Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.

• Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.

• Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.

• Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.

• Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.

• Mejorar la eficacia del SGSI donde sea necesario.

Formación y Concienciación

La formación y la concienciación en seguridad de la información son uno de los elementos más importantes para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas. Se deberá:

• Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.

• Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado.

• Evaluar la eficacia de las acciones realizadas.

• Mantener registros de estudios, formación, habilidades, experiencia y cualificación.

Además, la dirección debe asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

Revisión del SGSI

La dirección del comité de seguridad es el encargado de al menos una vez por año revisar la documentación del SGSI para que continúe siendo eficaz. Para ello, es necesario el levantamiento de información para una toma decisiones, entre las que se pueden enumerar:

• Resultados de auditorías y revisiones del SGSI.

• Observaciones de todas las partes interesadas.

• Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.

• Información sobre el estado de acciones preventivas y correctivas.

• Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.

• Resultados de las mediciones de eficacia.

• Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.

• Cualquier cambio que pueda afectar al SGSI.

• Recomendaciones de mejora.

3 SITUACIÓN ACTÚAL DE LA EMPRESA

3.1 DELIMITACIÓN DEL ALCANCE

3.1.1 *Misión*

Empresa con cultura de calidad, procesos efectivos, innovadas plataformas tecnológicas y colaboradores con certificaciones técnicas, comprometidos en satisfacer las necesidades integrales de telecomunicaciones, manteniendo la fidelidad de nuestros clientes. [1]

3.1.2 *Visión*

Brindar soluciones tecnológicas integrales, acercando nuestros clientes al mundo, porque sabemos como hacerlo.

3.1.3 *Características del Negocio*

La permanente evolución tecnológica en la que nos hallamos inmersos, hace que el mercado de las Telecomunicaciones constituya actualmente un factor diferenciador de éxito para las Empresas, es así como PuntoNet continuamente desarrolla nuevas soluciones de conectividad acordes a la demanda nacional, así como la inclusión de servicios multiplay, los que en ámbito mundial de las Telecomunicaciones se encuentran en pleno auge. Estamos seguros que contamos con la RED FISICA MAS ROBUSTA Y A PRUEBA DEL FUTURO del país, la cual es administrada por personal técnico certificado de primer nivel, lo que nos permite contar con un amplio portafolio de productos diseñados para soportar las necesidades de conectividad de hoy y del mañana.

3.1.4 *Servicios que Ofrece*

Voz sobre IP

Se presentan dos alternativas:

Contamos con un softswitch de clase 5 montado sobre una plataforma de hardware altamente redundante, lo que garantiza una óptima disponibilidad técnica y eficiencia económica tanto en llamadas locales como internacionales que el cliente requiera. Este producto posee las siguientes características:

- Integración con plataformas de telefonía convencional del cliente.
- Activación del sistema en puntos específicos de la red, sin hacer uso de la telefonía convencional.
- Plan de numeración personalizado.
- Enrutamiento de llamadas solo entre redes privadas. Seguridad y confidencialidad en las llamadas realizadas.

1 PUNTONET. Obtenido el 23 noviembre de 2011 de http://www.puntonet.ec

- Manejo de perfiles de usuario para el uso del sistema

Beneficios:

- Compatibilidad con el sistema de telefonía actual que el Cliente posea.
- Posibilidad de habilitar servicios propietarios de la telefonía tradicional como son: caller id, voice mail, multiconferencia, redireccionamiento de llamadas, llamadas en espera, grabación, entre otras.
- Creación de perfiles de usuario para optimizar el uso de la plataforma.
- Posibilidad de generar llamadas internacionales por medio de redes ip.
- Integración de servicios, voz, data y video en la infraestructura actual de la red lan del cliente.
- Generación de reporte de llamadas y CDR´s
- Soporte para cola de llamadas
- Libreta telefónica (Phone Book) con capacidad clic-to-call
- Versatilidad de crecimiento en hardware y software.

Banda Ancha

Productos orientados al mercado residencial, en los cuales usted podrá encontrar servicios de conexión ADSL, Wifi.

Datacenter

En nuestros Datacenters se puede hacer uso de los siguientes servicios: Virtualización, Hosting, Housing, Correo Electrónico, respaldos de la información crítica para la empresa, publicación de servicios en línea (real audio y real video). En los Datacenters usted encontrará:

- Estricta seguridad tanto física como lógica en el acceso.
- Sistema de servidores en modalidad clusters.
- Energía y temperatura regulada.
- Escalabilidad ilimitada.
- Soporte técnico en línea y personal calificado.
- Asesoría en la implementación de nuevas soluciones.
- Backbone de acceso redundante de alta velocidad.

Transmisión de Datos

Diseñar la solución que más se acople a sus necesidades tanto económicas como tecnológicas, con lo que obtendrá beneficios como:

- Integración entre sus oficinas dispersas geográficamente funcionando como una red única.
- Centralización de operaciones y control de información.
- Toma de decisiones oportunas en base a los datos obtenidos.
- Convergencia de servicios (voz, datos y video) en una sola plataforma.
- Optimización de Recursos al contar con plataformas de hardware centralizada.
- Seguridad de la información.
- Mínimo riesgo de obsolescencia en equipamiento ya que este es provisto por PuntoNet.
- Asistencia técnica las 24 horas del día.
- Asesoría permanente en la mejora de proyectos actuales e implementación de nuevos.
- Corto tiempo de instalación y puesta en marcha de la solución.

Internet

Ponemos a su disposición, nuestros productos, en los que encontrará:

- Conexión permanente 24 horas al día.
- Transferencia ilimitada de datos.
- Ancho de banda garantizado.
- Alta disponibilidad.
- Escalabilidad inmediata.
- Seguridad y confidencialidad en la transmisión y recepción de datos.
- Soporte para creación y configuración de vpn´s.
- Baja latencia.
- Enlaces basados en tecnología de última generación que posibilita la integración a redes multiservicios.

Sistemas Satelitales

La globalización de las Telecomunicaciones ha convertido a los sistemas satelitales en una herramienta fundamental e indispensable para la universalización de redes y servicios, ya que constituyen el vehículo ideal para llevar las comunicaciones a entornos rurales, de difícil acceso o en zonas con poca disponibilidad de conexión a red terrestre. Contamos con soluciones que van acorde a sus necesidades de su empresa tanto en Transmisión de datos como Acceso a Internet, en los que encontrará:

- Cobertura en localizaciones de difícil acceso.
- Conexión permanente 24 horas al día.
- Flota Satelital con tecnología de vanguardia
- Equipamiento con los más altos estándares en la industria satelital.
- Soporte y monitoreo en línea.
- Personalización de aplicaciones
- Plataforma tecnológica y logística propietaria que agilita los tiempos de instalación y soporte.

3.1.5 *Diagrama Organizacional*

La empresa actualmente cuenta con la siguiente organización jerárquica y funcional como se muestra en la figura 3.1 2. El diagrama organizacional está realizado en base a entrevistas al personal de la organización.

3.1.6 *Grado de Penetración Nacional*

La acogida entregada tanto a nuestros productos y servicios así como a nuestro personal, nos ha permitido expandir la cobertura a lo largo del país. Actualmente contamos con POP'S PRIMARIOS (Puntos de Presencia) con oficinas técnicas comerciales y POP'S SECUNDARIOS que poseen personal técnico dispuesto a ofrecer un adecuado y oportuno soporte.

3.1.7 *Ubicación y Area de Cobertura*

3.1.8 *Procesos*

Se reconocen tres areas fundamentales del negocio: el area administrativa, de ventas y técnica, en donde se efectúan los principales procesos necesarios para la realización de labores diarias con la finalidad de cumplir con las metas de la empresa.

El área administrativa está encargada de procesos como el registro de clientes, facturación y post venta; estos procesos hacen uso de los

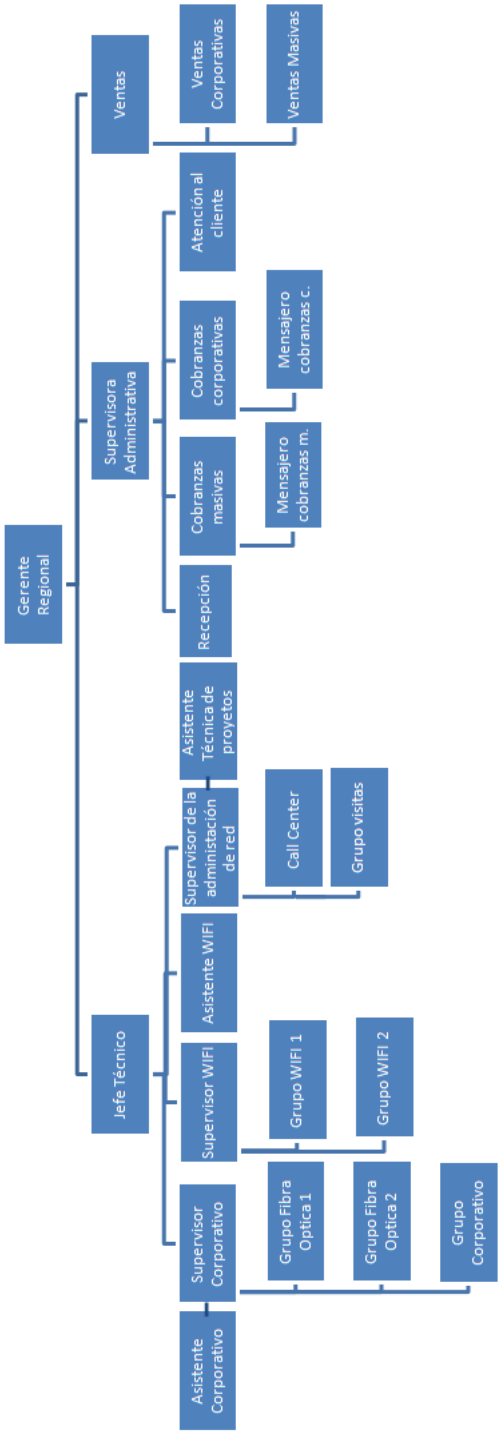


Figura 2: Diagrama Organizacional Fuente: PUNTONET

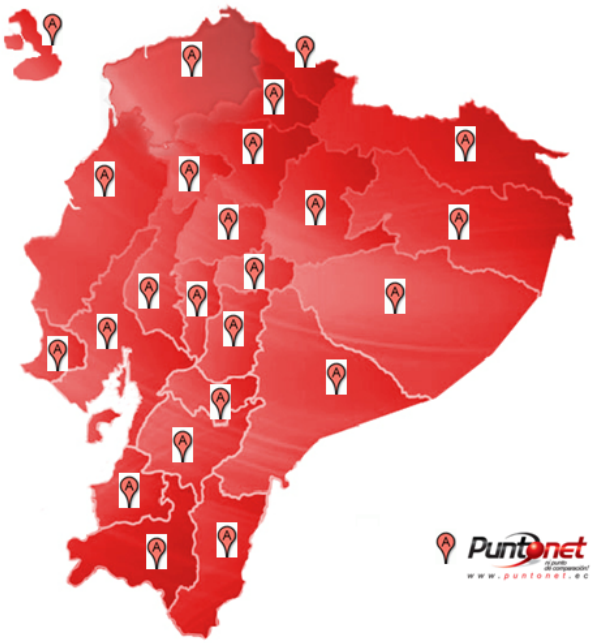


Figura 3: Ubicación y Area de Cobertura Fuente: PUNTONET

Función del negocio: **Administrativo**		
Registro Clientes	**Facturación**	**Post Venta**
Netplus	Netplus	Personal Administrativo
Personal de Ventas	Personal Administrativo	Netplus
Personal Administrativo	Clientes	Clientes
Clientes	Red de datos	Red de datos
Red de datos	Proxy	Proxy
Proxy		

Cuadro 1: Función del negocio: Administrativo Fuente: PUNTONET

Función del negocio: **Ventas**	
Atención al cliente	**Comercialización**
Netplus	Personal de Ventas
Clientes	Clientes
Red de datos	Red de datos
Proxy	Proxy
Asterisk	Asterisk

Cuadro 2: Función del negocio: Ventas Fuente: PUNTONET

Función del negocio: **Técnico**				
Instalación	**Monitoreo**	**Mantenimiento**	**Administración red**	**Soporte Técnico**
Personal Técnico	Syscorp	Bodega	Email	Syscorp
Bodega	Personal Técnico	Personal Técnico	Asterisk	Netplus
Clientes	Proveedores	Personal Standby	Personal Técnico	Personal Técnico
Nodos Corpora.	Email	Proveedores	Red de datos	Personal Standby
Nodos WIFI	Personal Standby	Nodos Corpora.		Clientes
Email	Proxy	Nodos WIFI		Baterias
Router Principal	Cacti	Servidor WIFI		Generadores E.E
Switch principal	Nagios			Equipos monitoreo
Servidor WIFI	Solarwinds			
Netplus	Reportes monitoreo			
Dialup				
Syscorp				
Anillo fibra óptica				
Internet				

Cuadro 3: Función del negocio: Técnico Fuente: PUNTONET

activos que se indican en el cuadro 3.1 1. Los datos de cada proceso se obtuvieron mediante entrevistas al personal de la empresa.

En el área de ventas se reconocen dos procesos: la atención al cliente y la comercialización, cuyos activos necesarios están indicados en el cuadro 3.2 2

El área técnica encargada de brindar soporte y asistencia a los clientes maneja cinco procesos imprescindibles que son: la instalación, monitoreo, mantenimiento, administración de red y soporte técnico, dentro de los cuales se requiere gran parte de los activos que maneja la empresa, tal como se indica en el cuadro 3.3 3.

Una amplia descripción de cada uno de los procesos mencionados se puede encontrar en el cuarto capítulo IV "Identificación de procesos realizados en la organización".

3.1.9 *Activos*

En el cuadro 3.4 4 se listan los principales activos de la organización que permiten cumplir con los procesos ya mencionados. Estos activos han sido categorizados según el tipo de activo al que pertenecen, para ello se ha tomado como referencia lo expuesto en la metodología

HARDWARE	Equipos de monitoreo
	Nodos corporativos
	Nodos WIFI
	Servidor WIFI
	Servidor de Email
	Asterisk
	Proxy
	Router principal
	Switch principal
SOFTWARE	Sistema Netplus
	Sistema Syscorp
	Sistema Dialup
	Cacti
	Solarwinds
	Nagios
DATOS	Reportes Monitoreo
EQUIPAMIENTO AUXILIAR	Generadores de Energía Eléctrica
	Baterías
RED DE COMUNICACIONES	Anillo de fibra óptica
	Red de datos
PERSONAL	Clientes
	Proveedores
	Personal Técnico
	Personal de ventas
	Personal Standby
	Personal administrativo
INSTALACIONES	Bodega
SERVICIO	Internet

Cuadro 4: Principales activos Fuente: PUNTONET

MAGERIT dentro del catálogo "Identificación de Activos"expuesto en el ANEXO A. Los datos expuestos se obtuvieron mediante entrevistas al personal de la organización.

A continuación se presenta una breve descripción de los activos:

- **Equipos de monitoreo (Monitor).-** equipo destinado para el monitoreo de enlaces, un CPU y una pantalla, en el que se encuentran instalados los programas para monitoreo de la red, los mismos que se encargan de asegurar el correcto funcionamiento de la redes en la productividad y eficiencia de la empresa. Al disponer de un equipo encargado de monitorear los problemas presentados en la red, permite corregirlos a tiempo y a su vez prevenir posteriores inconvenientes que podrían afectar el desarrollo de la empresa.

- **Nodos Corporativos.-** antenas y bases que sirven de backhaul para los clientes corporativos. Es decir, es el punto de retrasmisión.

Estos nodos se encuentran en zonas estratégicas de la ciudad para poder tener una mayor área de cobertura; nodos como el Nodo Barabón, Nodo Rayoloma, Nodo Hitocruz, y Nodo Oficina (ubicación Av. Remigio Crespo).

- **Nodos WIFI.-** sirven de backhaul para los clientes WIFI. También estos nodos están ubicados por zonas en la ciudad de Cuenca y uno en Azogues. Brindan servicio a los clientes residenciales.
- **Servidor WIFI.-** en este se encuentra la configuración de los distintos nodos WIFI.
- **Servidor Email.-** es el servidor de correo interno de la empresa, cuya finalidad es comunicar los diferentes sucesos a los empleados.
- **Asterisk.-** es el servidor de telefonía interna; este permite iniciar y administrar llamadas internas; además permite la conexión a otros servicios de telefonía, incluyendo la red telefónica pública conmutada (PSTN).
- **Proxy.-** sirve de intermediario entre una petición de un usuario hacia su destino, es decir en lugar de que una petición vaya a su destino directamente, deberá pasar por el servidor proxy. Trae muchas ventajas como el control, velocidad, ahorro y filtrado.
- **Sistema Netplus.-** sistema que permite:

1. Llevar un registro de todos los clientes.
2. Presentar información sobre los equipos asignados a los clientes.
3. Presentar información relacionada a los empleados que labora en la empresa.
4. Controlar todos los procesos y requerimientos generados por los clientes (instalaciones, desinstalaciones, upgrades, visitas técnicas, gestión cobranzas).
5. Asignar tareas al personal encargado para los diferentes requerimientos de los clientes.
6. Asignar los equipos a los empleados.
7. Llevar un inventario de los equipos destinados para las instalaciones.

- **Sistema Syscorp.-** sistema que contiene la información de los clientes corporativos y de los nodos. Esta información comprende detalles sobre tecnologías, ips de red, equipos instalados, datos del cliente, Gateway, etc.

- **Sistema Dialup.-** Sistema en el cuál se registran las direcciones mac para los clientes de hogares o clientes wifi; se registra el ancho de banda y la ip.
- **Cacti.-** Sistema que sirve para el monitoreo de los enlaces mediante la generación de gráficos de red. Además brinda métodos para la recopilación de datos y manejo de usuarios.

Figura 4: Sistema Netplus - Departamento Técnico Fuente: PUNTONET

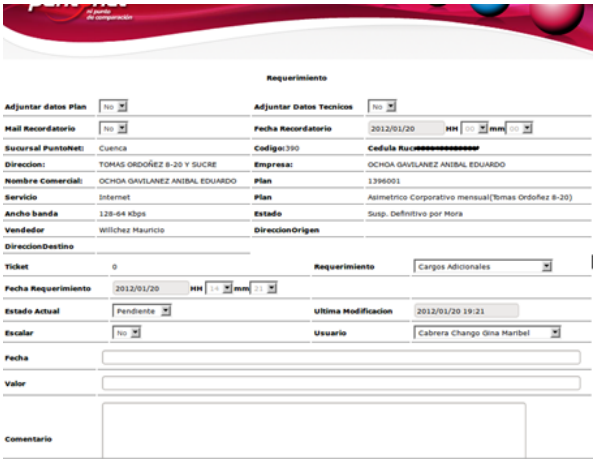


Figura 5: Sistema Netplus - Requerimientos Fuente: PUNTONET

CLIENTE

puntonet

Anotar Llamada | MRTGs | Inspección

Estado

SUCURSAL NETPLUS | CODIGO NETPLUS 0 | Buscar

NOMBRES NETPLUS

PLAN NETPLUS

CODIGO SISCORP 12188 | GRUPO Clientes

EMPRESA NODO WIFI CENTRO 1

DNS

CONTACTO Hector Francisco Bravo Zuñiga | CIUDAD Cuenca

DIRECCIÓN HUMBOLT 2-42 y AV. DE LA AMERICAS | INSTALADOR Diestra Paul

TELEFONOS 2848093/099675942 | EJECUTIVO CUENTA Willchez ,Mauricio

EMAIL | EJECUTIVO TECNICO Diestra ,Paul

DOMINIO | FECHA INSTALACIÓN 2010-03-01

VELOCIDAD ENLACE Radio PuntoNet 1MB | PROV.ULT.MILLA/TECNOLOGIA Mikrotik

TIPO ANTENA Antena Externa | NIVEL COMPARTICION 6 a 1

LATITUD Sur | 02 ° 53 ' 11,2 "

LONGITUD Oeste | 79 ° 00 ' 55,7 "

ALT. SOBRE NIVEL MAR 2615

DIRECCION RED [redacted] | MASCARA [redacted]

GATEWAY [redacted] | IP_ENLACE [redacted]

ROUTER CENTRAL (IP) [redacted] | DLCI/PVC/TS/VLAN: [redacted]

IPS_DISPONIBLES

DESDE | HASTA

SO. SERVER | SOFTWARE PROXY:

CLAVE OPERADOR: | CLAVE ROOT:

USUARIO MRTG wificentro | CLAVE MRTG wificentro

PUERTO/MAC/IP PROST 2 | IP SERVIDOR

SNMPID 1 | CODIGO EMPRESA

TODO INCLUIDO No | CODIGO ATDATOS

Comentario

base 1 [redacted] 20 Mhz

base 2 [redacted] 10 Mhz

Monitoreo | Alarma

Figura 6: Sistema Syscorp Fuente: PUNTONET

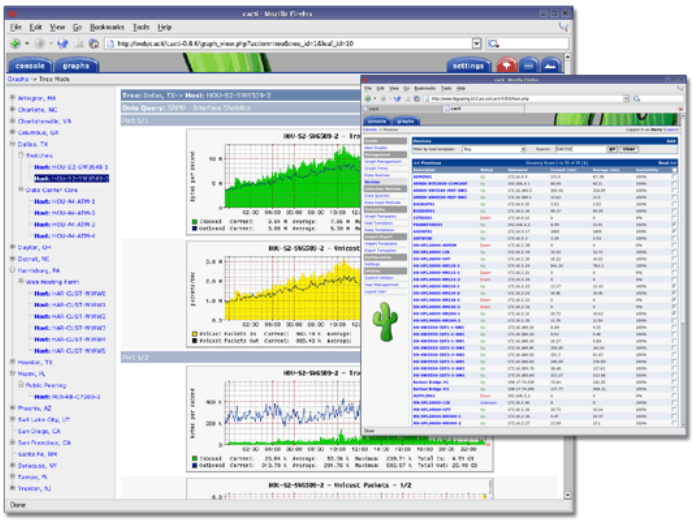


Figura 7: Software de Monitoreo Cacti Fuente: PUNTONET

- **Solarwinds.-** sistema de monitoreo y alarmas sonoras; este sistema monitorea y recoge datos de routers, switches, servidores, y cualquier otro dispositivo de red con capacidad SNMP.
- **Nagios.-** sistema de monitoreo de enlaces y estados de red. Monitorea la red, vigila los equipos y servicios que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red.
- **Reportes de monitoreos.-** reportes realizados para indicar el estado de un enlace. Así como su comportamiento, disponibilidad y uptime.
- **Generadores de Energía Eléctrica.-** colocados en los nodos y en las bases. En caso de que un nodo tenga una falla de energía el generador comenzará su funcionamiento, garantizando así que el nodo no tenga fallos.
- **Baterías.-** cumple con una función semejante a la de un generador. Respalda el funcionamiento de un nodo en caso de haber una falla eléctrica.
- **Router principal.-** es usado para la interconexión de la red y para determinar la mejor ruta.
- **Switch principal.-** en este switch están configurados todos los enlaces con los que se trabaja, así como la interconexión de los mismos.
- **Anillo de fibra óptica.-** es el tendido de fibra óptica que posee la empresa; provee enlaces más robustos, así como de mayor velocidad.
- **Internet.-** servicio que la empresa ofrece.
- **Red de datos.-** comprende todo el conjunto de sistemas y equipos informáticos conectados entre sí, el cual sirve para enviar o recibir un determinado flujo de información que pretende servir al objetivo del negocio.
- **Clientes.-** personas a las que se les brinda el servicio de internet o telecomunicaciones.
- **Proveedores.-** encargados de brindar el servicio de internet para luego distribuirlo; permiten la salida internacional.
- **Personal Técnico.-** personal o empleados del área técnica encargados de la parte operativa del negocio.
- **Personal de Ventas.-** personal encargado de asesorar a los clientes en el proceso de contratación y adquisición del servicio.
- **Personal Standby.-** personal que en turnos rotativos tiene que estar disponible las 24 horas del día para resolver cualquier eventualidad ya sea en los enlaces corporativos, o en los nodos.
- **Personal Administrativo.-** personal o empleados encargados de cobros, facturación y demás tareas administrativas.
- **Bodega.-** ubicación en donde se alojan los equipos. Esta comprende todos los equipos necesarios para instalaciones.

Valor		Criterio
10	muy alto	**daño muy grave a la organización**
7-9	alto	**daño grave a la organización**
4-6	medio	**daño importante a la organización**
1-3	bajo	**daño menor a la organización**
0	despreciable	**irrelevante a efectos prácticos**

Cuadro 5: Criterios de valoración de activos Fuente: MAGERIT

Valoración de los Activos

Como se muestra en el cuadro 3.6 6 la valoración que recibe un activo representa la magnitud de la degradación de un activo en una dimensión específica.

Para la valoración de cada activo conviene registrar la siguiente información:

- Dimensiones en las que el activo es relevante: las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.
  - **Disponibilidad D:** asegurar que únicamente los usuarios autorizados accedan en todo momento a la información.
  - **Integridad I:** garantizar que la información sea exacta y completa.
  - **Confidencialidad C:** proteger que la información sea accedida solo por usuarios autorizados.
  - **Autenticidad A:** asegura la identidad u origen.
  - **Trazabilidad T:** asegurar que se podrá saber quién y en qué momento se modificó la información.
- Estimación de la valoración en cada dimensión: para la estimación es necesario tomar como referencia lo expuesto en el cuadro 3.5 5.

La valoración de cada uno de los activos se obtuvo mediante encuestas realizadas al personal que labora en las diferentes áreas de la organización; áreas indicadas en el ANEXO 1 "Valoración de los Activos".

3.2 DECLARACIÓN DE APLICABILIDAD

En cuanto a políticas de seguridad están en proceso de implementación, pero actualmente no se cuenta con documentos formales que las respalden, al igual que no se realiza ninguna revisión por parte de las autoridades o de los responsables. Se lleva actualmente una organización interna para la seguridad delegando esto a personas específicas. Las responsabilidades sobre los activos de la empresa están delegadas a personal según el cargo que ejercen, de esta forma se distribuyen cargas. En cuanto a la información, esta no dispone de guías de clasificación, al igual que no se cuenta con un procedimiento para la destrucción de la misma.

	Dimensiones de Seguridad				
ACTIVO	**D**	**I**	**C**	**A**	**T**
HARDWARE					
Equipos de monitoreo	8	7			
Nodos corporativos	9	8			
Nodos WIFI	9	8			
Servidor WIFI	9	8	9	8	7
Servidor de Email	9	9	9	8	8
Asterisk	9	6	6	7	7
Proxy	7	6	6	6	5
Router principal	10	10	10	8	9
Switch principal	9	9	9	9	9
SOFTWARE					
Sistema Netplus	10	8	8	9	9
Sistema Syscorp	7	6	7	7	7
Sistema Dialup	9	9	9	8	8
Cacti	8	7	7	6	6
Solarwinds	8	7	7	6	6
Nagios	8	7	7	6	6
DATOS					
Reportes Monitoreo	7	8			
EQUIPAMIENTO AUXILIAR					
Generadores de Energía Eléctrica	10	7			
Baterías	8	7			
RED DE COMUNICACIONES					
Anillo de fibra óptica	8	8	9		
Red de datos	10	7	7		
PERSONAL					
Clientes	10				
Proveedores	9				
Personal Técnico	9		8		
Personal de ventas	9		8		
Personal Standby	9		8		
Personal administrativo	9		8		
INSTALACIONES					
Bodega	10	8			
SERVICIO					
Internet	9	7	7		

Cuadro 6: Valoración de los Activos Fuente: PUNTONET

Dentro de los procedimientos existentes se puede mencionar los respaldos de los equipos más sensibles, planes de contingencia de equipos como: router principal, switch principal, servidor de correo.

Así como también cuenta con los planes de contingencia para los nodos tanto corporativos como WIFI, estos planes tienen personal designado para hacerlos cumplir. Las personas encargadas de mantener estos planes de contingencia se encuentran en constante actualización y son responsables de que estos se cumplan.

3.3 POLÍTICAS Y PROCEDIMIENTOS

La política de la empresa se rige a la matriz en Quito, se cuenta con políticas para las diferentes áreas. [2]

Los procedimientos se van creando dentro de las distintas áreas, según el personal vaya desarrollando sus actividades. Luego de aplicar la respectiva corrección se realiza una revisión para determinar si se están dando las mejoras respectivas. Son los supervisores y jefes los encargados de verificar que estos procedimientos y políticas se estén cumpliendo así como los responsables de las sanciones si es que estas no se llegan a cumplir.

Dentro de los procedimientos para medidas preventivas se los realiza mediante Excel, el mismo que permite ver como se están mejorando las falencias existentes.

3.4 PLAN DIRECTOR DE SEGURIDAD

La empresa cuenta con un Plan director de seguridad. Existen medidas correctivas para los procesos que no se están llevando a cabo de una forma correcta, se lo realiza mediante reuniones con las personas involucradas, o enviando un informe vía mail.

El plan de seguridad se encuentra en desarrollo, así como sus dependencias, poco a poco se ha ido delegando al personal que apoye este proyecto.

3.5 PLAN DE CONTINUIDAD DE NEGOCIO

Existen planes de contingencia para eventos críticos o inesperados. Para cada activo importante se tiene un plan de contingencia, cada uno de los cuáles tiene una persona encargada.

Los planes de contingencia conforman uno de los pilares fundamentales para la empresa, ya que garantizan se lleve con eficiencia el objetivo del negocio que es un buen servicio al cliente.

3.6 PLAN DE FORMACIÓN

Se maneja un plan de formación de personal para conocer y cumplir las medidas de seguridad establecidas.

Se trata de mantener al personal capacitado, especialmente a los que se encuentran más ligados a funciones técnicas, para de esta manera poder dar un mejor y eficiente servicio a los usuarios del servicio. [3]

---

2 Capítulo 4. Análisis de Riesgos. Sección 4.1 "Identificación de procesos realizados en la organización"

3 Capítulo 4. Análisis de Riesgos. Sección 4.1 "Estudio de las actividades para cada uno de los procesos"

3.7 GESTIÓN DE INCIDENTES

Se dispone de procedimientos básicos para la gestión de incidentes, es decir se toma en cuenta los activos más sensibles para darles mayor protección frente a riesgos. Son los supervisores los que se encargan de revisar y evaluar posibles vulnerabilidades para de esta forma minimizar la interrupción del servicio.

3.8 AUDITORIA INTERNA

Las auditorías se las realiza cuando desde la matriz (Quito) se informa que se va a realizar una auditoría interna, los mismos que se encargan de establecer el tiempo en el cual se va a realizar la auditoría. Los procedimientos para medidas correctivas se los realiza mediante una revisión por parte del personal involucrado en a donde se analiza el problema con fecha límite para la corrección y reporte. Toda esta información no se la lleva en registros.

La auditoría es una parte fundamental dentro de una organización, ya que de una u otra manera obliga a que todas las distintas áreas estén preparadas.

4 ANÁLISIS DE RIESGOS

Un informe detallado sobre diferentes metodologías de Análisis de Riesgos, así como el porqué de la metodología a emplear para nuestro proyecto, lo podemos ver en el ANEXO 1 "Metodología de Análisis de Riesgos".

4.1 IDENTIFICACIÓN DE PROCESOS REALIZADOS EN LA ORGANIZACIÓN

Función del Negocio: Administrativo

Registro Clientes

Al momento en que un nuevo cliente adquiere los servicios de la empresa se ingresa un nuevo contrato, el cual se registra en el sistema NetPlus con todos los datos pertinentes al cliente y a la contratación del servicio, especificando todos los detalles técnicos y del contrato.

Esta información es uno de los activos más importantes de la empresa ya que constituye la esencia del negocio, que son los clientes.

Post Venta

Luego de que el cliente adquirió el servicio, se le brinda el soporte necesario para verificar su conformidad. Comprende todo aquello que ocurre después de la venta: soporte técnico, aplicación de garantía y manejo de quejas.

Facturación

El sistema de facturación se encarga de llevar los procesos económicos y financieros de la empresa, como los cobros, ventas, etc. Los encargados de manejar está información son el personal del área comercial. Ya que los accesos a este tipo de información lo tendrá únicamente el personal autorizado.

Función del Negocio: Ventas

Atención al cliente

El agente de ventas es el encargado de contactarse con el cliente e indicarle todas las características del servicio, así como de la contratación. Él también está encargado de llevar a cabo una inspección, para constatar si es o no factible instalar en el lugar, e ingresar todos los datos necesarios para su posterior registro.

Comercialización

Se enfoca a la publicidad que se den a los servicios que brinda la empresa, sean estos mediante contactos, publicidad visual o auditiva.

Función del Negocio: Técnico

Instalación

Una vez pasado el requerimiento de instalación al área técnica, se procede a asignar a un grupo de personal técnico que se dirija hasta el lugar de instalación.

A este personal encargado, se le asigna los equipos necesarios para proveer el servicio como por ejemplo cable, antenas y demás.

Una vez instalada la parte física se solicita al personal de la oficina, se registre toda la parte lógica de la red como ip, registro de la mac en cada nodo en caso de ser una instalación para hogares, caso contrario las configuraciones necesarias en caso de ser una instalación corporativa.

Se deben realizar pruebas conjuntas del personal de oficina, como del personal de instalaciones, pruebas como latencia del enlace, velocidad, ancho de banda, etc.

Luego de estas pruebas se harán las respectivas demostraciones al cliente, donde aprobará o no la instalación.

Monitoreo

El Sistema de monitoreo es una parte esencial en los procesos de la empresa, está encargado de garantizar la disponibilidad de los enlaces.

Está implementado un sistema de monitoreo con Nagios de todos los enlaces, al igual que un sistema de alarmas sonoras y monitoreo con Solarwinds de donde se pueden obtener reportes sobre el estado de cada enlace.

El personal asignado del monitoreo deberá estar pendiente de que todo esté funcionando correctamente, así como de comunicarse y dar una solución en caso de que un enlace tenga inconvenientes o no esté operacional.

Se deben seguir procedimientos para revisar los enlaces y realizar las respectivas pruebas con los clientes.

Mantenimiento

Se tiene que dar un mantenimiento de las diferentes bases y nodos así como de los routers, switchs baterías, etc.

Esto se realiza con la finalidad de evitar caídas por fallas eléctricas o mecánicas.

Administración de Red

La persona encargada de la administración de la red tiene que garantizar el correcto uso y gestión de los recursos, para que estos sean utilizados de manera más eficiente, tiene que garantizar una red interna saludable.

La persona encargada de la administración de la red también debe encargarse de que servidores estén funcionando correctamente, así como aplicaciones, la centralilla telefónica del Asterisk, la instalación del sistema operativo, la instalación de software de aplicación, la administración de redes debe controlar tanto a los usuarios como a sus contraseñas para ingresar en el sistema; instalar un hardware que pueden ser por ejemplo, tarjetas, impresoras, terminales y módems; también debe diagnosticar y reparar aquellos problemas que puede llegar a presentar el software.

Soporte Técnico

Cuando un cliente necesita que se le asesore en algún problema técnico que se esté presentando netamente en el servicio ya sea de internet o de enlace de datos, se sigue una serie de procedimientos para llegar a detectar cuál es el inconveniente, si el problema resulta ser una falla por parte de los servicios de la empresa, se procede a realizar cambios en los equipos o a buscar una solución. Si el problema se soluciona, se llena un informe indicando problema y solución para un posterior control y respaldo del soporte. Caso contrario si no se solucionó remotamente, se procede a enviar una visita técnica, es decir un grupo de técnicos que se dirijan hasta el punto y revisen físicamente los equipos. Si se soluciona de esta forma se debe de igual manera entregar un informe del porque el problema y cuál fue la solución que se le ofreció al cliente, esto para garantizar una buena calidad en el servicio y un buen soporte técnico.

4.2 ESTUDIO DE LAS ACTIVIDADES QUE SE REALIZA PARA CADA UNO DE LOS PROCESOS

Para cumplir el objetivo de negocio se deben llevar a cabo diariamente una serie de procesos de los cuales dependerá el éxito o fracaso de la organización. Los datos presentados a continuación han sido obtenidos a través de varias entrevistas realizadas al personal involucrado en las actividades diarias, donde se detallan las mismas.

Registro Clientes

Una vez que el cliente solicita alguno de los servicios que ofrece la empresa se lleva a cabo estas actividades de la figura 4.1 8

Post Venta

Una vez realizada la instalación al cliente, se procede a generar el proceso de Facturación de la figura 4.2 9, para en lo posterior verificar si la instalación y el funcionamiento del servicio contratado es el óptimo.
Facturación

Dentro de este proceso se indica paso a paso las actividades necesarias para efectuar la facturación de servicios brindados por parte de la empresa indicados en la figura 4.3 10.
Atención al Cliente

Realizar la atención al cliente se la puede lograr por las siguientes vías: ya sea que el cliente se dirija a la oficina de la empresa, mediante una llamada telefónica, envió de un email indicando el inconveniente o a través de una de la red social: Facebook. Para ello se puede observar los siguientes pasos de la figura 4.4 11
Comercialización

Como es de nuestro conocimiento la empresa da a conocer los servicios que brinda, para ello es necesario disponer de contactos a los

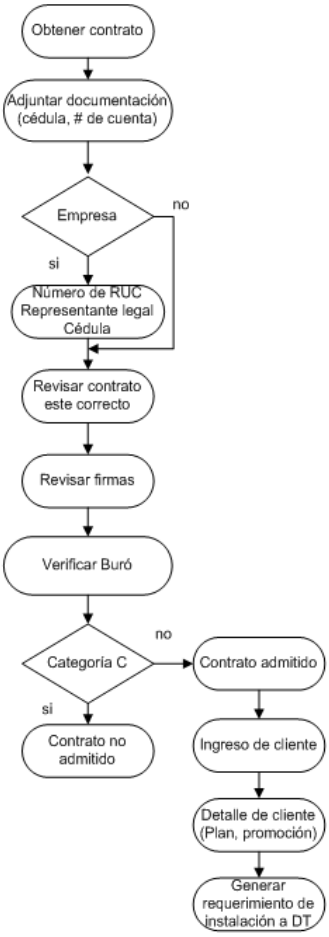


Figura 8: Actividades para el proceso Registro de Clientes

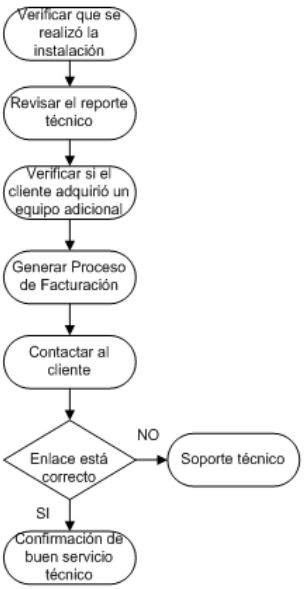


Figura 9: Actividades para el proceso de Post Venta Fuente: Puntonet

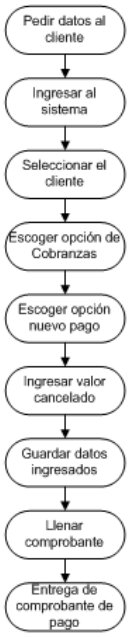


Figura 10: Actividades para el proceso de Facturación Fuente: Puntonet

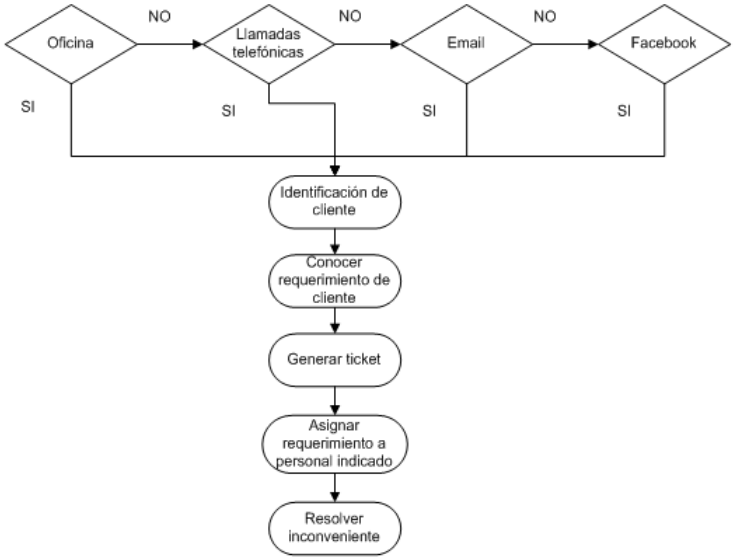


Figura 11: Actividades para el proceso de Atención al Cliente Fuente: Puntonet

Figura 12: Actividades para el proceso de Comercialización Fuente: Puntonet

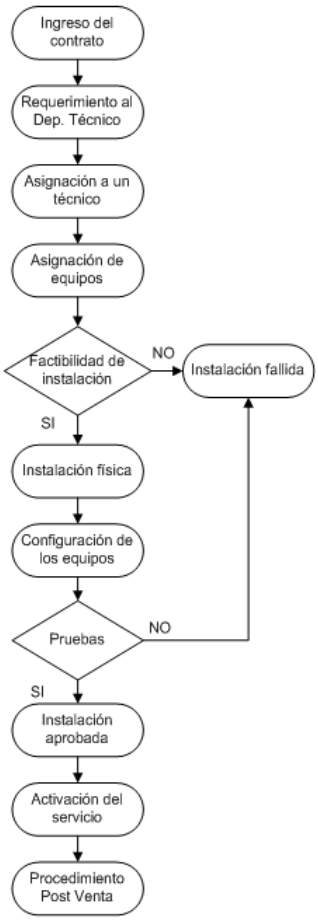


Figura 13: Actividades para el proceso de Instalación Fuente: Puntonet

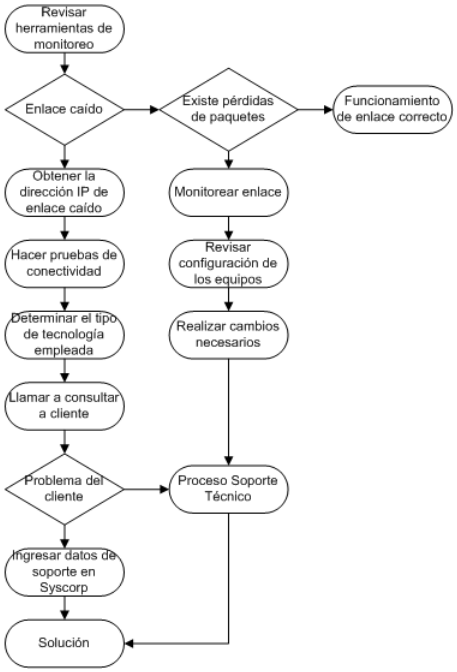


Figura 14: Actividades para el proceso de Monitoreo Fuente: Puntonet

que se pueda llegar para ofertar los servicios tal como se detalla en la figura 4.5 12.

Instalación

Para la instalación de equipos según los requerimientos del cliente se describe la siguiente secuencia de actividades de la figura 4.6 13:

Monitoreo

Para mantener un control de los enlaces es necesario disponer de herramientas de monitoreo, con la finalidad de mantener así la disponibilidad del servicio. Se deben seguir estas actividades para revisar

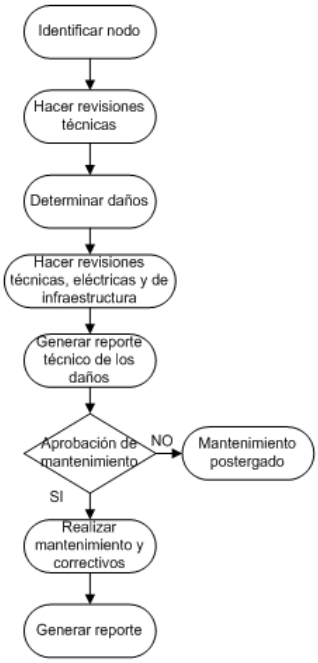


Figura 15: Actividades para el proceso de Mantenimiento Fuente: Puntonet

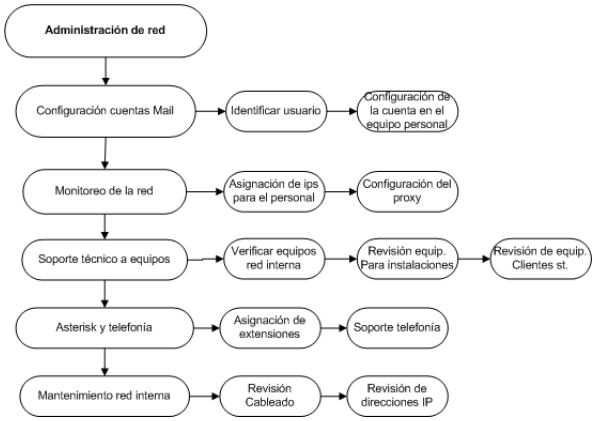


Figura 16: Actividades para el proceso de Administracion de Red Fuente: Puntonet

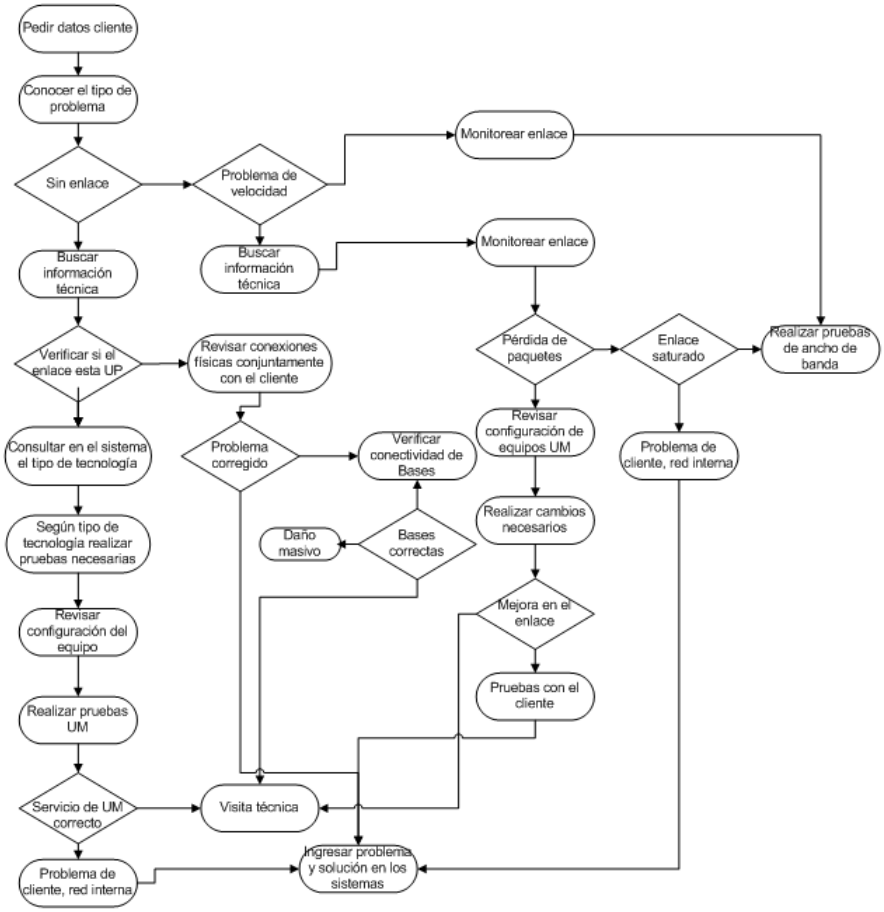


Figura 17: Actividades para el proceso de Soporte Técnico Fuente: Puntonet

los enlaces y realizar las respectivas pruebas con los clientes como se indica en la figura 4.7 14.
Mantenimiento

Para realizar el mantenimiento se especifican las actividades de la figura 4.8 15.
Administración de Red

Dentro de la red interna se requiere también una administración que a continuación se presenta en la Figura 4.9 16
Soporte Técnico

Al realizar el proceso de soporte técnico se lleva a cabo una extensa secuencia de pasos indicados en la figura 4.10 17 para lograr corregir el daño y reanudar el servicio al cliente.

4.3 ANÁLISIS DE RIESGOS

4.3.1 *Caracterización de los Activos*

Dentro de la actividad de caracterización de los activos, se identifican los principales activos que maneja o de los que dispone la empresa, para luego determinar la dependencia existente entre los mismos. Al ser identificados estos activos pueden ser valorados en las diferentes dimensiones de seguridad.
Identificación de los Activos

Al realizar la identificación de un activo se determinan sus características y atributos, como son un código, nombre y la descripción, descritos en el cuadro 4.1 7. Dentro de la metodología se especifican diferentes clases de activos a los que se les puede asociar un activo, en base al "Catálogo de Identificación de Activos" del ANEXO A.

A continuación se presentan los activos esenciales para el proyecto, como se puede observar en la figura 4.11 18
Dependencias entre Activos

En esta tarea se identifican las dependencias entre los activos, como se indica en el cuadro 4.2 8, se les podría asignar un valor que no es más que el grado de dependencia en que un activo superior se puede ver afectado por una falla de seguridad en un activo inferior, como se puede ver en la figura 4.13 19.
Valoración de los Activos

Esta tarea se ve relacionada con los pasos mencionados anteriormente como son la identificación de los activos y las dependencias entre los mismos. Al realizar la valoración de los activos, se identifica las dimensiones en las cuales el activo es considerado valioso, en donde el valor representa el coste de destrucción del activo como se observa en la figura 4.13 20.

Para realizar esta tarea se hace uso de la "Escala de criterios de valoración" del cuadro 4.3 9.

En el cuadro 4.4 10, se presentan criterios de valoración adicionales recomendados por MAGERIT para agregar calificaciones importantes, como en el caso de la disponibilidad en donde se puede medir las consecuencias en base al tiempo de interrupción del activo.

(1) [7.adm]Administración y gestión: probablemente impediría la operación efectiva de la organización

SUBCAPA	ACTIVOS
[HW] HARDWARE	[equiposMoni] Equipos de monitoreo
	[nodoC] Nodos corporativos
	[nodoW] Nodos WIFI
	[servidorWifi] Servidor WIFI
	[servidorEmail] Servidor de Email
	[servidorAsterisk] Asterisk
	[servidorProxy] Proxy
	[router] Router principal
	[switch] Switch principal
[SW] SOFTWARE	[netplus] Sistema Netplus
	[syscorp] Sistema Syscorp
	[dialup] Sistema Dialup
	[cacti] Cacti
	[solarwinds] Solarwinds
	[nagios] Nagios
[D] DATOS	[reportes] Reportes Monitoreo
[AUX] EQUIPAMIENTO AUXILIAR	[gen]Generadores de Energía Eléctrica
	[bate]Baterías
[COM] RED DE COMUNICACIONES	[fibraOptica]Anillo de fibra óptica
	[redDatos]Red de datos
[S] SERVICIOS	[Internet]Internet
[P] PERSONAL	[clientes] Clientes
	[prov] Proveedores
	[personalTec] Personal Técnico
	[personaVent] Personal de ventas
	[personalStan] Personal Standby
	[personalAdmin] Personal administrativo
[L] INSTALACIONES	[bodega] Bodega

Cuadro 7: Identificación de los activos en las diferentes subcapas Fuente: LAS AUTORAS

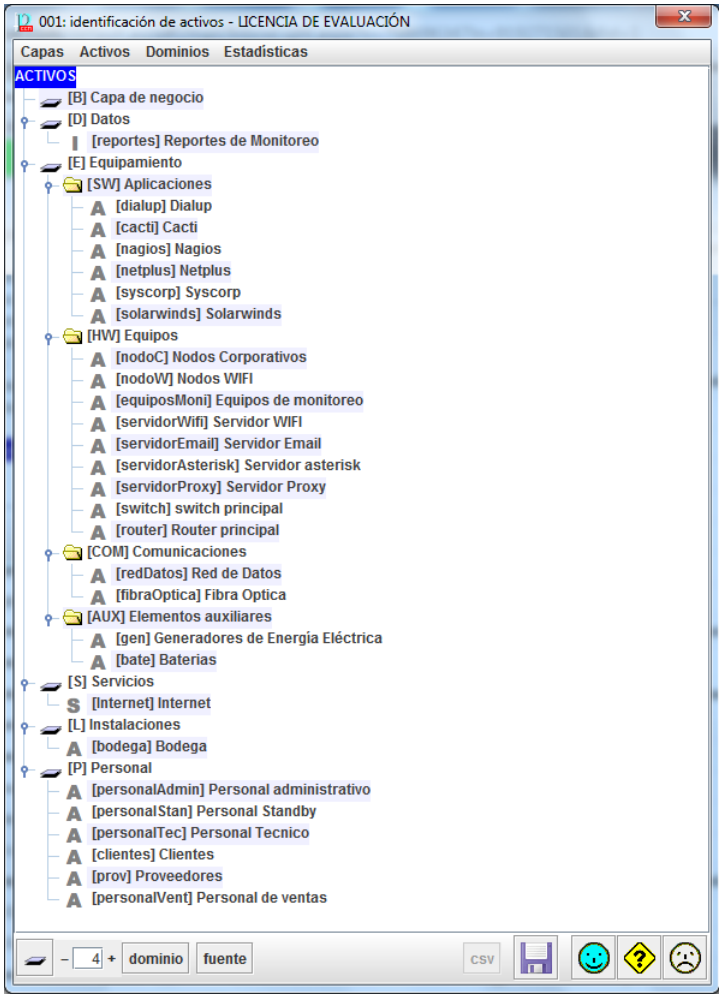


Figura 18: Tarea Identificación de Activos Fuente:PILAR

ACTIVOS	Netplus	Syscorp	Dial up	WIFI	Email	Cacti	Solarwinds	Nagios	Equipos de monitoreo	Reportes de monitoreos	Bodega	Nodos Corporativos	Nodos Wifi	Asterisk	Generadores de Energía Eléctrica	Baterías	Router principal	Switch	Anillo de fibra óptica	Internet	Red de datos	Proveedores	Clientes	Administrativo	Personal Standby	Personal Técnico	Personal Ventas	Proxy
Sistema Netplus		√																					√	√		√		
Sistema Syscorp						√	√	√		√													√			√		
Sistema Dialup				√		√	√	√		√																√		
Servidor WIFI													√				√	√	√							√		
Servidor Email										√													√	√	√	√	√	
Cacti										√													√					
Sistema Solarwinds										√													√					
Nagios										√													√					
Equipos de monitoreo							√			√													√					
Reportes de monitoreo																							√					
Bodega												√	√												√	√		
Nodos Corporativos													√				√	√	√	√	√		√		√			
Nodos Wifi																	√	√	√	√	√		√		√			
Asterisk																							√	√	√	√	√	
Generadores de Energía Eléctrica												√	√				√	√	√									
Baterías												√	√				√	√										
Router principal	√	√		√														√	√	√	√		√					
Switch principal	√	√		√													√		√	√	√		√					
Anillo de fibra óptica																		√			√		√					
Internet																							√	√	√	√	√	
Red de datos	√	√	√		√					√				√			√	√	√	√			√	√	√	√	√	√
Proveedores																							√					
Clientes	√	√																										
Personal Administrativo	√																								√	√	√	
Personal Standby			√	√						√	√	√	√		√	√	√	√	√		√		√			√	√	
Personal Técnico						√	√	√		√	√	√	√	√	√	√	√	√	√		√		√					
Personal Ventas																								√	√	√		
Proxy	√																				√							

Cuadro 8: Identificación de Dependencia entre activos Fuente: Puntonet

	Valor	Criterio
10	Muy alto	Daño muy grave
7-9	Alto	Daño grave
4-6	Medio	Daño moderado
1-3	Bajo	Daño mínimo
0	Despreciable	Sin efectos

Cuadro 9: Escala de criterios de valoración Fuente: MAGERIT

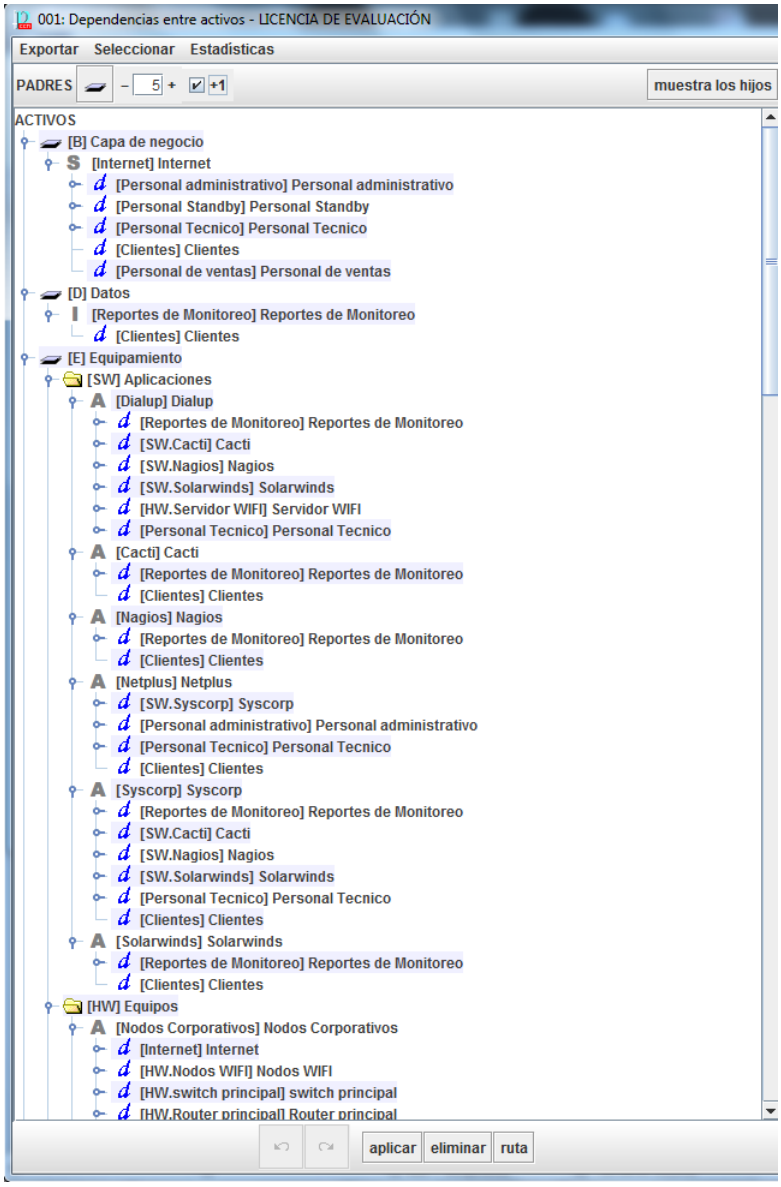
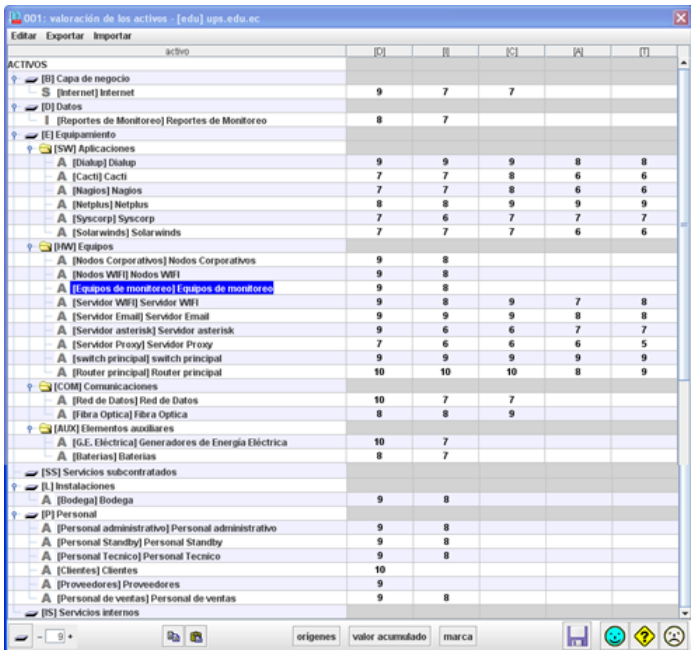


Figura 19: Tarea Dependencia entre activos Fuente: PILAR

ACTIVOS	D	I	C	A	T
[equiposMoni] Equipos de monitoreo	9^4	8^4			
[nodoC] Nodos corporativos	9^4	8^4			
[nodoW] Nodos WIFI	9^4	8^4			
[servidorWifi] Servidor WIFI	9^5	8^5	9^5	7^5	8^5
[servidorEmail] Servidor de Email	9^3	9^3	9^3	8^3	8^3
[servidorAsterisk] Asterisk	9^3	6^3	6^3	7^3	7^3
[servidorProxy] Proxy	7^3	6^3	6^3	6^3	5^3
[router] Router principal	10^4	10^4	10^4	8^4	9^4
[switch] Switch principal	9^4	9^4	9^4	9^4	9^4
[netplus] Sistema Netplus	8^3	8^3	9^3	9^3	9^3
[syscorp] Sistema Syscorp	7^3	6^3	7^3	7^3	7^3
[dialup] Sistema Dialup	9^2	9^2	9^2	8^2	8^2
[cacti] Cacti	7^2	7^2	8^2	6^2	6^2
[solarwinds] Solarwinds	7^2	7^2	7^2	6^2	6^2
[nagios] Nagios	7^2	7^2	8^2	6^2	6^2
[reportes] Reportes Monitoreo	8^2	7^2			
[gen]Generadores de Energía Eléctrica	10^6	7^6			
[bate]Baterías	8^6	7^6			
[fibraOptica]Anillo de fibra óptica	8^4	8^4	9^4		
[redDatos]Red de datos	10^4	7^4	7^4		
[Internet]Internet	9^1	7^1	7^1		
[clientes] Clientes	10^1				
[prov] Proveedores	9^8				
[personalTec] Personal Técnico	9^7		8^7		
[personaVent] Personal de ventas	9^7		8^7		
[personalStan] Personal Standby	9^7		8^7		
[personalAdmin] Personal administrativo	9^7		8^7		
[bodega] Bodega	9^6	8^6			

Cuadro 10: Criterios de valoración adicionales Fuente: MAGERIT



001: valoración de los activos - [edu] ups.edu.ec

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Capa de negocio					
[Internet] Internet	9	7	7		
[D] Datos					
[Reportes de Monitoreo] Reportes de Monitoreo	8	7			
[E] Equipamiento					
[SW] Aplicaciones					
[Dialup] Dialup	9	9	9	8	8
[Cacti] Cacti	7	7	8	6	6
[Nagios] Nagios	7	7	8	6	6
[Netplus] Netplus	8	8	9	9	9
[Syscorp] Syscorp	7	6	7	7	7
[Solarwinds] Solarwinds	7	7	7	6	6
[HW] Equipos					
[Nodos Corporativos] Nodos Corporativos	9	8			
[Nodos WIFI] Nodos WIFI	9	8			
[Equipos de monitoreo] Equipos de monitoreo	9	8			
[Servidor WIFI] Servidor WIFI	9	8	9	7	8
[Servidor Email] Servidor Email	9	9	9	8	8
[Servidor asterisk] Servidor asterisk	9	6	6	7	7
[Servidor Proxy] Servidor Proxy	7	6	6	6	5
[switch principal] switch principal	9	9	9	9	9
[Router principal] Router principal	10	10	10	8	9
[COM] Comunicaciones					
[Red de Datos] Red de Datos	10	7	7		
[Fibra Optica] Fibra Optica	8	8	9		
[AUX] Elementos auxiliares					
[G.E. Eléctrica] Generadores de Energía Eléctrica	10	7			
[Baterias] Baterias	8	7			
[SS] Servicios subcontratados					
[L] Instalaciones					
[Bodega] Bodega	9	8			
[P] Personal					
[Personal administrativo] Personal administrativo	9	8			
[Personal Standby] Personal Standby	9	8			
[Personal Tecnico] Personal Tecnico	9	8			
[Clientes] Clientes	10				
[Proveedores] Proveedores	9				
[Personal de ventas] Personal de ventas	9	8			
[IS] Servicios internos					

origenes valor acumulado marca

Figura 20: Tarea Valoración de Activos Fuente: PILAR

(2) [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)

(3) [3.da]Probablemente cause la interrupción de actividades propias de la Organización

(4) [9.da]Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

(5) [5.olm]Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa logística

(6) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

(7) [1.olm]Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

(8) [7.cei.e] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

Para poder observar la información completa de los criterios de valoración adicionales, verificarlos en el ANEXO B "Criterios de Valoración adicionales".

4.3.2 *Caracterización de las Amenazas*

Actividad que identifica las posibles amenazas que pueden afectar en alguna de las dimensiones de valoración de un activo, en donde es necesario considerar la degradación y la frecuencia de ocurrencia sobre dicho activo.

Identificación de las Amenazas

En la identificación de las amenazas se detallan las principales amenazas sobre cada uno de los activos con referencia al "Catálogo de amenazas" propuesto por MAGERIT, que se observa en el ANEXO C.

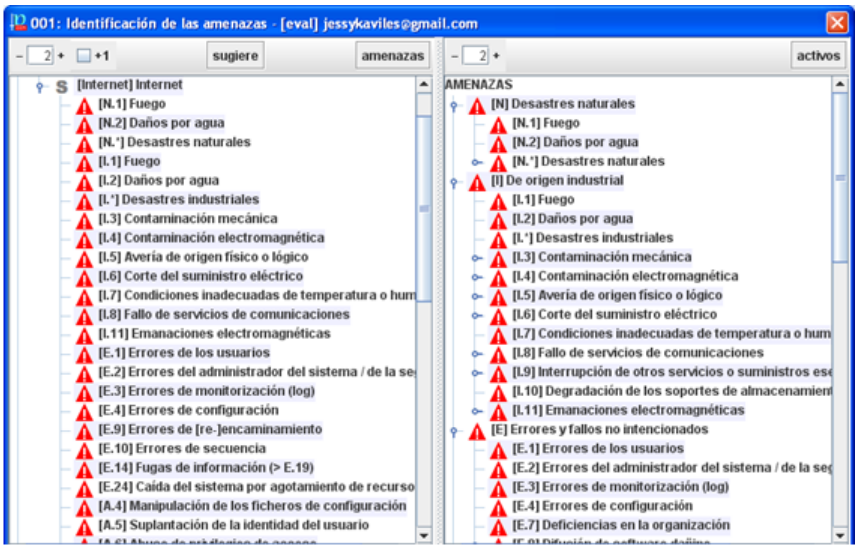


Figura 21: Tarea Identificación de las Amenazas Fuente: PILAR

Degradación en porcentaje	Simbología	Descripción
0 %		Nulo
10 %	B	Bajo
50 %	M	Medio
90 %	A	Alto
100 %	MA	Muy alto

Cuadro 11: Estimación de la frecuencia Fuente: MAGERIT

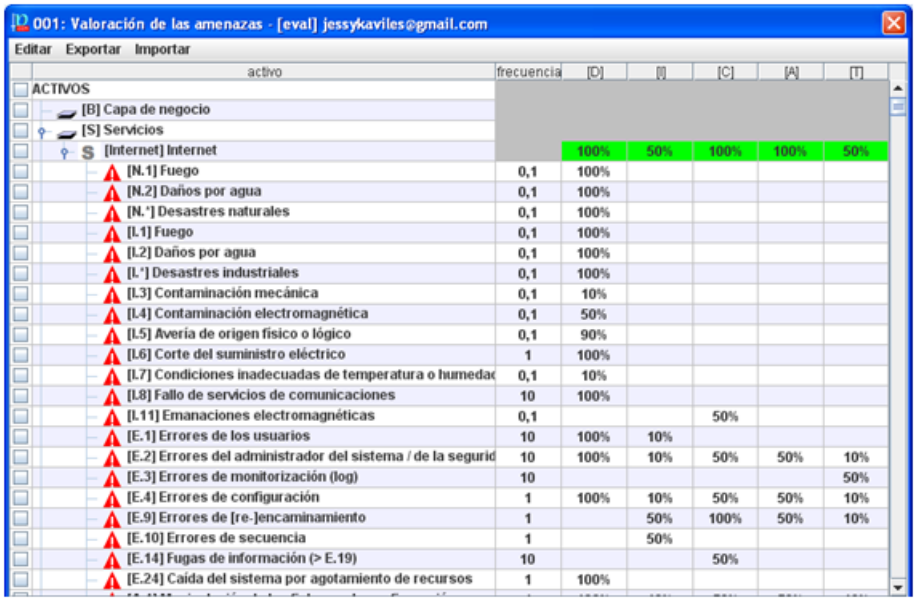
En la figura 4-1421 se muestra la identificación de las amenazas sobre los diferentes activos a estudiar.

Valoración de las Amenazas

En la valoración de las amenazas sobre un activo, se determina el valor de la frecuencia; que representa la tasa anual de ocurrencia siendo los valores típicos los indicados en el cuadro 4.5 11, y el valor de la

Degradación en porcentaje	Simbología	Descripción
0 %		Nulo
10 %	B	Bajo
50 %	M	Medio
90 %	A	Alto
100 %	MA	Muy alto

Cuadro 12: Estimación de la degradación Fuente: MAGERIT



001: Valoración de las amenazas - [eval] jessykaviles@gmail.com

Editar Exportar Importar

activo	frecuencia	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[B] Capa de negocio						
[S] Servicios						
[Internet] Internet		100%	50%	100%	100%	50%
[N.1] Fuego	0,1	100%				
[N.2] Daños por agua	0,1	100%				
[N.*] Desastres naturales	0,1	100%				
[I.1] Fuego	0,1	100%				
[I.2] Daños por agua	0,1	100%				
[I.*] Desastres industriales	0,1	100%				
[I.3] Contaminación mecánica	0,1	10%				
[I.4] Contaminación electromagnética	0,1	50%				
[I.5] Avería de origen físico o lógico	0,1	90%				
[I.6] Corte del suministro eléctrico	1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad	0,1	10%				
[I.8] Fallo de servicios de comunicaciones	10	100%				
[I.11] Emanaciones electromagnéticas	0,1			50%		
[E.1] Errores de los usuarios	10	100%	10%			
[E.2] Errores del administrador del sistema / de la seguridad	10	100%	10%	50%	50%	10%
[E.3] Errores de monitorización (log)	10					50%
[E.4] Errores de configuración	1	100%	10%	50%	50%	10%
[E.9] Errores de [re-]encaminamiento	1		50%	100%	50%	10%
[E.10] Errores de secuencia	1		50%			
[E.14] Fugas de información (> E.19)	10			50%		
[E.24] Caída del sistema por agotamiento de recursos	1	100%				

Figura 22: Tarea Valoración de las Amenazas Fuente: PILAR

degradación que simboliza el daño causado por un incidente en el caso de que ocurriera como se puede ver en el cuadro 4.6 12.

En la figura 4.15 22se muestra la valoración de todas las amenazas en cada una de las dimensiones de los activos utilizados.

4.3.3 *Caracterización de las Salvaguardas*

En esta actividad se identifican las salvaguardas existentes en la organización junto con la eficacia que tiene cada una de ellas para la mitigación de riesgos. Dentro de la metodología se pueden definir varias fases de estudio que pueden abarcar lapsos de tiempo cortos o largos incluso de un año,pero para nuestro caso de estudio tomaremos tres fases:

- Primera fase llamada POTENCIAL (Potencial)
- Segunda fase llamada ACTUAL (Current)
- Tercera fase llamada OBJETIVO (Target)

Identificación de las Salvaguardas Existentes

En esta tarea se identifica las salvaguardas desplegadas actualmente en la organización, se toma como referencia los controles de las ISO 27001 y 27011 para esto es necesario hacer el levantamiento de información las cuales se obtuvieron por medio de encuestas que se pueden apreciar en el Anexo 3 “Situación Actual de la Empresa”.

ISO 27001

Políticas de Seguridad

- La política de seguridad se maneja internamente, es decir no existe documentación alguna referente a las políticas de seguridad, por lo tanto no se realiza ninguna revisión de la misma.

Organización de la Seguridad de la Información

- Se delega al personal tareas específicas y responsabilidades que deben manejar sobre diferentes procesos relacionados con las actividades de la organización.
- En el contrato de trabajo para el personal se firma un acuerdo de confidencialidad el mismo que está sujeto a normas internas de la empresa y acciones legales en caso de que se revele información relativa a productos, servicios, clientes, proveedores, personal, método de trabajo, organización, estrategias empresariales, información económica y financiera, entre otros.

Administración de Recursos

- Para los activos más sensibles de la empresa se tiene un responsable designado por el jefe inmediato, para el tratamiento y gestión de los mismos.
- De igual manera la empresa cuenta con un inventario de activos esenciales para cumplimiento de objetivos del negocio.

Seguridad de los Recursos Humanos

- Antes de la contratación laboral se describe en el contrato de trabajo, los términos y condiciones del mismo, bajo los cuales el empleado debe regirse para el cumplimiento eficaz de sus actividades.
- La selección del personal se la efectúa mediante referencias y verificación de la hoja de vida.
- EL empleado antes de acceder a información que maneje la empresa debe firmar un acuerdo de confidencialidad.

Seguridad Física y del Entorno

- La empresa cuenta con un perímetro de acceso físico como son paredes y puertas, las cuales permiten el ingreso únicamente al personal que dispone de las llaves.
- Existe monitoreo mediante cámaras de seguridad.
- En caso de incendio existen las respectivas normativas de seguridad industrial (extintor, detector de humo, señalización y luminaria de emergencia).
- Se dispone de una normativa sobre seguridad industrial que deben seguir los empleados para evitar accidentes el momento de ejecutar alguna tarea que incluya riesgo laboral. Para el cumplimiento de estas normal se capacita al personal para que tengan conocimiento del mismo.

- Se protegen los equipos con reguladores, UPS, electrodos, pararrayos y con conexiones a tierra.
- En caso de que exista una falla eléctrica se protegen activos como los nodos, switch, router principales con bancos de baterías y generadores. Se cuenta con procedimientos para saber cuando es necesario colocar estos equipos de suministro eléctrico.
- El momento que haya una falla en el suministro de energía, existen baterías que entran automáticamente en funcionamiento y en caso de que estas se agoten, es necesario colocar un generador.
- Para garantizar la disponibilidad de los equipos como los nodos, rack, y otros equipos importantes se realiza un mantenimiento establecido previamente, así como mantenimiento por adecuación.
- Los equipos que ya no tienen utilidad alguna, se los retorna a la matriz bajo la supervisión de personal encargado de verificar las respectivas labores.

Administración de las Comunicaciones y Operaciones

- La prestación de servicios por terceras partes se mantiene en una política de calidad interna que garantice el cumplimiento del contrato establecido.
- Se toman precauciones para evitar y detectar la intrusión de códigos maliciosos como: Firewall, proxy, anti-spam, access list.
- Los activos más importantes tienen un respaldo backup

Control de Accesos

- Política de control de acceso: mediante la creación de access list, iptables, proxy.
- Gestión de privilegios: implementado mediante Radius
- Gestión de contraseñas de usuario: para ciertos activos, ya que no todos los sistemas tienen definidos usuarios y roles.
- Control de acceso en red: a través de la creación de vlans.
- Autenticación de usuario para conexiones externas: se realiza mediante VPN's.
- Protección a puertos de diagnóstico remoto: Creado en el border principal y firewalls internos.
- Segregación en las redes: Se tiene separados los servidores, por vlans.
- Control de conexión a las redes: Mediante control por MAC address.
- Control de acceso al sistema operativo: Con uso de claves de usuario.

- Identificación y autenticación de usuario: creado y aplicado a ciertos activos.
- Sistema de gestión de contraseñas: sistema básico que permite la creación, modificación de las cuentas de usuario.
- Uso de los servicios del sistema: aplicado mediante el uso de VPN y certificados.
- Limitación del tiempo de conexión: efectuada para ciertos equipos de red como routers, switchs, OLT.
- Control de acceso a las aplicaciones: mediante el uso de Access List para controlar el acceso de la red interna, para uso remoto mediante VPN o escritorio remoto.
- Trabajo remoto: VPN, un túnel encriptado y certificados digitales.

Adquisición de Sistemas de Información, Desarrollo y Mantenimiento

- Este dominio no es aplicable para nuestro caso de estudio debido a que los controles se definen más a lo relacionado a protección de sistemas y desarrollo de software, proceso que se realiza en la matriz.

Administración de los Incidentes de Seguridad

- Los incidentes de seguridad que hayan ocurrido en cualquiera de los procesos de la empresa, son comunicados al jefe inmediato por medio de reuniones, en donde también se busca evaluarlos así como tomar las acciones correctivas.

Administración de la Continuidad del Negocio

- Existe el desarrollo de planes de continuidad del negocio que incluyen planes de contingencia, los cuales están a cargo de los supervisores para que actúen en caso de que alguna amenaza afecte a alguno de los activos sensibles.
- Se cuenta con documentación que indica como proceder en caso de que se materialice una amenaza.

Cumplimiento

- La empresa cuenta con una política interna que garantiza que el personal de un uso debido a dispositivos de tratamiento de la información, y al no cumplirse se aplicará las sanciones correspondientes.

- Son los supervisores los que se encargan de que las normas y procedimientos se cumplan, así como de hacer la revisión de los mismos.

ISO 27011

Arquitectura de Seguridad para Interconexión de Sistemas Abiertos para Aplicaciones del CCITT

- No existen procedimientos documentados sobre como proteger a los activos en cada capa del modelo de referencia OSI pero existen distintos mecanismos que garantizan el cumplimiento de ciertos controles tales como:
  - Servidores Radius
  - Access list
  - Enrutamiento
  - Autenticación
  - Cifrado

Arquitectura de Seguridad para Sistemas de Extremo a Extremo de las Comunicaciones

- No se cuenta con procedimientos o políticas especificadas bajo este control sin embargo existen controles internos que aseguran la comunicación de extremo a extremo protegiendo algunas de las dimensiones de seguridad.

Sistemas de Gestión de la Calidad

- La organización cuenta con una política de seguridad donde se compromete a mejorar continuamente tanto las expectativas como las necesidades de los clientes, esto se especifica en el contrato, al igual que las sanciones por el incumplimiento.

Sistemas de Gestión Ambiental

- El sistema de gestión ambiental no se encuentra implementado.

001: salvaguardas - [edu] ups.edu.ec

[base] Base

asp...	estr...	salvaguarda	dudas	fuente	com...	reco...	on / off	aplic...
		SALVAGUARDAS						
G	PR	[H] Protecciones Generales	...			7		
G	PR	[D] Protección de la Información				7		
G	PR	[S] Protección de los Servicios				5	off	n.a.
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				6	off	n.a.
G	PR	[HW] Protección de los Equipos Informáticos (HW)				5	off	n.a.
G	PR	[COM] Protección de las Comunicaciones				8		
G	PR	[IP] Puntos de interconexión: conexiones con otros sistemas					off	n.a.
G	PR	[SI] Protección de los Soportes de Información					off	n.a.
G	PR	[AUX] Elementos Auxiliares				5		
F	PR	[L] Protección de las Instalaciones	...			6		
P	PR	[P] Gestión del Personal				5		
G	AD	[G] Organización				4		
G	RC	[BC] {or} Continuidad del negocio				5		
G	AD	[E] Relaciones Externas				3	off	n.a.
G	AD	[C] Productos certificados o acreditados					off	n.a.
G	EL	[K] Gestión de claves criptográficas					off	n.a.

nivel – 1 + fuentes eliminar recomendación sólo si ... SoA

Figura 23: Tarea Identificación de Salvaguardas. Fuente PILAR

Tecnología de la Información

- La empresa debe realizar las respectivas legalizaciones con los organismos pertinentes tales como uso de frecuencias, permisos para el tendido de fibra, ubicación de nodos

Gestión del Riesgo

- La empresa no cuenta con una metodología específica para la gestión de riesgos.

Seguridad de la Información

- No existe implementado un SGSI.

En PILAR se determina los controles que son aplicables para el análisis como se muestra en la figura 4.16 23.

Valoración de las Salvaguardas Existentes

En esta tarea se determina que tan eficaces son las salvaguardas existentes para realizarlo fue necesario realizar entrevistas al personal

Eficacia	Nivel	Significado
0 %	L0	inexistente
10 %	L1	inicial / ad hoc
50 %	L2	reproducible, pero intuitivo
90 %	L3	proceso definido
95 %	L4	gestionado y medible
100 %	L5	optimizado

Cuadro 13: Niveles de madurez de las salvaguardas. Fuente: MAGERIT

relacionado con la seguridad de la información, con la finalidad de obtener una visión más amplia de como está estructurada la seguridad en la organización como se muestra en la figura 4.17 24.

MAGERIT afronta el riesgo dividiendo el análisis por etapas con el objetivo de mostrar el avance de la mitigación. Se puede realizar en las etapas que se crea conveniente siendo a corto o largo plazo dependiendo las necesidades y el tiempo en que se va a realizar el análisis.

Para este caso de estudio se ha creído conveniente analizar en tres etapas, siendo estas: la etapa potencial, la etapa actual y la etapa objetivo. La etapa potencial muestra la situación actual sin salvaguardas. La etapa actual (current) recoge el nivel de madurez indicado en el cuadro 4.7 13 de las salvaguardas existentes previo al análisis, mientras que la etapa objetivo (target) especifica la madurez después de aplicar las salvaguardas necesarias para reducir el nivel de riesgo.

Insuficiencias detectadas

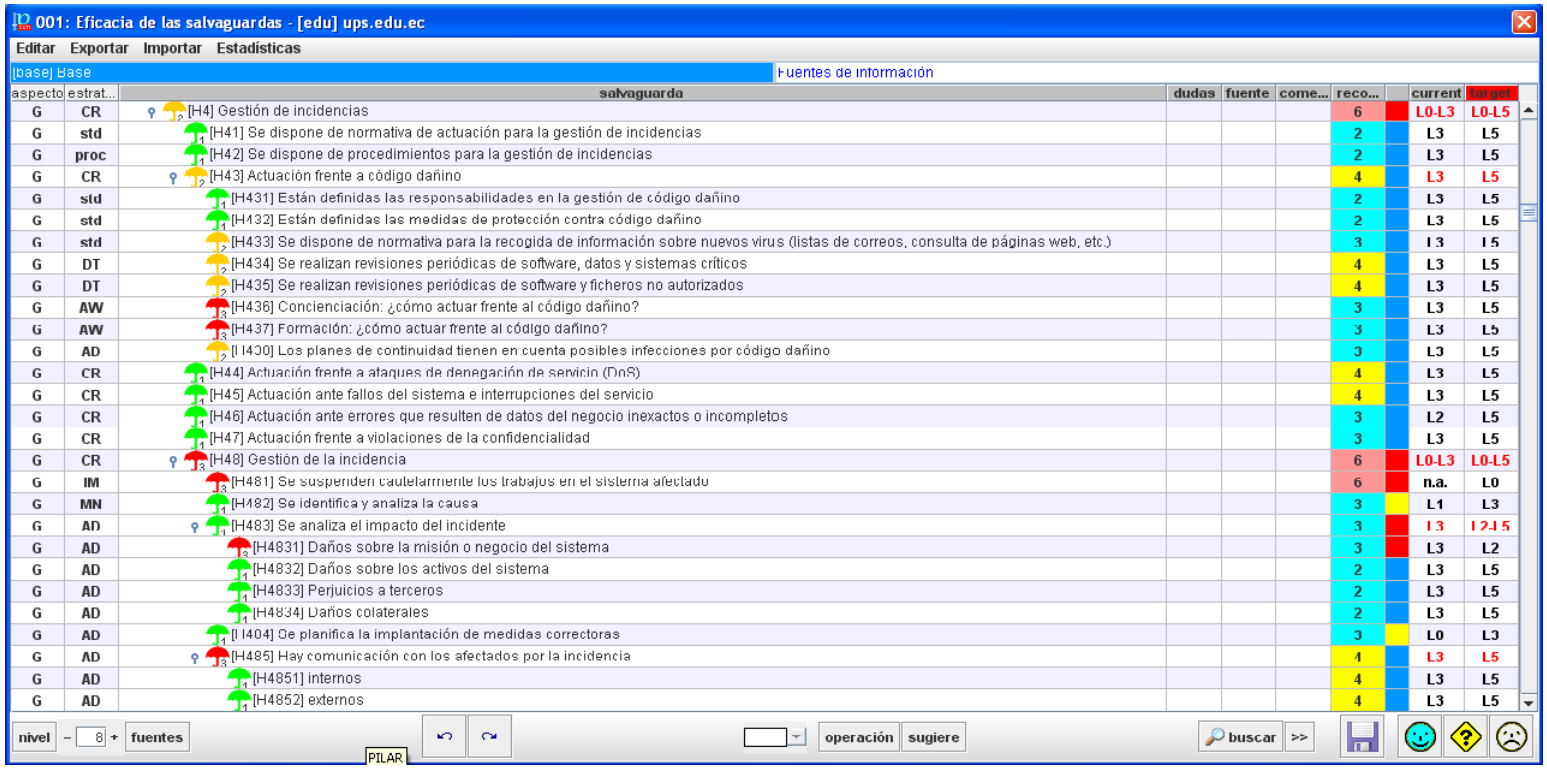
ISO 27001

Políticas de Seguridad

- Se debe crear un documento de las políticas de seguridad que contengan el objetivo, el alcance y la importancia de proteger la información.
- Es importante realizar una revisión periódica de las políticas de seguridad mediante reuniones o presentaciones.

Organización de la Seguridad de la Información

- Es necesario definir claramente las responsabilidades para la protección de los activos, así como designar los roles de los empleados para ellos controlen que se estén cumpliendo las normas establecidas.
- Cuando se detecte un incidente de la seguridad de la información, el personal debe saber con que autoridad contactar y reportar oportunamente los incidentes.
- Obtener asesoría sobre la seguridad de la información donde todo el personal comprenda la importancia de la misma mediante advertencias oportunas relacionadas con ataques y vulnerabilidades.



aspecto	estrat...	salvaguarda	dudas	fuente	come...	reco...	current	target
G	CR	[H4] Gestión de incidencias				6	L0-L3	L0-L5
G	std	[H41] Se dispone de normativa de actuación para la gestión de incidencias				2	L3	L5
G	proc	[H42] Se dispone de procedimientos para la gestión de incidencias				2	L3	L5
G	CR	[H43] Actuación frente a código dañino				4	L3	L5
G	std	[H431] Están definidas las responsabilidades en la gestión de código dañino				2	L3	L5
G	std	[H432] Están definidas las medidas de protección contra código dañino				2	L3	L5
G	std	[H433] Se dispone de normativa para la recogida de información sobre nuevos virus (listas de correos, consulta de páginas web, etc.)				3	L3	L5
G	DT	[H434] Se realizan revisiones periódicas de software, datos y sistemas críticos				4	L3	L5
G	DT	[H435] Se realizan revisiones periódicas de software y ficheros no autorizados				4	L3	L5
G	AW	[H436] Concienciación: ¿cómo actuar frente al código dañino?				3	L3	L5
G	AW	[H437] Formación: ¿cómo actuar frente al código dañino?				3	L3	L5
G	AD	[I.I430] Los planes de continuidad tienen en cuenta posibles infecciones por código dañino				3	L3	L5
G	CR	[H44] Actuación frente a ataques de denegación de servicio (DoS)				4	L3	L5
G	CR	[H45] Actuación ante fallos del sistema e interrupciones del servicio				4	L3	L5
G	CR	[H46] Actuación ante errores que resulten de datos del negocio inexactos o incompletos				3	L2	L5
G	CR	[H47] Actuación frente a violaciones de la confidencialidad				3	L3	L5
G	CR	[H48] Gestión de la incidencia				6	L0-L3	L0-L5
G	IM	[H481] Se suspenden cautelarmente los trabajos en el sistema afectado				6	n.a.	L0
G	MN	[H482] Se identifica y analiza la causa				3	L1	L3
G	AD	[H483] Se analiza el impacto del incidente				3	L3	L2-L5
G	AD	[H4831] Daños sobre la misión o negocio del sistema				3	L3	L2
G	AD	[H4832] Daños sobre los activos del sistema				2	L3	L5
G	AD	[H4833] Perjuicios a terceros				2	L3	L5
G	AD	[H4834] Daños colaterales				2	L3	L5
G	AD	[I.I404] Se planifica la implantación de medidas correctoras				3	L0	L3
G	AD	[H485] Hay comunicación con los afectados por la incidencia				4	L3	L5
G	AD	[H4851] internos				4	L3	L5
G	AD	[H4852] externos				4	L3	L5

Figura 24: Tarea Valoración de las Salvaguardas. Fuente PILAR

- Identificación de riesgos concernientes a los servicios prestados por proveedores.
- Estipular los acuerdos de tal manera que no existan malos entendido entre clientes, proveedores y la empresa.

Administración de Recursos

- No se realiza un completo inventario de activos en el cual se detalle aspectos importantes como su valor, importancia, ubicación y propietarios.
- No hay documentación sobre el uso de activos.
- No existen guías de clasificación para de esta manera poder obtener los grados de sensibilidad y protección de la información.

Seguridad de los Recursos Humanos

- No se cuenta con programas de concientización sobre la seguridad de los activos que el personal maneja.
- Cuando el contrato laboral finaliza no se realiza la devolución de los activos asignados al personal, ni se cancelan los derechos de acceso.

Seguridad Física y del Entorno

- No existe tecnologías de autenticación como tarjetas, biométricos para el acceso a las instalaciones y registros de entrada y salida.
- No existen seguridad en el cableado.
- El mantenimiento de los equipos no se realiza de forma periódica sino de forma intempestiva.
- No se cuenta con una política para el manejo de equipos fuera de la organización.
- Un procedimiento para la destrucción de la información y eliminación de equipos no se encuentra establecido.

Administración de las Comunicaciones y Operaciones

- No existe una planificación para minimizar el riesgo por fallas de sistema, como riesgo de sobrecarga.
- No se monitorea el cumplimiento de acuerdos de prestación de servicios.

- Concientizar al personal del correcto uso de los activos como evitar la intrusión de códigos maliciosos mediante herramientas de protección así como evitar la divulgación o destrucción de activos no autorizados.
- No se encuentra implementado un sistema de monitoreo para detectar las actividades sospechosas o intrusiones en la red.

Control de Acceso

- No se llevan bitácoras para mantener un control de quienes acceden a los diferentes activos.
- En ciertos activos no existe gestión de privilegios ya que el personal accede con un mismo usuario y contraseña, de esta forma no se puede identificar ni llevar bitácoras.
- En la gestión de contraseñas de usuario, estas no se revocan, ni tienen un tiempo de vida, tampoco verifica su robustez.
- No se tiene un proceso formal para revisión periódica de los derechos de acceso a los distintos activos.
- No existe un procedimiento de la autenticación del usuario para conexiones externas.
- Tras un periodo de inactividad los equipos no se desconecta.

Adquisición de Sistemas de Información, Desarrollo y Mantenimiento

- Este dominio no es aplicable para nuestro caso de estudio debido a que los controles se definen más a lo relacionado a protección de sistemas y desarrollo de software, proceso que se realiza en la matriz.

Administración de los Incidentes de Seguridad

- No existe un responsable que maneje los eventos y debilidades de los activos.
- Existe una identificación de responsables para los incidentes de seguridad, pero no son suficientes debido a que es necesaria una respuesta rápida para el inmediato tratamiento de los incidentes así como las acciones logrando la recuperación de brechas de seguridad.

Administración de la Continuidad del Negocio

- No existe un mantenimiento, ni evaluación de los planes de contingencia, para garantizar que estos funcionen en situaciones reales.

Cumplimiento

- En la sucursal Cuenca no se realiza una auditoría interna ya que la auditoría se la realiza por parte del personal de la matriz de Quito.
- No se hacen revisiones periódicas de la seguridad de los sistemas de información para garantizar la conformidad en base a las políticas.
- No se realizan revisiones regulares que aseguren que se está cumpliendo las políticas y su correcta implementación.

ISO 27011

Arquitectura de Seguridad para Interconexión de Sistemas Abiertos para Aplicaciones del CCITT

- No se tiene una documentación para dar una descripción general de los servicios de seguridad y mecanismos, que pueden ser proporcionados por el modelo de referencia OSI.
- No se han identificado servicios y mecanismos básicos de seguridad y su ubicación apropiada para todas las capas del modelo de referencia básico.

Arquitectura de Seguridad para Sistemas de Extremo a Extremo de las Comunicaciones

- No existe un procedimiento guiado que especifiquen estos controles.

Sistemas de Gestión de la Calidad

- No existe una concientización a todo el personal sobre la importancia de la política de calidad y sobre el mejoramiento continuo de su eficacia.
- Debería existir mayor capacitación sobre el trato al cliente a todo el personal.

Valoración	Riesgo	
5 o más	Crítico	
4	Muy alto	
3	Alto	
2	Medio	
1	Bajo	
0	Despreciable	

Figura 25: Niveles de Criticidad Fuente: MAGERIT

Sistemas de Gestión Ambiental

- El sistema de gestión ambiental no se encuentra implementado.

Tecnología de la Información

- No todo el personal tiene el conocimiento necesario.

Gestión del Riesgo

- La empresa no cuenta con una metodología específica para la gestión de riesgos.

Seguridad de la Información

- Actualmente no se encuentra implementado un Sistema de Gestión de Seguridad de la información.

4.3.4 *Estimación del Estado de Riesgo*

Dentro de esta actividad se procesa e interpreta los valores obtenidos del estudio de las actividades mencionadas anteriormente para detallar un informe del estado de riesgo que indique el riesgo e impacto acumulado y el repercutido de cada uno de los activos. Para la estimación del estado de riesgo empleamos la siguiente escala de valores especificados en la figura 4.18 25.
Impacto Residual

Si se han hecho todos los deberes a la perfección, el impacto residual debe ser despreciable. Si hay deberes a medio hacer entonces se dice que el sistema permanece sometido a un impacto residual.

FÓRMULA:

Un sistema de salvaguardas absolutamente ineficaz (ei = 0) deja el impacto donde estaba, mientras que un sistema de salvaguardas plenamente eficaz (ei = 1) reduce el impacto a 0.

$$impacto_residual = impacto \times (1 - e^{i})$$

Figura 26: Impacto Residual

$$riesgo_residual = impacto_residual \times frecuencia\ residual$$

Figura 27: Riesgo Residual

El impacto acumulado se realiza con los datos de impacto acumulado sobre un activo y las salvaguardas adecuadas para las amenazas sobre dicho activo. El impacto repercutido se realiza con los datos de impacto repercutido sobre el activo superior y las salvaguardas adecuadas para las amenazas del activo inferior.

Riesgo Residual

Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable. Si hay deberes a medio hacer entonces se dice que el sistema permanece sometido a un riesgo residual.

FÓRMULA:

DONDE:

Un sistema de salvaguardas absolutamente ineficaz (ef = 0) deja la frecuencia donde estaba, mientras que un sistema de salvaguardas plenamente eficaz (ef = 1) reduce la frecuencia a 0. En forma de cálculo:

Estimación del Impacto

Esta tarea determina el impacto acumulado y repercutido de cada uno de los activos de la organización, sin aplicar la eficacia del despliegue de las salvaguardar existentes en cada activo. El resultado final de esta tarea es un informe del impacto acumulado y repercutido sobre los diferentes activos.

Impacto Acumulado

Se lo calcula en cada activo teniendo en cuenta:

• Su valor acumulado (el propio mas el acumulado de los activos que dependen de él).

• Las amenazas a que está expuesto. Es la pérdida de valor acumulado.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. El impacto acumulado, al calcularse sobre los activos, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo.

$$frecuencia_residual = frecuencia \times (1 - e^{f})$$

Figura 28: Frecuencia Residual

$$\text{impacto} = i = v \times d$$

Figura 29: Impacto Acumulado

$$\text{impacto} = v \times d \times \text{grado}(A \Rightarrow B)$$

Figura 30: Impacto Repercutido

FÓRMULA:

DONDE:

- v es el valor acumulado (suma tradicional de valores de los activos superiores, ponderados por el grado de dependencia)
- d la degradación que sufre el activo

Impacto Repercutido

Se lo calcula en cada activo teniendo en cuenta:
• Su valor propio
• Las amenazas a que están expuestos los activos de los que depende.
El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

FÓRMULA:

Si el activo A depende del activo B, las amenazas sobre B repercuten sobre A. Si B sufre una degradación "d", A pierde en la proporción en que dependa de B. Si el activo A tiene un valor propio "v", el impacto es

Estimación del Riesgo

Esta tarea determina el riesgo acumulado y repercutido de cada uno de los activos de la organización, sin aplicar la eficacia del despliegue de las salvaguardar existentes en cada activo. El resultado final de esta tarea es un informe del riesgo acumulado y repercutido sobre los diferentes activos.

Riesgo acumulado

Se lo calcula en cada activo teniendo en cuenta:
• El impacto acumulado sobre un activo debido a una amenaza y
• La frecuencia de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza. El riesgo acumulado, al calcularse sobre los activos, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo.

En el cálculo del riesgo acumulado, se usará el impacto acumulado sobre el activo; es decir, la pérdida de valor acumulado por amenazas sobre el mismo.

Riesgo repercutido

Se lo calcula en cada activo teniendo en cuenta:

- El impacto repercutido sobre un activo debido a una amenaza y
- La frecuencia de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza. El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Pues es una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

4.4 EVALUACIÓN DEL RIESGO

Es necesario evaluar el impacto en el efecto que produciría un fallo de seguridad que cause la pérdida en alguna de las cinco dimensiones de seguridad, ya sea de confidencialidad, integridad o disponibilidad, autenticidad y trazabilidad de un activo de información.

Para la evaluación del riesgo hemos tomado las valoraciones según la figura 4.18 25"Niveles de Criticidad".

Evaluación Riesgo Residual Repercutido

Para esto es necesario tomar los valores calculados con la metodología MAGERIT, de la figura 4.19 31, cuyos valores indican que las deficiencias de seguridad que afectan a un activo inferior afectará también a uno superior, dejándolo sin los recursos necesarios para alcanzar los objetivos de la organización.

Se puede apreciar que la implementación de las salvaguardas existentes ha reducido en un alto porcentaje los riesgos logrando evitar que algunas de las amenazas definidas hayan alcanzado materializarse.

Sin embargo se ha encontrado que en algunos de los activos todavía existe un nivel ALTO de riesgo, debido a que el despliegue de salvaguardas no ha podido solventar las necesidades de seguridad que requieren los activos. Para evaluar por activos es necesario tomar la valoración obtenida en cada una de las dimensiones de seguridad.

Como ejemplo se va a tomar el activo Switch Principal de la tabla 31

- En la dimensión Disponibilidad existe un riesgo **MUY ALTO** de que no se pueda contar con el activo en un momento dado, lo que afectaría en gran medida algunos procesos de la organización que dependan de él.
- En la dimensión Integridad se puede comprobar que existe un riesgo **ALTO** indica que a pesar de que el activo cuenta con salvaguardas para resguardarlo, esta dimensión tiene un alto grado

de ineficacia para enfrentar ciertas amenazas que no permitan mantener con exactitud la información tal como fue creada.

- En la dimensión Confidencialidad se observa que existe un riesgo **MEDIO** esto supone que la elección de las salvaguardas que actúan sobre este activo son moderadamente eficaces pero aún existe un cierto grado de riesgo de que la información pueda ser expuesta u obtenida por terceros sin autorización.
- En la dimensión Autenticidad se verifica que hay un riesgo **BAJO** de que una amenaza pueda afectar al activo de que se compruebe que un usuario sea quién dice ser.
- En la dimensión Trazabilidad de igual forma se confirma que las salvaguardas aplicadas permiten asegurar quién y en qué momento se efectuó alguna operación sobre el activo.

Evaluación Riesgo Residual Acumulado

La evaluación de riesgo residual acumulado nos indicará la medida en que las amenazas afectaran a los activos de orden superior que dependen de dicho activo. Según la figura 4.20 32 los activos marcados con rojo en su respectiva dimensión de seguridad son aquellos que a pesar de contar con una salvaguarda aún presentan deficiencias, entonces es necesario reforzar las salvaguardas para tratar de mitigar el riesgo en su máximo valor. A continuación se tomará un activo para su respectivo detalle.

Se tomará el activo Red de datos de la figura 32.

- En las dimensionesDisponibilidad e Integridad, existe un riesgo **CRÍTICO** de que la red de datos no siempre esté disponible dadas ciertas condiciones, esto puede afectar procesos críticos de la organización, ya que los activos que dependan de la red de datos se verán afectados en la misma dimensión como por ejemplo el Netplus, Syscorp, etc, pudiendo esto influir hasta en aspectos económicos.
- En la dimensiónde confidencialidad se puede apreciar que hay un riesgo **MUY ALTO** esto indica que el activo y sus dependencias pueden verse afectados al momento del procesamiento de la información al no saber si la misma que se recibe es la misma que se generó inicialmente.
- En la dimensión de Autenticidad existe un riesgo **BAJO** esto es consecuencia de que las salvaguardas aplicadas casi en su totalidad garantizan que los datos que se difundan en la red sean de quién dice ser.
- En la dimensión Trazabilidad se puede verificar que existe un riesgo **DEPRECIABLE** es decir que gracias a las salvaguardas que han sido aplicadas en este activo se va a poder determinar quiénes y en qué momento accedieron para realizar alguna modificación.

	D	I	C	A	T
Internet	4,3k	2,4k	1,81k		
Reportes de Monitoreo	145	72			
Dialup	3,6k	3,1k	2,3k	940	1,04k
Cacti	310	155	110	20	35
Nagios	310	155	110	20	35
Netplus	3,6k	2,7k	2,3k	1,06k	1,17k
Syscorp	1,06k	2,1k	1,81k	830	910
Solarwinds	310	155	96	20	35
Nodos corporativos	3,4k	2,7k			
Nodos WIFI	3,4k	2,7k			
Equipos de monitoreo	600	240			
Servidor WIFI	2,3k	2,7k	2,3k	830	1,04k
Servidor Email	4,6k	3,2k	2,4k	1,01k	1,11k
Asterisk	4,3k	2,1k	1,56k	830	910
Proxy	3,2k	2,1k	1,59k	710	650
Switch principal	4k	3,1k	2,3k	1,06k	1,17k
Router principal	3,8k	3,4k	2,6k	940	1,17k
Red de Datos	360	230	310		
Fibra óptica	920	2,7k	2,3k		
Generador de energía eléctrica	3,8k	2,4k			
Baterías	3k	2,4k			
Bodega	4k	2,7k			
Personal administrativo	4k	2,7k			
Personal standby	4k	2,7k			
Personal técnico	4,3k	2,7k			
Clientes	82				
Proveedores	24				
Personal de ventas	48	2,1			

Figura 31: Riesgo Residual Repercutido. Fuente: PILAR

	D	I	C	A	T
Internet	4,8k	1,67k	2,7k	960	400
Reportes de Monitoreo	1,28k	1,8k	590	100	22
Dialup	4,8k	7,4k	1,94k	610	730
Cacti	2,9k	1,72k	730	135	420
Nagios	2,9k	1,72k	730	135	420
Netplus	4,8k	8,2k	2,4k	600	1,3k
Syscorp	4,2k	8,2k	2,4k	600	1,3k
Solarwinds	3,1k	1,81k	720	135	420
Nodos corporativos	4,3k	1,25k	790	540	210
Nodos WIFI	1,81k	187	155	65	102
Equipos de monitoreo	196	58			
Servidor WIFI	3k	2,6k	1,29k	600	670
Servidor Email	164	131	99	70	76
Asterisk	1,05k	2,1k	1,13k	600	650
Proxy	102	22	35	4,2	
Switch principal	1,58k	2k	1,22k	530	510
Router principal	2,4k	3k	1,79k	970	910
Red de Datos	5,9k	5k	4,3k	1,33k	930
Fibra óptica	3,4k	1,36k	185	150	194
Generador de energía eléctrica	107	0,022			
Baterías	54				
Bodega	112	56	7,1		
Personal administrativo	800	40	44	28	
Personal standby	800	40	44	28	
Personal técnico	830	40	44	28	
Clientes	1,75k	83	31	39	
Proveedores	24				
Personal de ventas	510	42	44	28	

Figura 32: Riesgo Residual Acumulado. Fuente: PILAR

	D	I	C	A	T
Internet	9	7	7		
Reportes de Monitoreo	8	6,3			
Dialup	9	9	9	8	7,2
Cacti	7	6,3	4	3	3
Nagios	7	6,3	4	3	3
Netplus	8	8	9	9	8,1
Syscorp	7	6	7	7	6,3
Solarwinds	7	6,3	3,5	3	3
Nodos corporativos	9	8			
Nodos WIFI	9	8			
Equipos de monitoreo	9	7,2			
Servidor WIFI	9	8	9	7	7,2
Servidor Email	9	9	9	8	7,2
Asterisk	9	6	6	7	6,3
Proxy	7	6	6	6	4,5
Switch principal	9	9	9	9	8,1
Router principal	10	10	10	8	8,1
Red de Datos	10	7	7		
Fibra óptica	8	8	9		
Generador de energía eléctrica	10	7			
Baterías	8	7			
Bodega	9	8			
Personal administrativo	9	8			
Personal standby	9	8			
Personal técnico	9	8			
Clientes	10				
Proveedores	4,5				
Personal de ventas	8,1	7,2			

Figura 33: Impacto Residual Repercutido. Fuente: PILAR

4.5 ANÁLISIS DEL IMPACTO Y EL FACTOR DE RIESGO

El análisis del impacto consiste en verificar que activo puede tener mayor probabilidad de verse afectado por una amenaza a pesar de que sus salvaguardas hayan sido desplegadas.

Impacto Residual Repercutido

El impacto repercutido residual describe si las normas, procedimientos y salvaguardas fueron los y las adecuadas y se aplicaron de correcta forma, si éste es el caso los valores que aquí se representen deben ser bajos o nulos.

En la figura 4.21 33 podemos verificar que las normas, procedimientos y salvaguardas se encuentran bien aplicados ya que el riesgo que aquí se presenta es depreciable, con esto lo que se quiere exponer es que no

	D	I	C	A	T
Internet	135	74	90	69	35
Reportes de Monitoreo	200	166	57	8,7	8,8
Dialup	36	148	81	35	63
Cacti	173	140	49	7,5	38
Nagios	173	140	49	7,5	38
Netplus	159	148	81	62	63
Syscorp	166	148	81	62	63
Solarwinds	182	147	49	7,5	38
Nodos corporativos	90	133	81	35	35
Nodos WIFI	135	133	81	35	35
Equipos de monitoreo	9	4			
Servidor WIFI	135	133	90	62	63
Servidor Email	9	8,1	9	7,2	7,2
Asterisk	54	133	90	62	63
Proxy	7	6	6	6	
Switch principal	135	148	90	69	63
Router principal	135	148	90	69	63
Red de Datos	176	155	97	69	35
Fibra óptica	166	133	45	35	35
Generador de energía eléctrica	64	0,7			
Baterías	62				
Bodega	57	74	9		
Personal administrativo	143	133	90	62	
Personal standby	143	133	90	62	
Personal técnico	149	133	90	62	
Clientes	210	92	57	44	
Proveedores	4,5				
Personal de ventas	151	140	90	62	

Figura 34: Impacto Residual Acumulado. Fuente: PILAR

existen activos a los que se les pueda perjudicar con un impacto Alto. Sin embargo puede existir todavía cierto impacto residual.

Impacto Residual Acumulado

De igual forma el impacto acumulado es aquel que puede perjudicar a un activo y o activos que dependen de éste. Se puede comprobar en la figura 4.22 34 que existen valores depreciables en las dimensiones de seguridad, por lo que se puede afirmar que una amenaza no puede impactar en gran valor a un activo.

4.6 EFECTOS DEL IMPACTO

Como se puede apreciar en la figura 4.23 35 indica la evolución del impacto en las tres etapas mencionadas de la gestión del riesgo, es decir: el estado actual, sin salvaguardas, y tras la ejecución de las salvaguardas. De esta manera se puede constatar que para todos los activos existe una minimización del impacto y riesgo sobre los activos tras la aplicación de la debida salvaguarda, con esto podemos distinguir

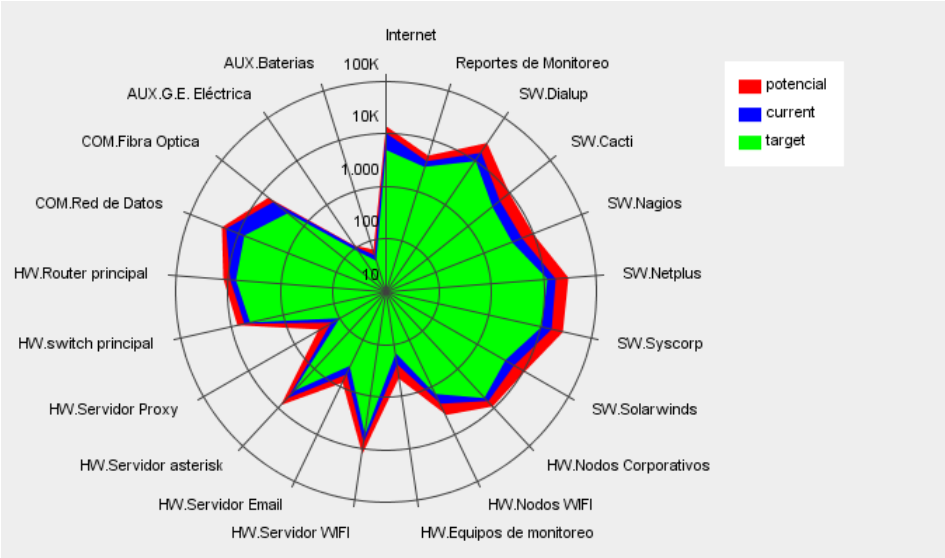


Figura 35: Efectos del impacto. Fuente: PILAR

de una manera más general como y en que medida se disminuye el riesgo e impacto después del análisis.

4.7 GESTIÓN DE RIESGOS

El proceso de Gestión de Riesgos detalla tareas con la finalidad de reducir, prevenir, impedir y controlar los efectos de materialización de amenazas sobre los diferentes activos, mediante la selección e implantación de salvaguardas adecuadas. Las salvaguardas que se van a aplicar están basadas en los estándares ISO 27001 Y 27011, descritos en el capítulo I y II respectivamente.

Este proceso se detalla en el capítulo V "Desarrollo de la Política de Seguridad", donde se realiza la gestión de riesgos de cada activo mitigándolos con las respectivas salvaguardas.

5 DESARROLLO DE LA POLÍTICA DE SEGURIDAD

5.1 PLANIFICACION DE LA POLITICA

Debido a que las salvaguardas actuales no han logrado reducir totalmente el riesgo al que pueden estar expuestos los activos, es necesaria la creación de políticas que contengan las salvaguardas idóneas para lograr, en lo posible, minimizar el estado de riesgo.

Según el análisis de riesgos realizado de los 28 activos se ha logrado determinar cuales son aquellos que necesitan de políticas de seguridad para reforzar las existentes. El criterio utilizado proviene del análisis de riesgo expuesto en las tablas de riesgo residual tanto acumulado como repercutido, para poder identificar que salvaguardas son las que necesitan se gestione más su seguridad.

5.2 CREACION DE LA POLITICA

Una vez identificados los activos que se deben proteger y en que dimensiones, se puede continuar con la definición de políticas.

En la tabla 5.1 36 se muestra la matriz donde se hallan las políticas a diseñar por cada activo así como aquellos que ya se tiene definidos algún tipo de política de seguridad

5.2.1 *Políticas Eegún el Estándar ISO 27001*

Política de Seguridad de la Información

Alcance:

- Email
- Bodega
- Nodos corporativos
- Nodos WIFI
- Router principal
- Switch principal
- Anillo fibra óptica
- Personal administrativo
- Personal técnico
- Personal standby
- Personal de ventas

	Netplus	Syscorp	Dial up	WIFI	Email	Cacti	Solarwinds	Nagios	Equipos de monitoreo	Reportes de monitoreos	Bodega	Nodos Coorporativos	Nodos Wifi	Asterisk	Generadores de Energía Eléctrica	Baterías	Router principal	Switch principal	Anillo de fibra óptica	Internet	Red de datos	Proveedores	Clientes	Personal Administrativo	Personal Standby	Personal Técnico	Personal Ventas	Proxy
Políticas de Seguridad					√						√	√	√				√	√	√					√	√	√	√	
Aspectos organizativos de la seguridad de la información			√	√		√	√	√		√																		
Administración de los recursos			√	√		√	√	√	√	√		√	√								√							
Seguridad de los Recursos Humanos																								√	√	√	√	
Seguridad Física y del entorno											√	√	√		√	√	√	√	√		√							√
Administración de las comunicaciones y operaciones						√	√	√									√	√			√	√						
Control de acceso			√	√	√							√	√				√	√			√					√		
Adquisición, desarrollo y mantenimiento de los sistemas de información																												
Administración de los incidentes de seguridad				√								√	√				√	√						√	√	√	√	
Gestión de la continuidad de negocio				√	√							√	√	√			√	√										√
Cumplimiento												√	√											√	√	√	√	
Arquitectura de seguridad de interconexión para sistemas abiertos												√	√				√	√			√							
Arquitectura de seguridad de interconexión para sistemas de extremo a extremo																	√	√										
Sistema de Gestión de calidad																				√		√	√					
Sistema de Gestión Ambiental												√	√															
Tecnología de la información												√	√															
Gestión de Riesgos*																												
Sistemas de Gestión de la Seguridad de la Información*																												

* Estas dos políticas comprenden los temas ya tratados en los Capítulos III y IV

Figura 36: Matriz de políticas. Fuente: Autoras

Responsabilidad:

- Gerente
- Jefe técnico
- Representante de cada área

Política:

La política de seguridad debe conformar un conjunto de normas y recomendaciones sobre como se manejaran los siguientes temas:

- **Organización de la Seguridad:** establecer un marco gerencial para controlar su implementación.
- **Seguridad del Personal:** reducir riesgos de error humano
- **Seguridad Física y Ambiental:** Impedir accesos no autorizados
- **Gestión de las Comunicaciones y las Operaciones:** Garantizar el funcionamiento correcto y seguro de las instalaciones de telecomunicaciones
- **Control de Acceso:** Controlar el acceso lógico a la información.
- **Desarrollo y Mantenimiento de los Sistemas**: Medidas de seguridad en los sistemas de información.
- **Administración de la Continuidad del negocio:** Proteger los procesos críticos Cumplimiento: Impedir infracciones y violaciones de las normas internas y externas.

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Alcance:

- Dialup
- WIFI
- Cacti
- Solarwinds
- Nagios
- Reportes de monitoreo

Responsabilidad:

- Coordinador del Comité de Seguridad de la Información.
- Comité de Seguridad de la Información: A cargo del mantenimiento y presentación de la presente Política.
- Responsable de Seguridad Informática.

Política:

Se deberá crear un Comité de Seguridad de la Información, integrado por representantes de cada área relacionada con la seguridad de la información en los que estén:

- Directivos y administrador de seguridad
- Personal

Sus funciones son:

- Revisar y proponer a la máxima autoridad del Organismo para su aprobación, la política y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de
- Información frente a las amenazas más importantes.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

Seguridad Física y Ambiental

Alcance:

- Nodos WIFI
- Nodos Corporativos
- Router Principal
- Switch Principal
- Servidores
- Bodega
- Generadores de energía eléctrica
- Baterías
- Red de datos
- Anillos de fibra óptica
- Proxy

Responsabilidad:

- Responsable de Seguridad Informática
- Jefe Técnico
- Supervisores
- Unidad de Auditoría Interna

Política:

Perímetro de Seguridad Física

- La protección física comprende la creación de diversas barreras o medidas de control físicas alrededor de las oficinas de la empresa y de las instalaciones de procesamiento de información.
- Se deben utilizar perímetros de seguridad para proteger las áreas que contienen activos importantes como switchs, routers de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.
- Un perímetro de seguridad se refiere por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas.

Controles de Acceso Físico

- Llevar un registro de los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso.
- Controlar y limitar el acceso a la información clasificada y a instalaciones dónde se encuentren activos importantes como el switch, router principal, olt's. El acceso se otorga exclusivamente a las personas autorizadas.
- Implementar el uso de una identificación visible para todo el personal del área.
- Definir un periodo para la revisión de los derechos de acceso para áreas protegidas. Esto debe ser documentado para posteriores actualizaciones.
- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

Protección de Oficinas, Recintos e Instalaciones

- Tener en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre.
- Se debe tomar en cuenta las disposiciones y normas en materia de sanidad y seguridad.

Mantenimiento de Equipos

- Someter el equipamiento a tareas de mantenimiento preventivo, de con períodos establecidos, especificaciones recomendados por el proveedor y con la autorización formal del Jefe Técnico.
- Se debe mantener un inventario actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Llevar un registro y generar un informe de todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- Registrar el retiro de equipamiento de la empresa para su mantenimiento.

Seguridad de los Equipos Fuera de las Instalaciones.

- El uso de equipamiento, fuera de las instalaciones de la empresa, será autorizado por el encargado de bodega.
- La seguridad para estos equipos contemplará la misma suministrada para los equipos dentro de la oficina teniendo en cuenta los riesgos de trabajar fuera de la misma.
- Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento.

Gestión de Comunicaciones y Operaciones

Alcance:

- Herramientas de monitoreo
- Switch
- Router
- Proveedores
- Red de datos

Responsable:

- Jefe técnico
- Administrador de seguridad
- Gerente
- Supervisores

Política:

Documentación de los Procedimientos Operativos

- Instrucciones para el manejo de errores u otras condiciones que puedan darse durante la ejecución de tareas.
- Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.
- Instalación y mantenimiento de equipos destinados a las comunicaciones.
- Monitoreo del procesamiento y las comunicaciones.
- Gestión de servicios.
- Resguardo de información.
- Gestión de incidentes de seguridad en las áreas donde se desarrollan actividades del negocio.

Procedimientos de Manejo de Incidentes

- Definir todos los posibles incidentes relativos a la seguridad
- Comunicar los incidentes tan pronto como sea posible a las personas encargadas
- Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas
- En los casos en los que se considere necesario, se solicitará la participación del Jefe técnico o Supervisores en el tratamiento de incidentes de seguridad ocurridos.

Política de Correo Electrónico

- Protección contra ataques al correo electrónico
- Protección de archivos adjuntos de correo electrónico.
- Uso de técnicas criptográficas para proteger dimensiones de seguridad
- Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados
- Definir para que actividades será el uso del correo electrónico por parte del personal de la empresa.
- Potestad de la empresa para auditar los mensajes recibidos o emitidos por el personal, lo cual se incluirá en el "Compromiso de Confidencialidad" .

Control de Accesos

Alcance:

- Nodos
- Switch
- Router
- Red de datos
- Servidor WIFI
- Email
- Servidor Dialup

Responsabilidad:

- Responsable de Seguridad Informática
- Jefe técnico

Política:

Reglas de Control de Acceso

- Indicar expresamente si las reglas son obligatorias u optativas
- Establecer reglas sobre protección y acceso a la información
- Controlar los cambios en los permisos de usuario
- Controlar las reglas que requieren la aprobación del administrador, y aquellas que no requieren aprobación

Administración de Accesos de Usuarios

- Otorgar derechos de acceso a los sistemas, datos y servicios de información mediante procedimientos.

Registro de Usuarios

- Utilizar identificadores de usuario únicos, con el fin de que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
- Verificar que el nivel de acceso otorgado es adecuado para el rol que cumple el usuario y es coherente con la Política de Seguridad de la empresa
- Entregar a los usuarios un documento que indique sus derechos de acceso

- Entregar un documento para que los usuarios lo firmen y acepten las condiciones de acceso.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización o salieron de la empresa.
- Efectuar revisiones en periodos establecidos
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal intentan accesos no autorizados.

Administración de Privilegios

- Mantener un registro de todos los privilegios asignados.
- Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Establecer un período de vigencia para el mantenimiento de los privilegios, luego del cual los mismos serán revocados.
- Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática.

Administración de Contraseñas de Usuario

- Generar contraseñas temporales seguras para otorgar a los usuarios.
- Almacenar las contraseñas sólo en sistemas protegidos.
- Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica, verificación de firma, uso de autenticadores de hardware.

Control de Acceso a la Red

Política de Utilización de los Servicios de Red

- Controlar el acceso a los servicios de red tanto internos como externos
- El Jefe Técnico tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red

Autenticación de Usuarios para Conexiones Externas

- Un método de autenticación físico (por ejemplo tokens de hardware)

- Un protocolo de autenticación desafío / respuesta
- También pueden utilizarse líneas VPN's o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Registro y Revisión de Eventos

- Se implementará un procedimiento de revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.
- La frecuencia de estas revisiones será definida por los Propietarios de la Información y el Responsable de Seguridad Informática.

Gestión de la continuidad del negocio

Alcance:

- Nodos corporativos
- Nodos WIFI
- Switch
- Router

Responsabilidad:

- Responsable de Seguridad Informática
- Supervisores
- Jefe Técnico
- Gerente

Política:

Proceso de la Administración de la Continuidad del Organismo

- Identificar y dar un primer lugar a los procesos críticos de las actividades de la empresa.
- Asegurar que todo el personal de la empresa comprenda los riesgos que la misma enfrenta, en relación con la probabilidad de ocurrencia e impacto de las posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de negocio.
- Elaborar y documentar una estrategia de continuidad de las actividades de la empresa conforme a los objetivos y prioridades acordados.

- Plantear planes de continuidad de las actividades de la empresa
- Crear conjuntamente con el representante de cada área un cronograma de pruebas de cada uno de los planes de contingencia asignando funciones para su cumplimiento.
- Diseñar actualizaciones periódicas de los planes y procesos implementados.

Continuidad de las Actividades y Análisis de los Impactos

- Identificar los eventos o amenazas que puedan ocasionar interrupciones en los procesos de las actividades.
- Realizar una evaluación de riesgos para de esta manera poder determinar el impacto que causarían estas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.
- Determinar controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y demás sistemas que puedan mitigar los daños.

Elaboración e Implementación de los Planes de Continuidad de las Actividades del Organismo

- Definir las acciones correctivas que se deban implementar y en que casos.
- Diseñar e implementar procedimientos de emergencia para de esta forma garantizar la recuperación y restablecimiento según un cronograma establecido.
- Llevar una documentación los procedimientos y procesos
- Capacitar al personal sobre procedimientos y procesos de emergencia acordados.
- Instruir al personal involucrado en los procedimientos de reanudación y recuperación

Marco para la Planificación de la Continuidad de las Actividades del Organismo

- Especificar cuáles son las condiciones de implementación para los planes que describan el proceso a seguir
- Describir los procedimientos de emergencia que indiquen que medidas tomar una vez ocurrido un incidente que ponga en peligro las operaciones de la empresa
- Definir los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la empresa.
- Definir un cronograma de mantenimiento donde conste por escrito cómo y cuándo será probado el plan

- Realizar la concientización e instrucción al personal, con el objetivo de que todos comprendan los procesos de continuidad de sus actividades y de esta forma garantizar de que los procesos van a seguir siendo eficaces.

Cumplimiento

Alcance:

- Nodos Corporativos
- Nodos WIFI
- Personal Técnico
- Personal Administrativo

Responsabilidad:

- El Responsable de Seguridad Informática
- Supervisores
- Jefe Técnico

Política:

Cumplimiento de la Política de Seguridad

- Los Responsables de cada una de las áreas de la empresa, serán los encargados de la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área.
- El responsable de la Seguridad Informática, realizará revisiones periódicas de todas las áreas de la empresa para garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

Sanciones Previstas por Incumplimiento

- Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas que rigen al personal.
- Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga según las políticas de la empresa existentes referente a incumplimientos y demás normativas específicas aplicables.

5.2.2 *Políticas Según el Estándar ISO 27011*

Sistema de Gestión de calidad

Alcance:

- Internet
- Proveedor
- Clientes

Responsabilidad:

- El Responsable de Seguridad Informática
- Gerente
- Jefe Técnico

Política:

Gestión de la calidad

- Determinar las necesidades y expectativas de los clientes
- Establecer la política y objetivos de la calidad de la organización
- Determinar los procesos y las responsabilidades necesarias para el logro de los objetivos de la calidad
- Determinar y proporcionar los recursos necesarios para el logro de los objetivos de la calidad
- Establecer los métodos para medir la eficacia de cada proceso y aplicar las medidas correspondientes
- Determinar los medios para prevenir no conformidades y eliminar sus causas;

Compromiso con la Calidad

- Establecer y mantener una política de calidad y asegurarse que se definen los objetivos de calidad de la organización, mesurable y coherente con dicha política.
- Comunicar la política y los objetivos de calidad en el seno de la organización para aumentar la concienciación, la motivación y la participación del personal.
- Asegurarse de que la organización está plenamente orientada a satisfacer tanto los requisitos del cliente como los legales y reglamentarios.

- Asegurarse de que se identifican y desarrollan todos los procesos necesarios para cumplir con estos requisitos y para alcanzar los objetivos de calidad definidos.
- Asegurarse de que se ha establecido, implantado y mantenido un SGC eficaz para alcanzar los objetivos de calidad definidos.
- Asegurarse de la disponibilidad de recursos necesarios.

Enfoque al Cliente

- Hablar con los clientes.
- Realizar estudios de mercado o de la clientela.
- Tener acceso a informes del sector.
- Identificar oportunidades de comercialización especializada.

Política de la Calidad

- Es adecuada al propósito de la organización.
- Incluye un compromiso de cumplir con los requisitos y de mejorar continuamente la eficacia del SGC.
- Proporciona un marco de referencia para establecer y revisar los objetivos de la calidad.
- Es comunicada y entendida dentro de la organización.
- Es revisada para su continua adecuación.

Sistema de Gestión Ambiental

Alcance:

- Nodos Corporativos
- Nodos WIFI

Responsabilidad:

- Responsable de la seguridad
- Jefe técnico
- Supervisores

Política Ambiental:

Dentro de la política ambiental se define la misión, la visión ambiental de la organización, objetivos y metas y como punto principal está la declaración que hace la empresa para garantizar su compromiso con la conservación del ambiente.

Aspectos Ambientales

- Reconocer los aspectos que la organización podría controlar o en los que influye de alguna manera como podría ser el consumo de energía
- Identificar las actividades que podrían tener grandes impactos en el medio ambiente.

Requerimientos Legales y Otros

- Crear un proceso por medio del cual se identifiquen cuáles son los requerimientos legales: requerimientos nacionales, locales, permisos, normas internacionales, y otras reglas que deba adoptar la empresa

Objetivos y Metas

- Capacitación a los empleados
- Mejorar la educación con respecto al medio ambiente.
- Metas ambientales como reducir el consumo de energía.

Programa de Gestión Ambiental

- El Programa de Gestión Ambiental es un plan de acción para lograr los objetivos y metas del sistema de gestión ambiental.
- Desarrollarlo priorizando acciones en relación con los procesos, productos, servicios y proyectos que se relacionen con los aspectos ambientales significativos establecidos, objetivos y metas, y la política ambiental de la empresa.
- El programa debe ser documentado, para poder ser sujeto a revisión posteriormente.

Tecnología de la información

Alcance:

- Nodos Corporativos
- Nodos WIFI

Responsabilidad:

- Responsable de la seguridad
- Jefe técnico
- Supervisores

Política:

- Gestión del nivel de servicios.
- Informes de servicios.
- Gestión de la continuidad y disponibilidad de servicios.
- Presupuesto y contabilidad de servicios de TI.
- Gestión de la capacidad.
- Gestión de la seguridad de la información.
- Gestión de la relación del negocio.
- Gestión de los proveedores.
- Optimizar costos a través de estructuras transparentes y gestión de servicios profesional.
- Gestionar riesgos sistemáticamente.
- Mejorar la escala de servicios
- Reaccionar efectivamente ante posibles problemas.

Servidor WIFI

Este activo presenta falencias en la dimensión de Integridad por lo que se recomienda según la ISO 27001:

- Identificar los perfiles de acceso y sus privilegios asociados.
- Registrar todas las operaciones.
- Administrar cambios.
- Administrar la seguridad.
- Monitorizar todas las operaciones.
- Definir los tipos de acceso.
- Creación de cuentas especificas para administradores del sistema.
- Creación de cuentas especificas para administradores de seguridad.
- Definir procedimiento de cancelación de privilegios.

- Comprobar previamente la identidad de los usuarios y los privilegios requeridos.
- Identificar los perfiles de acceso y sus privilegios asociados.
- Aprobación de los derechos de acceso son por el propietario del servicio.
- Separar las responsabilidades de administración y operación.
- Mantener un registro de los privilegios de acceso.
- Crear procedimiento de concesión de privilegios (Control de acceso logico).

Email

El activo Email según el análisis presenta riesgo se recomienda según la ISO 27001.

- Activación, creación, modificación y baja de las cuentas de usuario.
- Suspensión temporal de cuentas de usuario.
- Eliminación de cuentas.
- Las cuentas que ya no son necesarias se bloquean o eliminan.

Switch y Router

Debido a la sensibilidad que representan estos activos, manejan el mismo tipo de información y se fortalecerá las salvaguardas en la misma dimensión 27001

- Reparar las vulnerabilidades que implican un alto riesgo.
- Procedimientos para concesión de privilegios (Control de acceso logico).
- Planificar la reparación de los defectos descubiertos que implican un riesgo bajo.
- Normas de copias de seguridad backup.
- Concienciación de los usuarios.
- Separar las responsabilidades de administración y operación.
- Anular cuentas de usuario cuando termine la autorización.
- Concienciación en la detección y reporte de incidentes.
- Probar regularmente los procedimientos de gestión de incidentes.
- Procedimiento de cancelación de privilegios.
- Actualizar los procedimientos de usuario para incorporar o mejorar la identificación y forma de reaccionar ante el mismo incidente o incidentes similares.

- Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias.
- Gestión de incidencias (Se identifica y analiza la causa).
- Se debe identificar el personal que va a gestionar el incidente.

Baterías y generador de energía eléctrica

Seguir las recomendaciones del fabricante.

Política para el control del personal:

Aquí se redefine nuevas salvaguardas para el personal, en este grupo se encuentra Personal Administrativo, Personal Técnico, Personal Standby

- Estimar las necesidades del personal.
- Asignar un responsable de la seguridad de la información.
- Estimar las necesidades de concientización y formación.
- Controlar las acciones de los usuarios para evitar ataques a otros sistemas.
- Anular privilegios cuando el usuario abandona la organización.
- Comprometer al usuario por escrito a mantener la confidencialidad del autenticador.
- Roles identificados Responsables de la información.
- La política debe ser conocida y aceptada por todos los afectados.
- Organización interna: coordinación interna, se identifican no conformidades e inclumplimientos, se aprueban metodologías, procedimientos, normas.
- Nombrar responsables de cada activo o proceso de seguridad.
- Crear normas de seguridad: todo el personal de la organización tiene acceso a los documentos, se revisan regularmente.
- Revisa periódicamente el cumplimiento por parte del personal.
- Se han previsto mecanismos para esta informados de vulnerabilidades del personal.
- Se estiman las necesidades de concienciación y formación.

Internet

- Concientizar en la detección y reporte de incidentes.
- Aprobar regularmente los procedimientos de gestión de incidentes.
- Dimensionar el sistema considerando necesidades futuras.

- Provocaría daños sobre la misión o negocio del sistema, perjuicios a terceros.
- Establecer canales para la comunicación de las deficiencias.
- Planificar la reparación de las vulnerabilidades que implican un riesgo bajo.
- Actualizar los procedimientos de usuario para incorporar o mejorar la identificación y forma de reaccionar ante el mismo incidente o incidentes similares.
- Actualizar, extender y mejorar u optimizar los procedimientos de resolución de incidencias.
- Identificar y analizar la causa (de un posible daño).
- Planificar la implantación de medidas correctoras.
- Identificar el personal que va a gestionar el incidente.
- Requerir autorización previa del personal que va a gestionar el incidente.
- Aprobar cada acción de emergencia por la dirección.
- Definir indicadores para la cuantificación y monitorización de las incidencias.
- Dar a conocer y aceptar las normas de seguridad a los afectados.

Dialup

- Activar, crear, modificar y eliminar las cuentas de usuario.
- Suspender temporal cuentas de usuario.
- Bloquear o eliminar las cuentas que ya no son necesarias.
- Comprobar previamente la identidad de los usuarios y los privilegios requeridos.
- Anular los privilegios cuando se termina la autorización.
- Revisar los privilegios cuando el usuario cambia de responsabilidades o de función.
- Definir roles con autorización exclusiva para realizar tareas(del sistema, de la seguridad).
- Entrada de datos.
- Identificar, caracterizar y valorar las amenazas más probables.
- Identificar y valorar las amenazas posibles.
- Identificar y valorar las vulnerabilidades posibles.
- Identificar y valorar las salvaguardas posibles.
- Disponer de normativa de identificación y autenticación.

- Disponer de procedimientos para las tareas de identificación y autenticación.
- Designar responsables.
- Evaluar el impacto en la integridad de datos.
- Evaluar el impacto de la prestación de servicios.

Red de datos

- Control de acceso a la red.
- Proveer protección frente al análisis de tráfico.
- Autenticación de nodos de red.

Bodega

- Disponer de normativa de seguridad para la protección de instalaciones.
- Disponer de una normativa para el control de accesos.
- La autorización para acceder se verifica antes de conceder el acceso.
- Mantener un registro de accesos.
- Establecer un protocolo de actuación en caso de contingencia.

5.3 REVISION DE LA POLITICA

Al finalizar el diseño de políticas de seguridad de la organización se debería definir que personas asumirán los cargos dentro del Comité de Seguridad de la Información, se debe designar una unidad de auditoría interna o en su defecto quien sea propuesto por el comité, quién será el encargado de realizar revisiones independientes sobre la vigencia e implementación de las Políticas de Seguridad.

Los directores por cada cambio que se realice deben también llevar a cabo una revisión exhaustiva, lo cual retrasa el cumplimiento de los objetivos estratégicos y apartan a los directores de sus responsabilidades de dirección. La política de seguridad de información se debe revisar en una frecuencia establecida para determinar si ocurrieron o no cambios significativos, para asegurar que siga siendo apropiada, adecuada y efectiva. Esta revisión incluye la evaluación de las oportunidades que tiene la política de seguridad de información para mejorar y un método para administrar la seguridad de información, en respuesta al entorno organizacional, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Una parte esencial de la revisión periódica de la política consiste en el mantenimiento, la cual debe tomar en cuenta los resultados de estas revisiones para mejoras futuras. Se deben crear procedimientos

definidos de revisión de la gerencia, que incluye un cronograma o fechas para la revisión.

5.4 APROBACION DE LA POLITICA

Como último paso para el diseño de políticas de seguridad es la aprobación. El objetivo de la aprobación es obtener el apoyo de la organización, esto debe ser realizado con una firma por parte de una persona que tenga una posición de autoridad dentro de la organización.

Una vez realizada la aprobación se puede dar inicio a la implementación de la política. Para esto es necesario que la persona que propone la política seleccione adecuadamente quién va a ser su autoridad aprobadora, para que conjuntamente coordine con dicho funcionario, presente las recomendaciones emitidas durante la etapa de revisión y haga el esfuerzo para que sea aceptada por la administración. También puede darse el caso de que por indesición de la autoridad de aprobación se necesite una aprobación temporal.

Las autoridades encargadas de la aprobación serán quienes tengan la responsabilidad de reconocer la importancia, de identificar y proteger los activos de información por medio de la aprobación y ejecución de esta política.

5.5 DESARROLLO DEL SGSI

Como se define en el capítulo II, el desarrollo del SGSI comprende cuatro etapas (PLAN, DO, CHECK, ACT) de las cuáles el proyecto se enfoca en las dos primeras fases:

- PLAN: Desarrollado en el capítulo III
- DO: Desarrollado en el capítulo IV

Las otras dos CHECK y ACT son las fases siguientes para el desarrollo del SGSI, pero no están contempladas para el trabajo de investigación realizado.

6 CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La adecuada elección de una buena metodología para el análisis de riesgos, es fundamental para realizar un completo estudio que tome en consideración todas las actividades necesarias para el desarrollo de las políticas de seguridad, así como también que cuente con documentación clara y guías que faciliten el diseño.
- El estudio toma como punto de partida lo expuesto en la Metodología MAGERIT con su respectiva herramienta de apoyo PILAR como una guía para el análisis y gestión de riesgos.
- La empresa no cuenta con procedimientos de seguridad guiados y documentados, como consecuencia no se puede estimar los riesgos e impactos en los activos que afecten en las actividades diarias que realiza la empresa.
- Es necesario definir que políticas son aplicables o no para una empresa de telecomunicaciones, como es el caso de las políticas para el estándar ISO 27011, ya que no todos contemplan los objetivos del negocio de la empresa Puntonet.
- No ha sido posible desarrollar las políticas con algunos de los controles del estándar ISO 27001, debido a que hay políticas referentes al uso, manejo y protección de sistemas de información y bases de datos, los cuáles son administrados en la matriz de Quito por lo cual no se tuvo todo el acceso para realizar el levantamiento de información necesaria para un análisis completo y exhaustivo.
- La empresa Puntonet presenta actualmente un estado de riesgo en ciertos activos, lo cual se puede contrarrestar con la aplicación de las actividades y tareas descritas en la política, así como llevar un control sobre el cumplimiento de las mismas. . . .

RECOMENDACIONES

- Se debe contar con la absoluta colaboración por parte del personal involucrado con los procesos de la organización, es por esa razón que se debe implantar según el manual MAGERIT I Método "una cultura de seguridad", la cual debe concientizar en todos

los niveles, es decir desde las personas que más entiendan de la materia hasta aquellos que no son expertos, de manera que todos puedan aportar al análisis de los activos esto se lo puede lograr con la creación de un foro de seguridad.

- Se debe tomar en consideración el nivel de las amenazas en los diferentes activos sobretodo en los niveles crítico, muy alto y alto ya que en caso de llevarse a cabo una amenaza podría poner en peligro el desempeño del activo. Para evitar lo mencionado es necesario brindar la atención necesaria mediante diferentes políticas.

- Es necesario que la documentación generada para la política se revise al menos una vez por año o se establezca conjuntamente con el foro de seguridad períodos para mantener la eficacia de las políticas ya que pueden darse cambios significativos en los requerimientos de seguridad de manera que esta documentación este actualizada.

- Para el desarrollo del proyecto necesariamente en el análisis de riesgos, es sumamente importante contar con amplios conocimientos estadísticos debido a que para la recolección de datos es indispensable realizar encuestas, tabulación de datos, interpretación de resultados y demás cálculos para utilizar y comprender de manera más precisa los datos obtenidos.

- La política desarrollada en lo posible debe ser clara, natural, no debe dificultar las actividades diarias, debe alcanzar los objetivos de negocio de la empresa, y permitir el cumplimiento de las buenas prácticas propuestas por los estándares tomados como referencia.

- Para un mejor desempeño de la política se debe controlar su cumplimiento a través del foro de seguridad y de no ser así aplicar sanciones. . . .

Fabio Tobón Londoño (1997). GUIA IMPLEMENTACION DE LA NORMA NTC ISO 14001. Obtenida el 15 de Noviembre de 2011. URL http://www.rosdary.files.wordpress.com/2008/03/guia-iso14000.pdf.

ISQ World (2005). Free ISO 27001 Curso de Capacitación en línea. Obtenida el 12 de Diciembre de 2011. URL http://www.isqworld.com/about-us.

Pen Y Geulan (2008). The ISO 27000 Directory. Obtenida el 02 de Octubre de 2011. URL http://www.27000.org/iso-27001.htm.

Burgos J (2010). Modelo Para Seguridad de la Información en TIC. Obtenida el 12 de Febrero de 2012a. URL http://sistemas.dis.ufro.cl/eig2008/files/papers/Burgos-Campos(pp234-253).pdfl.

Mañas J (2010). EAR / PILAR Entorno de análisis de riesgos. Obtenida el 05 de Febrero de 2012b. URL http://www.pilar-tools.com/es/index.html.

MARTIN L (2011). Diseño de un sistema de Gestión de Seguridad de la Información SGSI. Obtenida el 21 de Febrero de 2012a. URL http://eciencia.urjc.es/handle/10115/4165.

POSSO G (2011). Desarrollo e implementación de seguridad informática e implementación de tres dominios de la norma 27002. Obtenida el 17 de Enero de 2012b. URL http://dspace.epn.edu.ec/bitstream/15000/9946/1/DESARROLLO.

THE ISO DIRECTORY (2011). An Introduction to ISO 27001, ISO 27002....ISO 270. Obtenida el 25 de Febrero de 2012c. URL http://www.27000.org5.

García Guzmán P (2007) Alvarez Zurita M. IMPLEMENTACION DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO 27001, PARA LA INTRANET DE LA CORPORACION METROPOLITANA DE SALUD. Obtenida el 23 de Octubre de 2011. URL http://www.bibdigital.epn.edu.ec/handle/15000/565.

Carter Bryan and Shumway Russell. *Wireless Security end to end*. TIS082535, Wiley, USA, 1fst edition, 2002.

C.Alberts and A.Dorofree. *Managing information Security risks*. Addison–Wesley, Adison, Wesley, 1fst edition, 2003.

Comité de la Seguridad de la Información (2009). POLITICAS DE SEGURIDAD DE LA INFORMACION. Obtenida el 14 de Octubre de 2011. URL http://www.utn.edu.ar/download.aspx?idFile=14736.

Magerit v2 (2006). EAR / PILAR - Entorno de Análisis de Riesgos. Obtenida el 13 de Noviembre de 2011. URL https://www.ccn-cert.cni.es/publico/herramientas/pilar43/magerit/index.html.

7 ANEXOS

7.1 ANEXO A: CATÁLOGO DE IDENTIFICACIÓN DE ACTIVOS

La metodología presenta un grupo de tipos de activos dentro de los cuales se especifican diferentes activos que se pueden emplear y a los que se les atribuye un código. Estos activos no pueden ser exhaustivos, si es necesario especificar un activo importante la metodología lo admite de igual manera este activo puede pertenecer a varios tipos de activos.

A continuación se presentan los tipos de activos de MAGERIT.

[S] Servicios

Aquí se encuentran:

- Servicios públicos prestados por la Administración para satisfacer necesidades de la colectividad;
- Servicios empresariales prestados por empresas para satisfacer necesidades de sus clientes;
- Servicios internos prestados por departamentos especializados dentro de la Organización, que son usados por otros departamentos u empleados de la misma; etc.
- Servicios prestados por la Organización a terceros.
- Servicios instrumentales donde tanto los usuarios como los medios son propios.
- Servicios contratados a otra organización que los proporciona con sus propios medios.

[D] Datos / Información

Los datos permiten a una organización prestar sus servicios. Se los puede considerar como un activo abstracto que se almacenará en equipos o soportes de información o será trasladado de un lugar a otro por los medios de transmisión de datos.

[SW] Aplicaciones (software)

Este tipo de activo se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

[HW] Equipos informáticos (hardware)

Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

[COM] Redes de comunicaciones

Incluye instalaciones dedicadas y servicios de comunicaciones contratados a terceros que se encargan de llevar datos de un sitio a otro.
[SI] Soportes de información

Contiene los dispositivos físicos en donde se almacena información de forma permanente o, durante largo periodos de tiempo.
[AUX] Equipamiento auxiliar

Considera otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[L] Instalaciones

Contiene los lugares donde se albergan los sistemas de información y comunicaciones.
[P] Personal

Personal concernidas con los sistemas de información.

7.2 ANEXO B: CRITERIOS DE VALORACIÓN ADICIONALES

Lo más normal es que un activo reciba una simple valoración en cada dimensión en la que es valioso. Este planteamiento puede y debe ser enriquecido en el caso de dimensiones más complejas como es el caso de la disponibilidad, en la que las consecuencias varían dependiendo del tiempo que dure la interrupción. En estos casos, la dimensión no recibe una única calificación, sino tantas como escalones se hayan considerado relevantes. Los criterios que siguen se aplican en cada escalón, pudiendo variar el motivo.

Valor: 10

[olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

[iio] Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información

[si] Seguridad: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[ps] Seguridad de las personas: probablemente suponga gran pérdida de vidas humanas

[po] Orden público: alteración seria del orden constitucional

[ir] Probablemente cause un impacto excepcionalmente grave en las relaciones internacionales

[lbl] Datos clasificados como secretos

Valor: 9

[da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

[adm] Administración y gestión: probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre

[lg] Probablemente causaría causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones

- **[lg.a]** a las relaciones con otras organizaciones
- **[lg.b]** a las relaciones con el público en general
- **[lg.c]** a las relaciones con otros países

[olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa logística

[iio] Probablemente cause serios daños a misiones muy importantes de inteligencia o información
[cei] Intereses comerciales o económicos:

- **[cei.a]** de enorme interés para la competencia
- **[cei.b]** de muy elevado valor comercial
- **[cei.c]** causa de pérdidas económicas excepcionalmente elevadas
- **[cei.d]** causa de muy significativas ganancias o ventajas para individuos u organizaciones
- **[cei.e]** constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

[lro] Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
[si] Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[ps] Seguridad de las personas: probablemente suponga la muerte de uno o más individuos
[po] Orden público: alteración seria del orden público
[ir] Probablemente cause un serio impacto en las relaciones internacionales
[lbl] Datos clasificados como reservados
Valor: 8
[ps] Seguridad de las personas: probablemente cause daño a la seguridad o libertad individual (por ejemplo, es probable que llegue a amenazar la vida de uno o más individuos)
[crm] Impida la investigación de delitos graves o facilite su comisión
[lbl] Datos clasificados como confidenciales
Valor: 7
[da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones **[adm]** Administración y gestión: probablemente impediría la operación efectiva de la organización
[lg] Probablemente causaría una publicidad negativa generalizada

- **[lg.a]** por afectar gravemente a las relaciones con otras organizaciones
- **[lg.b]** por afectar gravemente a las relaciones con el público en general
- **[lg.c]** por afectar gravemente a las relaciones con otros países

[olm] Probablemente cause perjudique la eficacia o seguridad de la misión operativa o logística
[iio] Probablemente cause serios daños a misiones importantes de inteligencia o información
[cei] Intereses comerciales o económicos:

- **[cei.a]** de alto interés para la competencia
- **[cei.b]** de elevado valor comercial

- **[cei.c]** causa de graves pérdidas económicas
- **[cei.d]** proporciona ganancias o ventajas desmedidas a individuos u organizaciones
- **[cei.e]** constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

[lro] Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
[si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[ps] Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos
[ir] Probablemente cause un impacto significativo en las relaciones internacionales
[lbl] Datos clasificados como confidenciales
Valor: 6
[pi1] Información personal: probablemente afecte gravemente a un grupo de individuos
[pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[ps] Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo
[po] Orden público: probablemente cause manifestaciones, o presiones significativas
[lbl] Datos clasificados como de difusión limitada
Valor: 5
[da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la organización
[lg] Probablemente sea causa una cierta publicidad negativa
[lg.a] por afectar negativamente a las relaciones con otras organizaciones
[lg.b] por afectar negativamente a las relaciones con el público
[olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
[iio] Probablemente dañe a misiones importantes de inteligencia o información
[pi1] Información personal: probablemente afecte gravemente a un individuo
[pi2] Información personal: probablemente quebrante seriamente leyes o regulaciones
[lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación
[ir] Probablemente tenga impacto en las relaciones internacionales
[lbl] Datos clasificados como de difusión limitada
Valor: 4
[pi1] Información personal: probablemente afecte a un grupo de individuos
[pi2] Información personal: probablemente quebrante leyes o regulaciones
[ps] Seguridad de las personas: probablemente cause daños menores a varios individuos
[crm] Dificulte la investigación o facilite la comisión de delitos
[lbl] Datos clasificados como de difusión limitada

Valor: 3
[da] Probablemente cause la interrupción de actividades propias de la Organización
[adm] Administración y gestión: probablemente impediría la operación efectiva de una parte de la organización
[lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
[iio] Probablemente cause algún daño menor a misiones importantes de inteligencia o información
[cei] Intereses comerciales o económicos:

- **[cei.a]** de cierto interés para la competencia
- **[cei.b]** de cierto valor comercial
- **[cei.c]** causa de pérdidas financieras o merma de ingresos
- **[cei.d]** facilita ventajas desproporcionadas a individuos u organizaciones
- **[cei.e]** constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros

[pi1] Información personal: probablemente afecte a un individuo
[pi2] Información personal: probablemente suponga el incumplimiento de una ley o regulación
[lro] Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[si] Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[ps] Seguridad de las personas: probablemente cause daños menores a un individuo
[po] Orden público: causa de protestas puntuales
[ir] Probablemente cause un impacto leve en las relaciones internacionales
[lbl] Datos clasificados como de difusión limitada
Valor: 2
[lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización
[cei] Intereses comerciales o económicos:

- **[cei.a]** de bajo interés para la competencia
- **[cei.b]** de bajo valor comercial

[pi1] Información personal: pudiera causar molestias a un individuo
[pi2] Información personal: pudiera quebrantar de forma leve leyes o regulaciones
[ps] Seguridad de las personas: pudiera causar daño menor a varios individuos
[lbl] Datos clasificados como sin clasificar
Valor: 1
[da] Pudiera causar la interrupción de actividades propias de la Organización

[adm] Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización
[lg] Pudiera causar una pérdida menor de la confianza dentro de la Organización
[olm] Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[iio] Pudiera causar algún daño menor a misiones importantes de inteligencia o información
[cei] Intereses comerciales o económicos:
[cei.a] de pequeño interés para la competencia
[cei.b] de pequeño valor comercial
[pi1] Información personal: pudiera causar molestias a un individuo
[lro] Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[ps] Seguridad de las personas: pudiera causar daños menores a un individuo
[po] Orden público: pudiera causar protestas puntuales
[ir] Pudiera tener un impacto leve en las relaciones internacionales
[lbl] Datos clasificados como sin clasificar
Valor: o
[1] no afectaría a la seguridad de las personas
[2] sería causa de inconveniencias mínimas a las partes afectadas
[3] supondría pérdidas económicas mínimas
[4] no supondría daño a la reputación o buena imagen de las personas u organizaciones

7.3 ANEXO C: CATÁLOGO DE AMENAZAS

A continuación se presenta un catálogo de amenazas para cada uno de los tipos de activos, indicando las dimensiones afectadas.
[N]Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[N.1] Fuego Incendios: posibilidad de que el fuego acabe con recursos del sistema.
[N.2] Daños por agua Inundaciones: posibilidad de que el agua acabe con recursos del sistema.
[N.*] Desastres Naturales: Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras. Se excluyen desastres específicos tales como incendios e inundaciones. Se excluye al personal por cuanto se ha previsto una amenaza específica para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.
[I] De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
[I.1] Fuego Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
[I.2] Daños por agua: Escapes, fugas, inundaciones posibilidad de que el agua acabe con los recursos del sistema.

[I.*] Desastres industriales: Otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas,accidentes de tráfico. Se excluyen amenazas específicas como incendioe inundación. Se excluye al personal por cuanto se ha previsto una amenaza específica, para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.

[I.3] Contaminación mecánica: Vibraciones, polvo, suciedad.

[I.4] Contaminación electromagnética: Interferencias de radio, campos magnéticos, luz ultravioleta.

[I.5] Avería de origen físico o lógico: Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

[I.6] Corte de suministro eléctrico: Cese de la alimentación de potencia.

[I.7] Condiciones inadecuadas de temperatura y/o la humedad: Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.

[I.8] Fallo de servicios de comunicaciones: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

[I.9] Interrupción de otros servicios y suministros esenciales: Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante.

[I.10] Degradación de los soportes dealmacenamiento de la información: Como consecuencia del paso del tiempo.

[I.11] Emanaciones electromagnéticas: Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST. Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "TEMPEST protection", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.

[E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

[E.1] Errores de los usuarios: Equivocaciones de las personas cuando usan los servicios, datos, etc.

[E.2] Errores del administrador: Equivocaciones de personas con responsabilidades de instalación y operación.

[E.3] Errores de monitorización (log): Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.

[E.4] Errores de configuración: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

[E.7] Deficiencias en la organización: Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.

[E.8] Difusión de software dañino: Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

[E.9] Errores de [re-]encaminamiento: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información adonde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.

[E.10] Errores de secuencia: Alteración accidental del orden de los mensajes transmitidos.

[E.14] Escapes de información: La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.

[E.15] Alteración de la información: Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.16] Introducción de información incorrecta: Inserción accidental de información incorrecta. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.17] Degradación de la información: Degradación accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.18] Destrucción de información: Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[E.19] Divulgación de información: Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.

[E.20] Vulnerabilidades de los programas (software): Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.

[E.21] Errores de mantenimiento / actualización de programas (software): Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

[E.23] Errores de mantenimiento / actualización de equipos (hardware): Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

[E.24] Caída del sistema por agotamiento de recursos: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[E.28] Indisponibilidad del personal: Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.

[A] Ataques intencionados

Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

[A.4] Manipulación de la configuración: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

[A.5] Suplantación de la identidad del usuario: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.

[A.6] Abuso de privilegios de acceso: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.

[A.7] Uso no previsto: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[A.8] Difusión de software dañino: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

[A.9][Re-]encaminamiento de mensajes (email): Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.

[A.10] Alteración de secuencia: Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.

[A.11] Acceso no autorizado: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.12] Análisis de tráfico: El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico".

[A.13] Repudio: Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.

[A.14] Interceptación de información (escucha): El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.

[A.15] Modificación de la información: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la

información está en algún soporte informático, hay amenazas específicas.

[A.16] Introducción de falsa información: Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[A.17] Corrupción de la información: Degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[A.18] Destrucción la información: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

[A.19] Divulgación de información: Revelación de información.

[A.22] Manipulación de programas: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

[A.24] Denegación de servicio: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.25] Robo: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

[A.26] Ataque destructivo: Vandalismo, terrorismo, acción militar. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.

[A.27] Ocupación enemiga: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

[A.28] Indisponibilidad del personal: Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.

[A.29] Extorsión: Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.

[A.30] Ingeniería social: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

7.4 ANEXO 1: METODOLOGÍA DE ANÁLISIS DE RIESGOS

Análisis de Riesgos

La seguridad de la Información comprende una serie de etapas, entre ellas está el Análisis de Riesgos, siendo esta una de las fases principales para el desarrollo de proyectos debido a que recoge datos indispensables y relevantes acerca de los activos, actividades y procesos que maneja una organización, con los cuales se realizan estudios posteriores acerca de amenazas que pudieran afectar activos.

El propósito de esto comprende el asegurar la continuidad del negocio y minimizar los riesgos o daños posibles sobre activos que maneje la

Figure 37: Proceso del Análisis de Riesgos

organización, mediante la aplicación de salvaguardas como se muestra en la figura 4.1 37

Descripción de la Metodologia de Analisis de Riesgos

Podemos encontrar varias herramientas metodológicas enfocadas en el análisis y tratamiento de los riesgos que se pueden presentar en el desarrollo de las actividades diarias de una organización.

Debido a los beneficios que puede brindar disponer de una metodología dentro de las actividades regulares de la organización se ve necesario incorporarla formalmente para que éstas actúen conjuntamente.

Esta metodología es el resultado de la combinación de diferentes propuestas existentes en la industria, y utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero, por ejemplo, en el caso de la selección de los controles adecuados, para mitigar un posible evento negativo a la operación y continuidad del negocio.

Descipción de Metodologías

Entre las metodologías más utilizadas para el Análisis de Riesgos de la Información tenemos:

- MAGERIT
- Cobit
- Octave

Magerit

Fue desarrollada por el Consejo Superior de Administración Electrónica que hace parte del Ministerio de Administraciones Publicas de España (CSAE)[1]. Es una metodología formal para analizar los riesgos presentes y para recomendar las medidas adecuadas que deberían tomarse en cuenta para controlar los riesgos en un momento dado.

1 El Consejo Superior de Administración Electrónica es el órgano adscrito al Ministerio de Hacienda y Administraciones Públicas de España, encargado de la preparación, la elaboración, el desarrollo y la aplicación de la política y estrategia del Gobierno en materia de tecnologías de la información.

Objetivos

- Sensibilizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de mitigarlos a tiempo
- Ofrecer un método ordenado para analizar tales riesgos
- Definir y planificar las medidas oportunas para mantener los riesgos bajo control
- Apoyar la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso
- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él.
- Señalar los riesgos existentes, identificando las amenazas que acechan al sistema de información, y
- Determinar las vulnerabilidades del sistema de prevención de dichas amenazas, obteniendo unos resultados.

Al obtener los resultados del análisis de riesgos estos permiten realizar una gestión de riesgos, recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

Principales Elementos

1. Método: describe la secuencia de pasos a seguir para realizar un completo análisis y gestión de riesgos. Además detallas las actividades y documentación necesarias para tener bajo control el desarrollo del proyecto.
2. Catálogo de Elementos: contiene información detallada de los activos así como su identificación, valoración, criterios para la valoración, de igual manera para las amenazas y salvaguardas.
3. Guía de Técnicas: esta guía especifica técnicas algorítmicas para la obtención de resultados para nuestro caso de estudio como es el modelo cuantitativo.

Cobit

Fue desarrollada por la Information Systems Audit and Control Association (ISACA)[2] y el IT Governance Institute (ITGI)[3]. Es una metodología aceptada en todo el mundo para el adecuado control de

2 Organización proveedora de certificaciones, comunidad, apoyo y educación en seguridad y aseguramiento de sistemas de información, gobierno empresarial, administración de TI así como riesgos y cumplimiento relacionados con TI.

3 Entidad sin fines de lucro, de investigación independiente que proporciona orientación a la comunidad mundial de negocios sobre temas relacionados con el gobierno empresarial de los activos de TI.

proyectos de tecnología, los flujos de información y los riesgos que éstas implican.

La metodología COBIT se utiliza para planear, implementar, controlar y evaluar la administración en una tecnología de la información, incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

Objetivos:

- Determinar un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en el negocio con el respaldo de las principales normas técnicas internacionales.
- Brindar métricas y modelos de madurez para medir logros del negocio.
- Brindar un modelo de procesos genéricos.
- Establecer una adecuada administración de riesgos.

Octave

Es un método de análisis de riesgos orientado a activos, desarrollado por el CERT[4], Estados Unidos. En OCTAVE, los activos incluyen personas, hardware y software, información y sistemas. Los activos se ordenan según la importancia que tienen para los objetivos de la organización, y las posibles amenazas y vulnerabilidades asociadas a dichos activos, así como el impacto que causaría un problema en cada activo.

Objetivos

• Desarrollar una perspectiva de seguridad dentro de una organización, tomando en consideración todos los niveles para asegurarse que las soluciones puedan implementarse con facilidad.

• Construcción de los perfiles de amenazas basados en Activos

• Identificación de la infraestructura de vulnerabilidades

• Desarrollo de planes y estrategias de seguridad

Principales Elementos de Octave:

- Medidas de probabilidad considerando un rango de frecuencias.
- Análisis del límite entre niveles de probabilidad.

Justificación de la Metodología MAGERIT

Una vez realizada una comparación entre las metodologías ya mencionadas para la realización de nuestro estudio se ha optado por la Metodología MAGERIT debido a las siguientes características:

- Documentación detallada acerca del análisis y gestión de riesgos.

4 Organización que se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo, así como publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones.

Valor		Criterio
10	muy alto	**daño muy grave a la organización**
7-9	alto	**daño grave a la organización**
4-6	medio	**daño importante a la organización**
1-3	bajo	**daño menor a la organización**
0	despreciable	**irrelevante a efectos prácticos**

Table 14: Criterios de valoración de activos Fuente: MAGERIT

- Cuenta con una completa documentación en español, que detalla los pasos a seguir.

MAGERIT Está estructurado en tres guías completas que describen una serie de aspectos prácticos para realizar un análisis del estado de riesgo, y para gestionar su mitigación. Cuenta con un software llamado PILAR[5], que sirve como herramienta para facilitar su desarrollo, el cual permite mediante la identificación de activos generar tablas de impactos, riesgos, gráficos, así como exportar todos los datos generados.

La herramienta soporta todas las etapas de la metodología MAGERIT:

- Caracterización de los activos
- Caracterización de las amenazas
- Evaluación de las salvaguardas

La herramienta estima calificaciones de seguridad siguiendo los controles establecidos en las normas ISO. Cabe citarse:

- Criterios de Seguridad, normalización y conservación
- UNE-ISO/IEC 17799:2002: sistemas de gestión de la seguridad

7.5 ANEXO 2: VALORACIÓN DE LOS ACTIVOS

ENCUESTA PARA LA VALORACIÓN DE ACTIVOS

¿Un deterioro o pérdida en el activo Netplus cuanto impacta la confidencialidad, integridad y disponibilidad en sus actividades diarias?

- ¿Un deterioro o pérdida en el Sistema Netplus cuanto impacta en la facturación?
- ¿Un deterioro o pérdida en el Sistema Netplus cuanto impacta en la atención al cliente?
- ¿Un deterioro o pérdida en el Sistema Netplus cuanto impacta en el soporte técnico?
- ¿Un deterioro o pérdida en el Sistema Netplus cuanto impacta en la instalación?

5 PILAR, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia (España) para soportar el análisis de riesgos de sistemas de información siguiendo la metodología MAGERIT.

7.6 ANEXO 3: SOLICITUD LICENCIA PILAR

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

Cuenca, 17 mayo de 2012

Sr. José A. Mañas
Su despacho

De mi consideración,

Reciba un cordial saludo de parte de la Universidad Politécnica Salesiana del Ecuador sede Cuenca, mi nombre es Byron Carrión Ramírez, supervisor de la tesis de grado de las estudiantes Jessica Maricela Avilés, María Elisa Uyaguari, intitulada DESARROLLO DE UNA POLÍTICA DE SEGURIDAD PARA LA EMPRESA DE TELECOMUNICACIONES PUNTONET EN LA CIUDAD DE CUENCA, EN BASE A LAS NORMAS DE SEGURIDAD ISO 27001 Y 27011 COMO LÍNEAS BASE PARA LAS BUENAS PRÁCTICAS DE TRATAMIENTO Y SEGURIDAD DE LA INFORMACIÓN.

El motivo de la presente es solicitar a usted la concesión de una licencia temporal completa para el software PILAR por un período mínimo de 2 meses, tiempo necesario para concluir la investigación, verificar y presentar resultados.

Asegurando, además, nuestro compromiso de utilizar la licencia exclusivamente en nuestra institución.

Seguro de contar con su colaboración, agradezco su apoyo para con el avance de este proyecto científico-educativo de investigación.

Ing. Byron Carrión

DOCENTE UNIVERSIDAD POLITÉCNICA SALESIANA

CARRERA DE INGENIERÍA EN SISTEMAS

SEDE CUENCA • Calle Vieja 12-30 y Elia Liut • Casilla 46 Sect. 2 • Telf.: 2862213 Ext. 1237 • Fax: (593 7) 2869117
E-mail: dsistemascue@ups.edu.ec • http://www.ups.edu.ec • Cuenca - Ecuador

Figure 38: Solicitud licencia PILAR