UNIVERSIDAD NACIONAL DE INGENIERÍA

Facultad de Ingeniería Industrial y de Sistemas

MEJORA DE LOS NIVELES DE SEGURIDAD DE INFORMACIÓN EN LAS PLATAFORMAS DE SISTEMAS – SERVIDORES

INFORME DE SUFICIENCIA

Para optar el Titulo Profesional de

INGENIERO DE SISTEMAS

MARCO ANTONIO PALOMINO PIO

LIMA – PERU

2008

A mis padres, quienes han sido el motor y fuente de motivación en el cumplimiento de estos años de carrera. Gracias por su apoyo constante e incondicional. Esto es para ustedes.

Pedro Palomino De la Cruz
Emerida Pio Silva

A mis Hijos, por quienes lucho todos los días de mi vida. Les dedico este logro.

Jairo y Gianfranco

AGRADECIMIENTOS

A Dios, por haberme dado la fortuna de la vida y por haberme permitido llevar esta carrera.

A mi esposa María Elena LLaury, por su gran ayuda, motivación y apoyo incondicional durante el desarrollo de este informe.

A mis hermanos Enrique y Franklin, por ser los motivadores del inicio de este camino.

A Irma Inga, Samuel Oporto y Celedonio Méndez por su incondicional colaboración, guía y asesoramiento en el presente informe.

ÍNDICE

Pág.

ÍNDICE DE TABLAS Y FIGURAS

Pág.

DESCRIPTORES TEMÁTICOS

1) Seguridad de Información

2) Plataforma de Sistemas

3) Servidores

4) Análisis de Riesgos

5) Retorno de la Inversión

6) Modelo PDCA

RESUMEN EJECUTIVO

Durante el periodo 2003 y 2004, en la Empresa ABC; que pertenece a un grupo de empresas como telefonía local, telefonía móvil, cable, y a la vez les presta servicios de Consultoría y Sistemas de Información, Recursos Humanos, Inmobiliaria, Recaudación y cobranzas, entre otros; se presentó cuatro casos de robos de información confidencial, dos denuncias legales por la no protección de información, doce casos reportados por usuarios que su información ha sido eliminada y dos casos de indisponibilidad de la plataforma de sistema o servidor de archivos. Después de revisiones y auditorias, por parte de consultoría externa en el 2006, se identificó que 32 plataformas de sistemas o servidores (críticos por la información que contienen) tiene un nivel de seguridad promedio de 29.3% y todos los servidores no superan el 40% de las recomendaciones de buenas prácticas de control de accesos, siendo la política de ésta cumplir por lo menos con el 90% de las mismas para tener un nivel adecuado de seguridad de información.

Para mejorar los niveles de seguridad, evalúa la contratación de consultoría externa para que brinde asesoría en el tema. De tres alternativas elige la alternativa que compone al proveedor B y producto ESM, el cual obtuvo la mayor calificación con un 74.7% de nivel de cumplimiento de los criterios de evaluación. Se adquiere el producto ESM para facilitar la labor administrativa de elaboración de reportes, configuraciones, control y evaluaciones del cumplimiento de configuraciones de Seguridad de Información

Se realiza un análisis de riesgos identificando vulnerabilidades de gestión de cuentas, gestión de contraseñas, configuraciones de acceso en las plataformas de sistemas, y responsabilidad de los usuarios en la seguridad de información. Asimismo se ha identificado amenazas como robo de información, denegación de servicio a toda la red corporativa; eliminación, modificación o divulgación de información confidencial, infección con virus; calculando un impacto de 851,803 soles anuales. Para tratar los riesgos se implanta procedimientos, producto ESM; configuraciones, validación y eliminación de accesos, capacitación y charlas de seguridad de información. Calculando una inversión de 597,936 para el desarrollo del proyecto con una duración de seis meses calendario. El retorno de inversión del proyecto es de ocho meses y medio, con un ahorro anual de 271,867 soles.

Al evaluar los resultados del proyecto se encontró que 28 de los 32 servidores superan el 90% de recomendaciones de buenas prácticas de control de accesos con un nivel de seguridad promedio de todos los servidores de 91.6% mejorando en un 62.3% comparado con la medición realizada antes de iniciar el proyecto.

INTRODUCCIÓN

En la actualidad, la información se considera un activo estratégico por lo que surge una fuerte necesidad de protegerla y de precaver su mal uso. Debido a ello, los gerentes, ejecutivos y administradores, se ven cada vez en la necesidad de implantar o mejorar la seguridad de información de su empresa y evitar consecuencias como sabotaje, robo de datos e ingreso de virus, el cual acarrea costos a la empresa o pérdida de oportunidades de negocio.

El informe encargado por MCafee del 5 de julio de 2005 [CHAR05] establece un panorama claro de la crecientes amenazas y delitos que se cometen mediante Internet, los aspectos más destacados del informe indican: el FBI estima que el crimen cibernético costó aproximadamente US$400 mil millones en el año 2004, en una investigación denominada "Operation Firewall" las autoridades estadounidenses y canadienses anunciaron el arresto de 28 personas de seis países, que estaban involucradas en una red mundial de crimen cibernético organizado, según estimaciones, probablemente sólo el 5% de los criminales cibernéticos son capturados y procesados

La seguridad de la información tiene como propósito proteger la información de las empresas. Por esto, la seguridad de la información es un asunto importante para todos, pues afecta directamente a los negocios de una empresa como a los individuos que hacen parte de ella. Es por ello que

hoy en día las empresas buscan la mejor forma de asegurar la organización y los recursos de la misma.

El motivo del presente es desarrollar un proyecto de mejora de los niveles de seguridad de información en las plataformas de sistemas, dividido en cuatro secciones: antecedentes: referido al diagnostico estratégico y funcional de la empresa· marco teórico relacionado a temas de seguridad de la información; proceso de toma de decisiones en la que se indica la problemática, se define el problema y se brinda modelos, metodologías de evaluación de proveedores, análisis de riesgos, retorno de inversión en seguridad de información e implantación de la solución basada en el modelo PDCA (Plan-Do-Check-Act: Planificar, Hacer, Revisar, Mejorar) de implantación de un Sistema de Gestión de la Seguridad de Información de la norma ISO 27001; y en la ultima sección se evalúa los resultados de la solución implantada.

CAPÍTULO I

ANTECEDENTES

1.1 DIAGNÓSTICO ESTRATÉGICO

La empresa desea ofrecer a las empresas líderes la oportunidad de rentabilizar sus operaciones y optimizar su negocio a través de la tercerización de sus áreas administrativas. Así, la empresa podrá concentrar en las actividades centrales de su negocio y delegar los temas de soporte a las operaciones en manos de especialistas.

1.1.1 Visión y Misión de la empresa

VISIÓN

Ser una empresa líder en la provisión de servicios integrales e integrados en el mercado nacional y regional, generando valor para nuestros clientes a través de la satisfacción de sus necesidades con servicios de calidad a precios competitivos.

MISIÓN

Prestar servicios integrales para satisfacer las necesidades de todos nuestros clientes, liberándolos de gestiones ajenas a su actividad, alcanzando los acuerdos de nivel de servicio, con precios competitivos, actuando de forma profesional y eficiente.

1.1.2 Objetivos estratégicos

Financiera

- Incrementar los ingresos manteniendo la rentabilidad de la compañía.
- Reducir costos de nuestros clientes.

Personal

- Desarrollar el Capital Humano, integrado, fidelizado y capacitado.
- Fortalecer la cultura de servicio orientado al cliente.
- Fomentar una cultura de creatividad e innovación.

Procesos

- Incrementar la calidad y eficiencia operacional.
- Desarrollar soluciones creativas para las necesidades del cliente.

Clientes

- Satisfacer y fidelizar a nuestros clientes.
- Posicionarse como proveedor de servicios integrales.

Seguridad de Información Corporativa

- Cumplimiento de la normativa corporativa de seguridad de información
- Certificación ISO /BS 27001 de los procesos de negocio y servicios mas relevantes
- Adecuación a las ley Sarbanes Oxley
- Cumplimiento de los requerimientos legales y regulatorios
- Establecimiento de plan de continuidad de Negocio

1.1.3 Fortalezas y Debilidades

Fortalezas

- Liderazgo en volumen de actividad, acostumbrados a dar servicio a empresas con gran volumen de negocio.
- Eficiencia y Calidad: Ofrece servicio eficiente y de calidad basado en las mejores prácticas y la homogeneización de los procesos, sujetos a mejora continua y soportada por la tecnología más adecuada, según cada caso.
- Amplio catálogo de servicios que permite cubrir la gran diversidad de necesidades de los clientes.

Debilidades

- Deficientes controles de accesos en los sistemas de información.
- Clientes no satisfechos

1.1.4 Oportunidades y Amenazas

Oportunidades

- Captar clientes externos fuera del grupo.
- Aprovechamiento de nuevas tecnologías.

Amenazas

- Robo de Información.
- Constante presión política.
- Competencia agresiva.

1.1.5 Matriz FODA: Fortaleza Oportunidades Debilidades y Amenazas

En la Tabla 1.1 se muestra la Matriz FODA. Donde la combinación de las Fortalezas y Debilidades con las oportunidades y Amenazas da como resultado los objetivos estratégicos de la empresa.

Matriz FODA	OPORTUNIDADES O1: Captar clientes externos fuera del grupo O2: Aprovechamiento de nuevas tecnologías	AMENAZAS A1: Robo de Información A2: Constante presión política A3: Competencia agresiva
FORTALEZAS F1: Liderazgo en volumen de actividad, acostumbrados a dar servicio a empresas con gran volumen de negocio F2: Eficiencia y Calidad: Ofrece servicio eficiente y de calidad basado en las mejores prácticas y la homogeneización de los procesos, sujetos a mejora continua y soportada por la tecnología más adecuada, según cada caso F3: Amplio catálogo de servicios que permite cubrir la gran diversidad de necesidades de los clientes	O1 y F1: Incrementar los ingresos manteniendo la rentabilidad de la compañía. O1 y F3: Posicionarse como proveedor de servicios integrales. O2 y F2: Reducir costos de nuestros clientes.	A3 y F2: Incrementar la calidad y eficiencia operacional
DEBILIDADES D1: Deficientes controles de accesos en los sistemas de información D2: Clientes no satisfechos	O2 y D2: Satisfacer y fidelizar a nuestros clientes	A1 y D1: Cumplimiento de la normativa corporativa de seguridad de información A2 y D1: Cumplimiento de los requerimientos legales y regulatorios

Tabla 1-1. Matriz FODA

1.2 DIAGNÓSTICO FUNCIONAL

1.2.1 Productos y/o Servicios

Ofrece un amplio catálogo de Servicios Integrados a las empresas que quieran externalizar actividad administrativa o de soporte a la gestión, no vinculada directamente al negocio, con el fin de reducir costos operativos y mejorar la eficiencia de su negocio. Estos servicios pueden englobarse en las siguientes grandes líneas de actividad.

Servicios de Consultoría y Sistemas de Información

Orienta la optimización e innovación de procesos o modelos de negocio, impulsando cambios y mejoras, que causan un evidente beneficio alineado a los objetivos estratégicos de nuestros clientes, brindándoles soluciones integrales a sus problemas.

- Consultoría
  - De solución integral orientada a resolver su problemática. Propone soluciones factibles analizando hechos concretos.
  - Lidera la implantación del cambio desarrollando estrategias frente a las dificultades.
  - Se tiene Know How de los procesos de negocio.
  - Asegura la máxima participación del cliente en todo lo que hace, de modo que, el éxito final se logre en virtud del esfuerzo de ambos.
  - Establece una relación de ayuda que facilita a los clientes a la adaptación a nuevas circunstancias.
  - Consultoría de Procesos.
  - Consultoría SAP.
  - Fábrica SAP: Ejecución de la construcción, mantenimiento o configuración específica a partir de la especificación.

- Gestión de Infraestructuras de Tecnologías de Información
  - Desarrollo de Proyectos.
    - Implementación de nuevas plataformas.
    - Migración de entornos existentes.
  - Soporte y Gestión.
    - Plataformas de servidores.
    - Plataformas de almacenamiento.
    - Plataforma desktop.
    - Servicios de mensajería y administración de red.
    - Soporte de base de datos.
    - Comunicaciones.
    - Soporte microinformático (Help Desk).
    - Seguridad de información.

Servicios de Recursos Humanos

Asistir a las empresas en la gestión de su capital humano, mediante las más actualizadas tecnologías y prácticas existentes en el mercado, adecuándonos a las necesidades de cada cliente

- Administración de Personal
- Gestión de Nómina y Beneficios
- Asesoría en Relaciones Individuales
- Gestión de la Capacitación
- Proyección Social
- Selección de Personal
- Gestión de Expatriados
- Productos de Recursos Humanos

Servicios de Gestión Integral Inmobiliaria

Brindar un servicio integral, desde la definición de sus necesidades inmobiliarias hasta la adaptación y mantenimiento de sus instalaciones sin barreras geográficas.

- Gestión del Patrimonio Inmobiliario

- Administración del Mantenimiento de Inmuebles
- Diseño y Gerencia de Proyectos Inmobiliarios
- Servicios Integral de Mensajería
- Administración del Parque Móvil
- Gestión Integral del Servicio de Taxi.
- Gestión de Adquisición y Distribución de Útiles de Oficina.
- Gestión de Adquisición y Distribución de Agua de Mesa.
- Gestión de Archivo Documental.

Servicios de Gestión de Seguridad Física

Ofrece una solución integral que comprende la planificación, organización y supervisión permanente de actividades de seguridad para la protección de los recursos de su empresa.
La seguridad, un recurso integrado al negocio

- Consultoría y Asesoría en Seguridad Física
- Gestión de Seguridad Física (vigilancia y guardianía)
- Gestión de Eventos
- Productos de Seguridad

Servicios de Recaudación y Cobranza

Presta servicios integrales de recaudación, con una cobertura de más de 250 puntos interconectados a nivel nacional, lo que facilita la cobranza en línea, adicionalmente somos especialistas en servicios de gestión de cobranza con personal especializado en banca, comercio, industria, minería y empresas públicas.

- Servicios Integrales de Recaudación
- Gestión de Registro y Control
- Servicios de Control y Administración de Stocks Valorados
- Gestión de Cobranza

Servicios de Gestión Logística

Integramos los diferentes eslabones de la Cadena de Suministros con el objetivo de satisfacer las necesidades de nuestros clientes, a través de servicios innovadores, adecuada infraestructura, y avanzada tecnología que les permite visualizar en línea sus inventarios.

- Recepción
- Control de Calidad
- Almacenamiento
- Picking y Despacho
- Distribución
- Toma de inventarios

Servicios de Contabilidad, Tesorería y Tributos

Nuestros servicios pueden integrarse con facilidad a los procesos de nuestros clientes y, por ende, ser brindados en forma integral o específica, manteniendo los niveles de oportunidad, confiabilidad y certeza que se requieren y soportados por altos niveles técnicos y con experiencia.

- Contabilidad General
- Contabilidad Analítica
- Contabilidad Regulatoria
- Cuentas por Pagar
- Activo Fijo y Existencias
- Conciliaciones Bancarias
- Cumplimiento Tributario
- Gestión de Pagos y Garantías
- Administración de Valores

1.2.2 Clientes

Esta conformada solamente por las empresas del Grupo:

- Telecomunicaciones
- Servicios de Telefonía Móvil
- Televisión por Cable
- Servicios de Telemarketing
- Transmisión de Datos
- Recaudación
- Procesamiento de Imágenes
- Educación y Cultura
- Comercialización
- Mensajería
- Seguros
- Servicios Editoriales
- Comunicación por Fibra Óptica
- Servicios de Entretenimiento por Internet
- Mantenimiento de Equipos
- Transmisión de Señal de Audio y video

1.2.3 Proveedores

- Microsoft
- IBM
- HP
- Bafing
- Trendcorp
- Licencias Online
- RSA
- Adexus
- ITSYS Peru
- Softland Peru S.A.

- Avances Tecnológicos
- Comsa
- Cosapi
- Inexxo
- Sicorp
- Oracle

1.2.4 Procesos

La empresa tiene diversos procesos por cada servicio que brinda a sus clientes. Para materia de este informe se menciona los procesos relacionados a la Gestión de la Seguridad de información en los sistemas informáticos.

1.2.4.1 Atención de Requerimientos

Este proceso comprende la atención de requerimientos informáticos, desde que el cliente lo solicita hasta que la empresa lo atiende. En la Figura 1.1 se muestra el flujograma general de la atención de requerimientos.

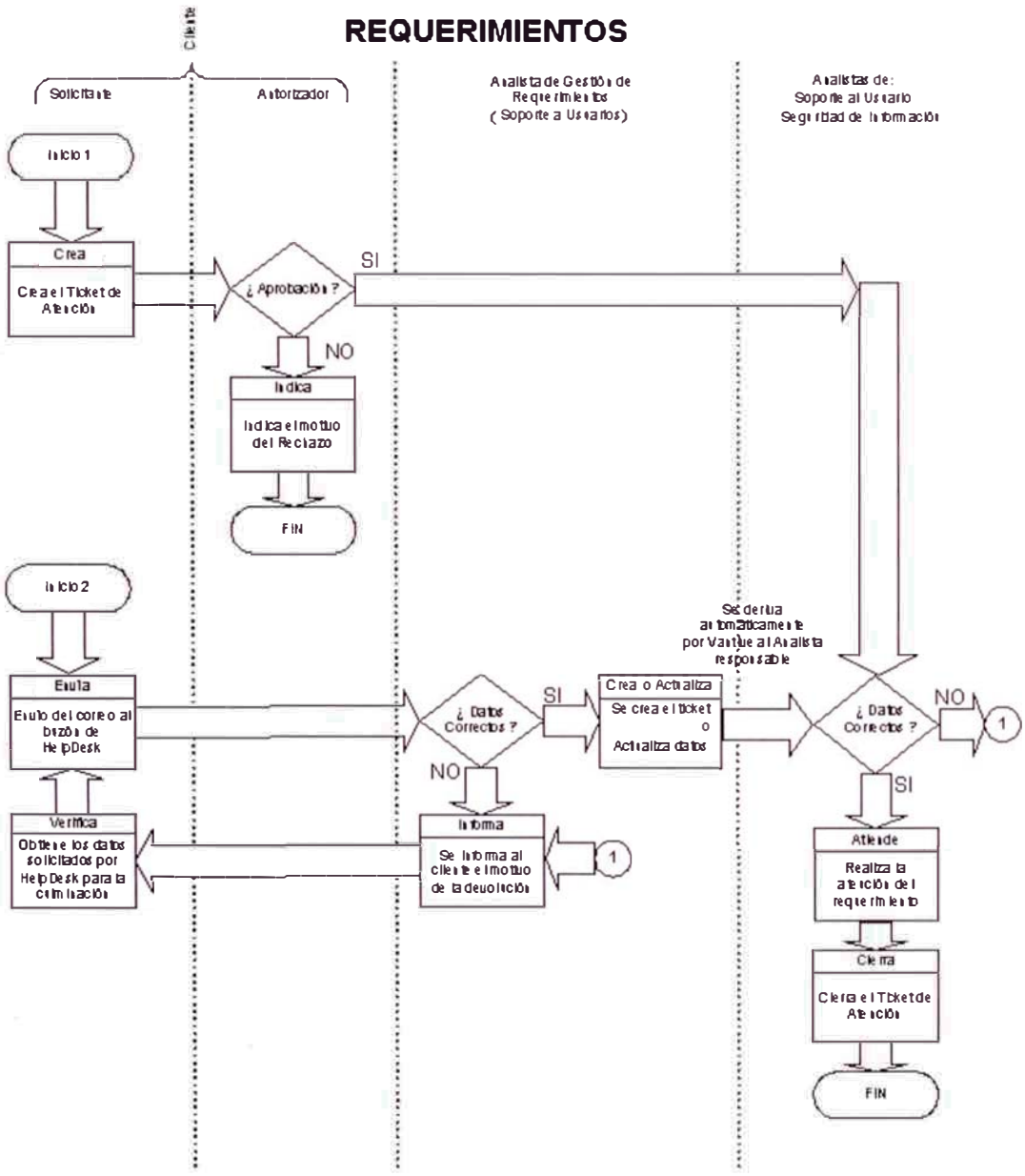


Figura 1-1. Flujograma de Atención de Requerimientos Informáticos

1.2.4.2 Gestión de Incidencias

Comprende la solución de incidencias o inadecuado funcionamiento detectado en los equipos, servicios y sistemas informáticos. En la

Figura 1.2 se muestra el flujograma general para la solución de incidencias.

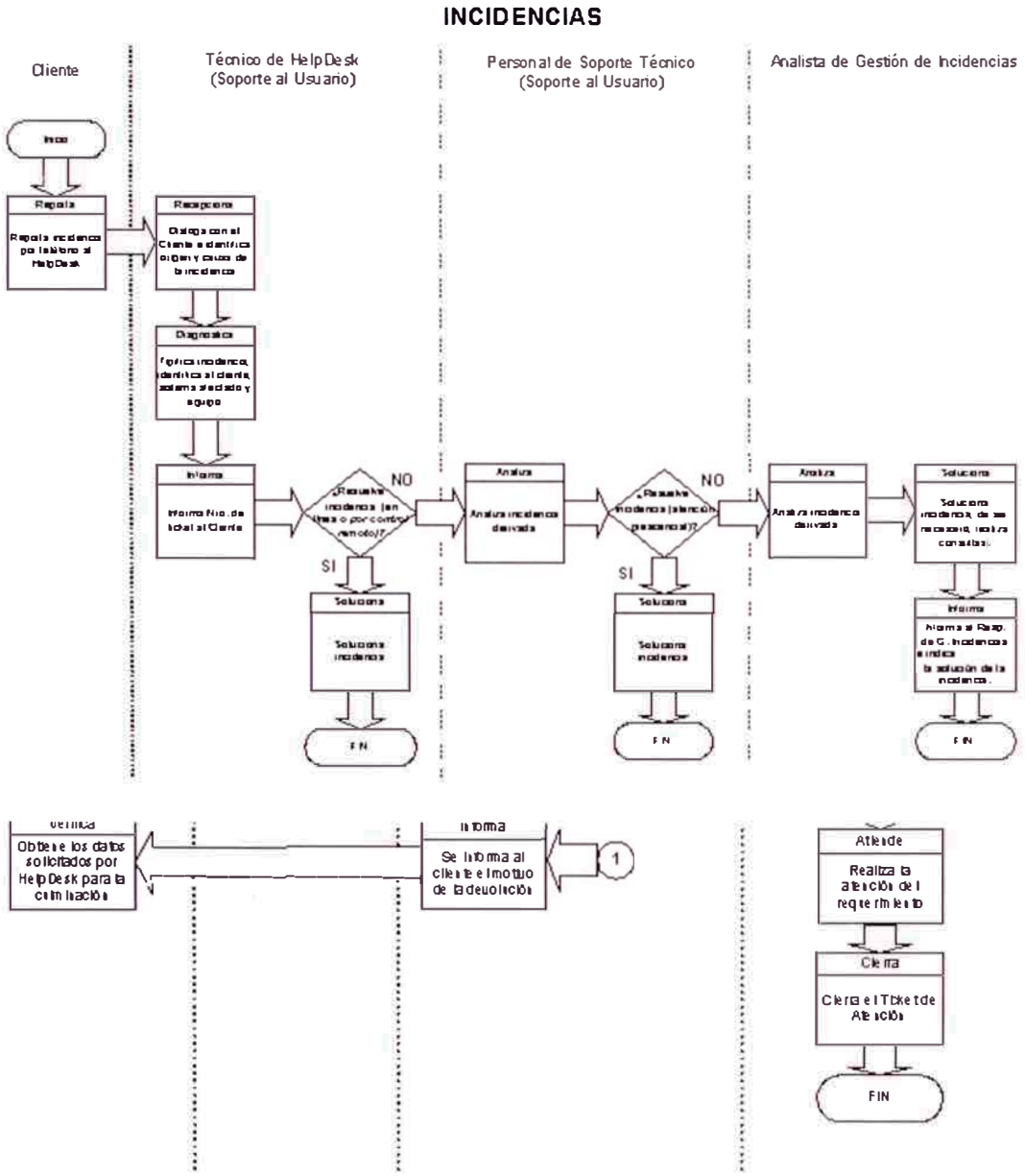


Figura 1-2. Flujograma de Gestión de Incidencias Informáticos

1.2.4.3 Gestión de cuentas y perfiles de Accesos a los sistemas

Este proceso comprende lo siguiente:

- Creación / Eliminación y Modificación de cuentas (identificadores) y perfiles de acceso a la red corporativa (Red, Correo, Internet) y de los sistemas corporativos de las empresas del grupo. En la Figura 1.3 se muestra el flujograma de la creación de la cuenta de red, necesario para la autentificación e ingreso a la red corporativa. Asimismo, en la Figura 1.4 se muestra el flujograma de la eliminación de la cuenta de red.
- Análisis y solución de incidencias relacionados a las cuentas y perfiles de acceso de los sistemas.
- Eliminación periódica de cuentas de acceso del personal cesado comunicado por Recursos Humanos y que no se hayan utilizado durante un periodo máximo de 60 días calendario.
- Revisión trimestral de cuentas y perfiles de accesos a los sistemas. Validación con el propietario de la información contenida en el sistema.
- Identificación y corrección de uso indebido de cuentas de acceso.
- Revisión periódica de cuentas privilegiadas

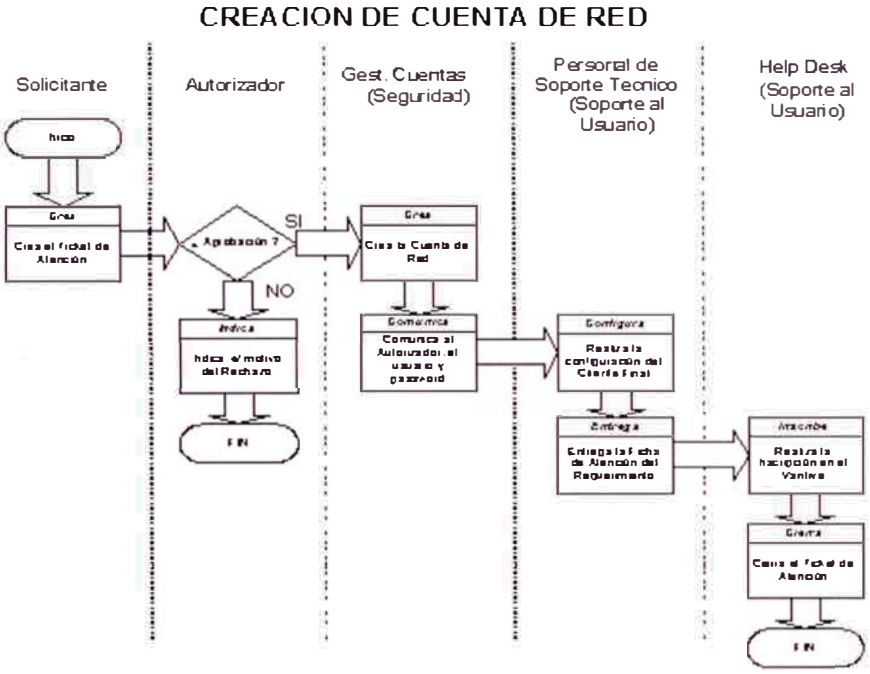


Figura 1-3. Flujograma de Creación de Cuenta de Red

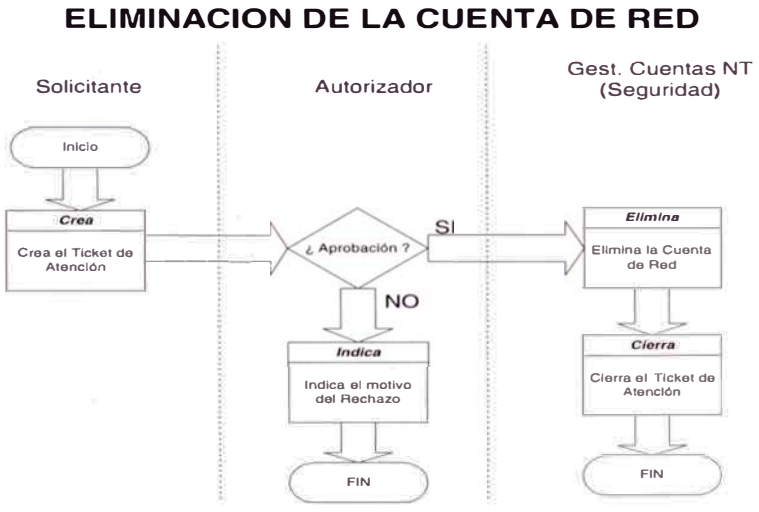


Figura 1-4. Flujograma de Eliminación de Cuenta de Red

1.2.4.4 Análisis de Riesgos

Este proceso comprende la identificación de riesgos a partir de las vulnerabilidades y amenazas identificadas sobre los activos de la empresa, posteriormente se cuantifica el daño potencial a la empresa para, finalmente, recomendar controles o preparar el plan de tratamiento de riesgos.

1.2.4.5 Revisión de cumplimiento de Auditorias y Normativas

Consiste en la revisión del cumplimiento de las auditorias internas y externas a las empresas del grupo, se realiza seguimiento y coordinaciones con los especialistas de subsanar las observaciones de auditoria. Así como la elaboración e implantación de procedimientos alineados a la normativa corporativa de Seguridad de Información.

1.2.4.6 Concientización en Seguridad de Información

Comprende la concientización de todo el personal de las empresas del grupo sobre la importancia de la Seguridad de la información para cumplir con los objetivos empresariales. Comprende charlas, difusión de boletines respecto a la normativa de seguridad, controles de accesos, delitos informáticos, amenazas, ingeniería social, uso de cuentas y contraseñas, entre otros.

1.2.5 Organización

La Empresa nace en el 2001 tiene la Gerencia Genera de Cobros y 8 direcciones que lo conforman: Comercial, Logística y Gestión Inmobiliaria, Gestión y Desarrollo Humano, Servicios Generales, Seguridad y Protección, , Servicios Económicos, Control y Gestión, y Tecnologías y Sistemas de información

La organización interna de la Dirección de Tecnologías y Sistemas de información está formada por 3 gerencias:

- La de Desarrollo, encargada de llevar proyectos y mantenimiento de desarrollo de los Sistemas
- La de Planificación, encargada de los gastos y
- La de Producción, encargada de toda la infraestructura informática.

La Gerencia de Producción a su vez tiene 4 áreas: la de Soporte Usuarios, encargada de dar soporte de Mesa de Ayuda a los usuarios en primera línea; la de Centro de Procesamiento de Datos, encargada del soporte de plataformas de toda la organización; la de Infraestructura y Tecnología, encargada de proyectos de implantación de nuevas tecnologías para el mantenimiento y mejora de la infraestructura de la red; y la de Seguridad de Información , encargada de gestión de cuentas, seguridad perimetral, normatividad e inducción, siendo su principal objetivo definir e implementar protecciones, políticas y procedimientos en búsqueda de la preservación de la integridad, disponibilidad y confidencialidad de la información en los sistemas

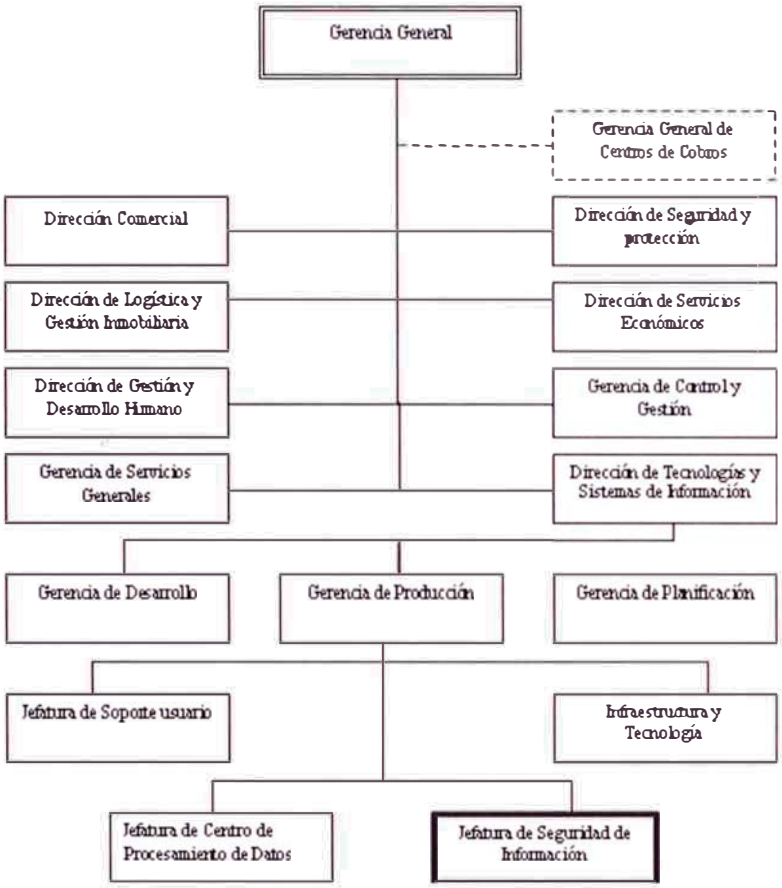


Figura 1-5. Organigrama de la Empresa

CAPÍTULO II

MARCO TEÓRICO

El marco teórico de este informe está centrado fundamentalmente en la seguridad de la información en los sistemas y se ha organizado de la siguiente manera:

1) Conceptos de seguridad de información en los sistemas.
2) Administración de la seguridad de la información.
3) Estándar de seguridad de información.
4) Modelo de implantación de sistemas de gestión de la seguridad de información.
5) Análisis de riesgos.
6) Modelo de retorno de inversión en seguridad de información.
7) Metodología de evaluación de soluciones

2.1 CONCEPTOS DE SEGURIDAD DE INFORMACIÓN

2.1.1 Definición de Seguridad

Podemos entender como **seguridad** una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas

operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de *seguridad* y se pasa a hablar de **fiabilidad** (probabilidad de que un sistema se comporte tal y como se espera de él) más que de *seguridad*; por tanto, se habla de *sistemas fiables* en lugar de hacerlo de *sistemas seguros*.

A grandes rasgos se entiende que mantener un sistema *seguro* (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad [SegUn02]

2.1.2 Objetivo de la Seguridad de Información

Los continuos desafíos de la seguridad de información, que han venido surgiendo, han llevado a esta área a definir metas y propósitos, los cuales han sido resumidos en su objetivo principal, y que permite hacer un acercamiento al cumplimiento de los nuevos y cambiantes retos. Es así como la Seguridad de Información busca dar apoyo a los objetivos y misión de las organizaciones, a través de la protección de sus principales recursos y activos: la información, la tecnología que la soporta (hardware y software) y las personas que la utilizan y/o conocen [ALSI05] [STON01], a través de la selección y aplicación de protecciones adecuadas, manteniendo así, el debido cuidado de sus recursos físicos, financieros, reputación, y otros activos tangibles e intangibles [NIST95].

Para el cumplimiento de dicho objetivo, la Seguridad de Información ha definido tres principios básicos (confidencialidad, integridad y disponibilidad) y 4 servicios (autenticación, autorización, no repudio y auditabilidad), los cuales serán detallados a continuación.

2.1.3 Principios básicos para Proteger la Información

Al ser la protección de los activos, uno de los objetivos principales de la seguridad de información, esto significa mantenerlos seguros frente a las diversas amenazas a las que se enfrentan y que pueden afectar su funcionalidad de diferentes maneras: corrupción, acceso indebido e incluso hurto y eliminación. [ALSI05], la Seguridad de Información se basa en la preservación de los siguientes principios básicos:

2.1.3.1 Confidencialidad

Este principio tiene como propósito asegurar que sólo la persona o personas autorizadas tengan acceso a cierta información. La información, dentro y fuera de una organización, no siempre puede ser conocida por cualquier individuo, si no por el contrario, está destinada para cierto grupo de personas, y en muchas ocasiones, a una sola persona. Esto significa que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos.

La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, es decir en los sistemas y dispositivos en los que reside dentro la red, como durante su procesamiento y tránsito, hasta llegar a su destino final [STON01].

2.1.3.2 Integridad

La integridad tiene como propósito principal, garantizar que la información no sea modificada o alterada en su contenido por sujetos no autorizados o de forma indebida. Asimismo, la integridad

se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos. Debido a esto, la integridad como principio de la Seguridad Informática [NIST95] [ALSI05].

2.1.3.3 Disponibilidad

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Al referirse a los sistemas que soportan la información, se trata de toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento de la información [ALSI05] [ALSI05-2].

Figura 2-1. Principios básicos para proteger la información. Fuente: TechNet

2.1.4 Servicios de la Seguridad de Información

Para lograr hacer cumplir la preservación y el cumplimiento de los tres principios básicos de la seguridad información, discutidos anteriormente, se han planteado cuatro servicios principales, que sirven como base para la implementación de una infraestructura de

seguridad de TI en una organización [STON01]. Las definiciones planteadas a continuación, son resultado del compendio de las definiciones dadas por los siguientes autores [NIST95], [STON01], [GASS88], [ALSI05], [BRIN95b]

2.1.4.1 Autenticación

Este servicio busca asegurar la validez de una identificación proporcionada para acceder cierta información, proveyendo medios para verificar la identidad de un sujeto, básicamente, de tres formas: por algo que el sujeto es, por algo que el sujeto tiene o por algo que el sujeto conoce.

2.1.4.2 Autorización

El servicio de autorización permite la especificación y continua administración de las acciones permitidas por ciertos sujetos, para el acceso, modificación o inserción de información de un sistema, principalmente, mediante permisos de acceso sobre los mismos.

2.1.4.3 No repudio

La administración de un sistema de información debe estar en capacidad de asegurar quién o quiénes son los remitentes y destinatarios de cualquier información. Es por esto que este servicio provee los medios y mecanismos para poder identificar quien ha llevado a cabo una o varias acciones en un sistema, para que los usuarios no puedan negar las responsabilidades de las acciones que han llevado a cabo.

2.1.4.4 Auditabilidad

Este servicio proporciona los mecanismos para la detección y recuperación ante posibles fallas o incidentes de seguridad, mediante el registro de todos los eventos y acciones hechas en un sistema.

2.1.5 Definición de la Seguridad de Información en los Sistemas.

Luego de comprender los objetivos principales y los principios básicos de la seguridad de información, ésta se puede definir como, la definición y posterior implementación de protecciones, políticas y procedimientos, en búsqueda de la preservación de la integridad, disponibilidad y confidencialidad de la información, los recursos que la soportan (hardware, software, firmware, dispositivos de comunicación) y los individuos que la utilizan o conocen.

Para llegar a cumplir los principios de la seguridad de información y lograr un buen funcionamiento de sus servicios, se debe tener una buena base de administración de los recursos, tanto tecnológicos como humanos, así como la información y los procesos que la seguridad busca proteger, tratando de llevar un manejo eficiente y eficaz de dichos recursos.

2.2 ADMINISTRACIÓN DE LA SEGURIDAD DE INFORMACIÓN

Administrar la Seguridad de información de una organización, es un trabajo fundamental para conservar confiables, los sistemas de la misma. La tarea de administración, comprende la administración de riesgos, definición, creación e implementación de

políticas de seguridad, procedimientos, estándares, guías, clasificación de información, organización de la estructura de seguridad de la compania, y la educación de los individuos de la organización, entre otras. [HARR03] [ALSI05]

La clave de un programa de seguridad de información, es la protección de los activos más importantes de la compañía. Estos activos pueden ser identificados mediante los análisis de riesgos, además de la identificación de las vulnerabilidades y amenazas que pueden llegar a afectar dichos activos, y estimar los costos y daños que tendría para la compañía, la materialización de una o más de dichas amenazas. Como resultado de los análisis de riesgos se puede lograr tener un presupuesto de las inversiones necesarias para la protección de dichos activos, contra los riesgos anteriormente identificados, no solo en cosas materiales, sino también en implementación de políticas, educación del personal, desarrollo de guías o estándares, etc. [ALSI05]

Una de las formas más utilizadas para hacer administración de la seguridad de información, se basa en la utilización de estándares. El cual se detalla en el punto 2.3

Para lograr los objetivos de la administración de la seguridad de información, ésta se vale de controles que se utilizan para hacer cumplir las directivas que esta área ha fijado para la organización. Dichos controles se clasifican en: controles administrativos, controles técnicos y controles físicos. [HARR03]

- Los controles administrativos, hacen referencia al desarrollo y publicación de políticas, estándares, procedimientos, investigación del personal, entrenamiento y el cambio de los procedimientos de control.

- Los controles técnicos, se refieren a los mecanismos de control de acceso, administración de recursos y contraseñas para su acceso, métodos de autenticación y autorización, dispositivos de seguridad, y la configuración de la infraestructura técnica de seguridad de la organización.

- Los controles físicos corresponden a los controles físicos de acceso a diferentes locaciones de la organización, monitoreo de los lugares críticos de almacenamiento y manejo de información, etc. [HARR03]

2.3 ESTÁNDAR DE SEGURIDAD DE INFORMACIÓN

El crecimiento de las necesidades de gestión de la seguridad de información en las organizaciones, ha motivado la creación de estándares locales e internacionales para la administración de tecnología de información, y en particular la seguridad de dicha información, y todo lo que a ésta concierne [OUD05].

Uno de los factores positivos de la existencia actual de los estándares, es la cantidad que hay de los mismos, ya que esto permite a una organización particular, acoplarse o acomodarse a uno de estos estándares, según sus características y necesidades, o en una situación determinada. Adicionalmente, otro punto a favor de las organizaciones gracias a los estándares, no sólo es el ahorro de recursos, tanto de dinero, como de personas y tiempo, en desarrollar estándares propios, sino que pueden utilizar estándares que han sido demostrados a partir de las mejores prácticas en el área, que para el caso de esta investigación, son las mejores prácticas en administración de la seguridad de información.

En dicha área, la administración de seguridad de información, existen varios estándares, nacionales e internacionales, que están orientados a ser una guía para las organizaciones en la formación y mantenimiento de la infraestructura de seguridad de información de las empresas.

2.4 MODELO DE IMPLANTACIÓN DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

En la norma ISO 27001 / ISO 17799 se presentan en detalle las etapas para el desarrollo del SGSI, para su implantación, así como aquellas para su mantenimiento. Incluye un método de evaluación, un proceso de documentación y un modelo de implantación del SGSI que sigue el modelo PDCA (Plan-Do-Check-Act).

Figura 2-2. Modelo PDCA para la implementación de un Sistema de la Gestión de la Seguridad de Información

De acuerdo con este modelo, la metodología de implantación de un Sistema de Gestión de la Seguridad de Información (SGSI) contempla

básicamente los siguiente pasos que se detallan en las siguientes tablas. Para cada etapa se identifican las acciones clave a llevar a cabo dentro de la misma.

Establecimiento del SGSI	
Inicio del Proyecto	Asegurar el compromiso de la dirección Seleccionar y entrenar a los miembros del equipo inicial que participan en el proyecto.
Definición del SGSI	Identificación del alcance del SGSI y de la Política de Seguridad del SGSI. Recopilar los documentos de seguridad existentes en la organización. Preparar los procedimientos relacionados con la gestión y la operación del SGSI.
Evaluación de Riesgos	Definición de una metodología para la clasificación de los riesgos. Creación de un inventario de activos. Evaluación de los activos a ser protegidos. Identificación y evaluación de amenazas y vulnerabilidades de los activos Cálculo del valor de riesgo asociado a cada activo

Tratamiento de Riesgos	Identificar y evaluar alternativas posibles para tratar los riesgos. Seleccionar e implantar los controles correctos que le permitan a la organización reducir el riesgo a un nivel aceptable Redactar el documento de declaración de aplicabilidad (documento de selección de controles), que debe ser firmado por Dirección. Identificar los riesgos residuales que han quedado sin cubrir y obtener la firma de Dirección. Preparar el Plan de Tratamiento de Riesgos Preparar procedimientos para implantar controles

Tabla 2-1. Modelo PDCA - Establecimiento del SGSI

Implantación y Operación	
Formación y sensibilización	Impartir formación entre los empleados sobre los nuevos procedimientos que se van a implantar Concienciar a la plantilla de la importancia que el proyecto de seguridad tiene para la Organización
Implantación del SGSI	Implantar el plan de tratamiento de riesgos Implantar políticas y procedimientos del SGSI Implantar los controles seleccionados

Tabla 2-2. Modelo PDCA - Implantación y Operación

Monitorización y Revisión	
Monitorización del SGSI	Ejecutar procedimientos de monitorización para detectar errores de proceso, identificar fallos de seguridad de forma rápida y acciones a realizar.
Revisión del SGSI	Revisiones periódicas de la política y alcance del SGSI, así como de su eficacia. Revisiones de los niveles de riesgos residuales y riegos aceptables

Tabla 2-3. Modelo PDCA - Monitorización y Revisión

Mantenimiento y Mejora	
Mantenimiento del SGSI	Comunicar los resultados de auditoria a las partes interesadas. Adoptar accesiones correctivas y preventivas
Revisión del SGSI	Medir el rendimiento del SGSI Implementar las mejoras identificadas en las revisiones del SGSI

Tabla 2-4. Modelo PDCA - Mantenimiento y Mejora

2.5 ANÁLISIS DE RIESGOS

El análisis de riesgos hace parte de la administración organizacional, como bien se define en [AZNZS] "La administración de riesgos es el término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. Administración de riesgos es tanto identificar oportunidades como evitar o mitigar pérdidas."

Las organizaciones poseen activos los cuales la seguridad de Información busca proteger, estos están conformados por tres elementos: la información, la tecnología que la soportan y las personas que la utilizan [ALSI05]. La seguridad de información busca dicha protección, pero para que ésta cumpla su función, requiere inversión, lo cual trae costos elevados que no siempre están disponibles en las organizaciones; por este motivo, es necesario tener una correcta administración de riesgos que incluya su correspondiente análisis de riesgos, para lograr decidir en qué

riesgos invertir y en cuáles no es necesario, según su prioridad.

El NIST 800-30 Risk Management Guide for Information Technology Systems [STON02], define el riesgo en función de la probabilidad de que se materialice una amenaza debido a una vulnerabilidad existente, y el impacto resultante que perjudica a la organización a razón de dicho evento. También propone una metodología para llevar acabo un análisis de riesgos. Esta propuesta consta de nueve pasos principales:

2.5.1 Caracterización del sistema

Define alcance, se identifican los límites del sistema a partir de recursos y de la información de éste.

Para identificar los riesgos en un sistema de tecnología de información se requiere tener conocimiento del ambiente y de los procesos del sistema. Para lograr este fin, se propone la recolección de información relacionada con el sistema, por medio de entrevistas, cuestionarios, revisión de documentos, etc. Este proceso debe ser completo y debe incluir el estudio del contexto organizacional y del negocio.

Después de realizar este paso podemos tener conocimiento de los límites del sistema, funciones, sistemas y datos críticos. Este paso es importante, ya que se logra obtener una contextualización en el ambiente organizacional.

2.5.2 Identificación de amenazas

Las amenazas son agentes capaces de explotar los fallos de seguridad, que denominamos puntos débiles y, como consecuencia de ello, causar pérdidas o daños a los activos de una

organización, afectando a sus negocios [ALSI05].

Las amenazas se pueden presentar por diferentes causas: naturales, humanas o del ambiente [STON02]; y pueden ser ocasionadas voluntarias o intencionalmente. La identificación de éstas, nos dan a luz algunas de las posibles necesidades de protección Informática que requiere la organización.

2.5.3 Identificación de vulnerabilidades

El análisis de identificación de amenazas (punto anterior) debe incluir un análisis de vulnerabilidades asociado con el ambiente del sistema.

Las vulnerabilidades son debilidades que son atacadas por las amenazas mediante la materialización de éstas, y afectan la confidencialidad, disponibilidad e integridad de una organización, su información o sus individuos [ALSI05].

2.5.4 Análisis de controles existentes

Consiste en analizar los controles que han sido implementados o se planean implementar, con el fin de reducir la probabilidad de que una amenaza sea materializada y tomen ventaja de una vulnerabilidad. Es importante tener en cuenta los controles implantados, ya que una vulnerabilidad puede tener menor probabilidad de ser explotada, si se tiene un mayor control de seguridad.

2.5.5 Determinación de probabilidad

Este proceso consiste en determinar la probabilidad de que una

vulnerabilidad sea explotada, en un ambiente con amenazas asociadas. Para estimar una probabilidad, se debe tener en cuenta las amenazas, la naturaleza de la vulnerabilidad y la existencia y eficiencia de controles actuales.

2.5.6 Análisis de impacto

Consiste en valorar el impacto causado, como resultado de la materialización de una amenaza. Para ello se debe tener en cuenta, en qué medida las amenazas afectan a los sistemas y a los datos críticos, la misión del sistema, sistemas y datos sensitivos. El impacto de un evento de seguridad, puede ser descrito en términos de pérdida o disminución de cualquiera de los siguientes principios de seguridad: integridad, disponibilidad y confidencialidad.

Es posible medir el impacto que causa la materialización de una amenaza, calculando el costo que implica la recuperación del daño causado. Pero esto solo es posible si los daños son tangibles y pueden ser estimados en dinero. Sin embargo existen otro tipo de impactos que no pueden ser medidos cuantitativamente, ya que son intangibles, por ejemplo la pérdida de imagen, reputación, confianza del sistema, etc.

Este tipo de impactos solo pueden ser estimados cualitativamente, ya que no pueden ser estimados en unidades específicas, sino calificados o descritos en términos de impacto Alto, Medio o Bajo. Este tipo de medidas cualitativas son relativas, ya que cada persona tiene un punto de vista diferente, y puede variar la valoración del impacto por cada persona que los califique.

Puede existir el caso en que para una persona, la pérdida de imagen

no afecte significativamente la organización, pero para otra persona, puede que sea algo esencial para lograr los objetivos de ésta. Por ello es importante definir qué es en realidad Bajo, Medio y Alto; para ello es necesario definir alguna métrica que ayude a calificar el impacto en un nivel más realista y menos relativo.

2.5.7 Determinación de riesgo

Este proceso consiste en la valoración del nivel de riesgo del sistema. La determinación de riesgo para una pareja particular de amenaza/vulnerabilidad puede ser expresado como una función de:

- La probabilidad de que una amenaza atente a una vulnerabilidad.
- La magnitud del impacto debido a la materialización de una amenaza.
- La adecuación de controles de seguridad planeados o existentes para reducir o eliminar riesgo.

Para determinar el nivel de riesgo, es necesario multiplicar el impacto por la probabilidad de ocurrencia. Esto puede llevarse a cabo a partir de una matriz con los diferentes niveles de impacto y probabilidad, y dándole así valores numéricos a cada uno de los niveles definidos. A partir de esta tabla se puede representar el nivel de riesgo que puede llegar a tener la materialización de una amenaza frente a una vulnerabilidad, esta matriz realmente muestra el nivel de riesgo que se tiene, el cual puede llegar a ser significativo para estimar el ROI, ya que nos presenta y prioriza la necesidad de inversión. Es necesario, al igual que para estimar el nivel de impacto, el uso de métrica para definir a qué se hace referencia con un nivel riesgo alto, medio o bajo, y así poder categorizar el nivel de riesgo al que esta expuesto el sistema.

2.5.8 Recomendaciones de control

El objetivo de las recomendaciones de control es reducir el nivel de riesgo del sistema y llevarlo a un nivel aceptable. Debe tenerse en cuenta los siguientes factores: recomendaciones efectivas, regulación y legislación, políticas organizacionales, impacto operacional y seguridad y confianza [STON02].

Aplicar seguridad es realmente lo que llamamos la inversión en Seguridad, al invertir en ésta, se disminuye el riesgo, por lo cual se pueden identificar mejor las amenazas que pueden llegar a tomar ventaja de una vulnerabilidad, las cuales podrían generar costos elevados para la recuperación del impacto causado.

2.5.9 Documentación de Resultados

Una vez finalizado cada paso del proceso, los resultados deben ser documentados en un reporte oficial.

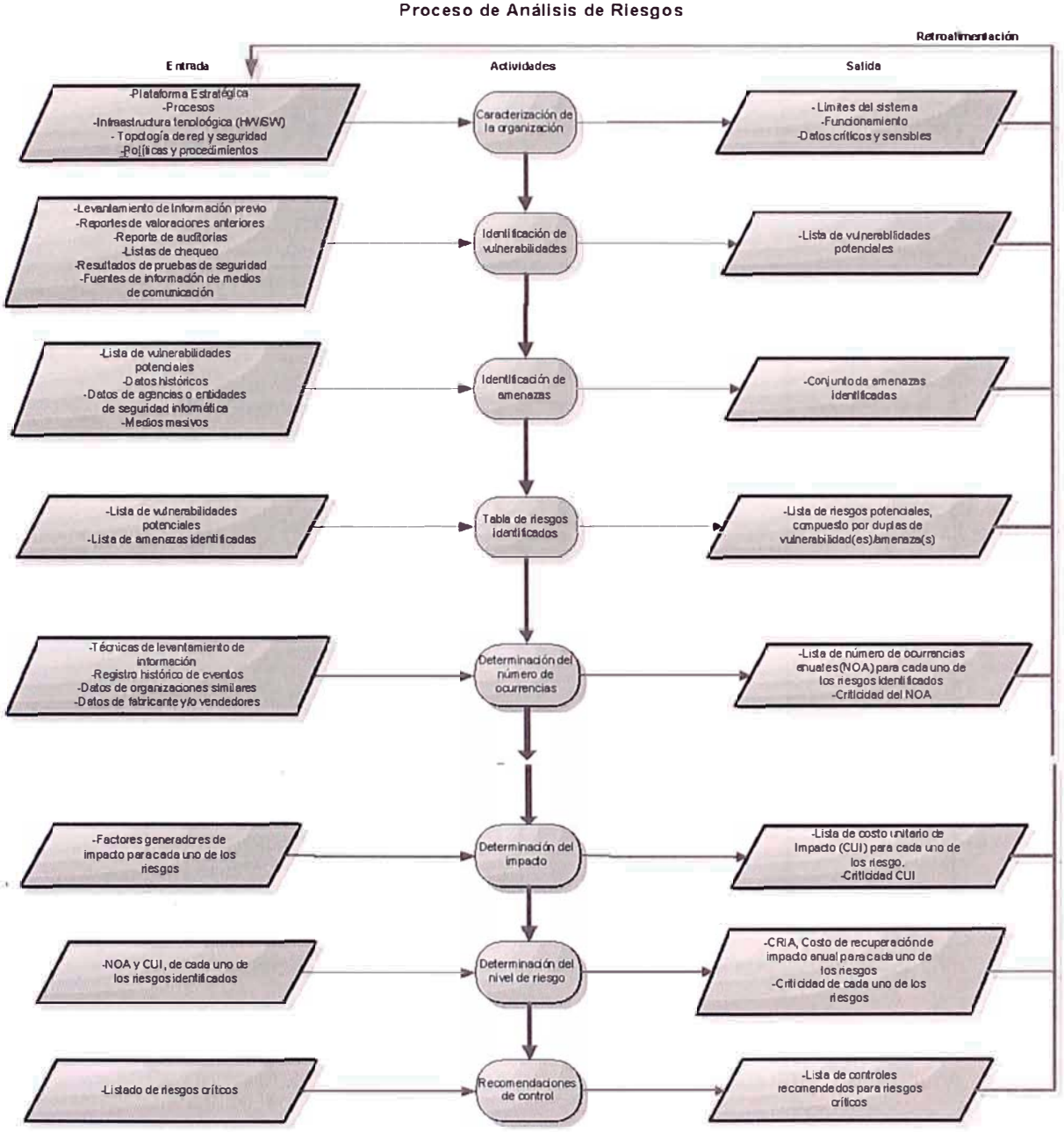


Figura 2-3. Proceso de Análisis de Riesgos

Para finalizar esta sección, se presenta en la Figura 2.3 un diagrama explicativo del Análisis de riesgos extraído de la metodología de Análisis y Gestión de Riesgos de los sistemas de información elaborado por el consejo superior de informática, MAGERIT [MAGE01].

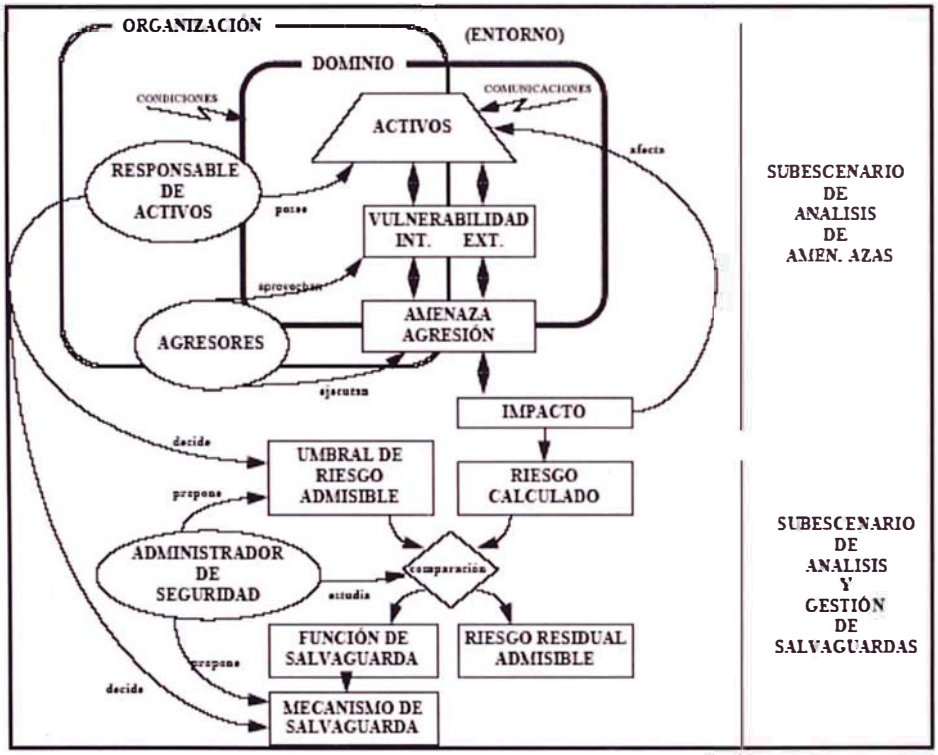


Figura 2-4. Análisis y Gestión de Riesgos. Modelo MAGERIT

El Dominio tiene como Actor principal al Responsable de Activos, quien determina su valor y necesidad de seguridad en forma de objetivos, de criterios de decisión o de decisiones.

Cabe señalar que en este modelo, el control cumple la misma función de salvaguarda. Asimismo, el riesgo residual admisible en un escenario real indica que puede enfrentarse a eventos amenazadores.

2.6 MODELO DE RETORNO DE LA INVERSIÓN EN SEGURIDAD DE INFORMACIÓN

2.6.1 Definición

El Retorno Sobre la Inversión de Seguridad de información (ROSI derivado del conocido indicador financiero ROI, Retorno Sobre la Inversión), busca justificar la inversión en seguridad de la información en términos monetarios. Para ello se tiene presente que los efectos de una implementación de seguridad en general no surgen en forma directa como beneficios económicos para una empresa, sino en todo caso como una reducción en las pérdidas que producen incidentes de seguridad como ataques, fallas o errores [ROSI07]

2.6.2 Modelo

Para, Marcia J. Wilson [WILS03] propone una serie de pasos para tener en cuenta al momento de tratar de estimar el ROSI, estos son:

Identificar los activos de información: recursos, productos, infraestructura computacional de red, la información referente a la organización, los clientes y empleados. Perder confidencialidad, integridad y disponibilidad pueden representar pérdida tangible en dólares y/o pérdidas intangibles, como puede ser de reputación o imagen organizacional.

Identificar amenazas y vulnerabilidades: una amenaza es cualquier evento que causa un resultado indeseado. Las amenazas pueden ser de diferentes tipos y causan diferentes efectos. Los terremotos, los pleitos, entre otros, son amenazas que podrían afectar los activos de la organización. Las

vulnerabilidades son debilidades o la ausencia de protección adecuada.

Hacer una valoración de los activos: valorar los activos es importante, ya que puede ayudar a priorizar la necesidad de protegerlos. Esta tarea puede llegar ser realizada a partir de una matriz que liste cada uno de los activos en riesgo, y ser clasificados en una escala de alto, medio o bajo según las necesidades del sistema.

Una vez recabada la información, es necesario comprender cuánto le costaría a la organización la pérdida de estos, versus el costo que tendría protegerlos. A partir de estos principios se podría llegar a estimar el ROSI de una organización.

Explicación del modelo a usar

La Figura2-5 muestra el modelo general de cálculo de retorno de inversión que será utilizado en este informe.

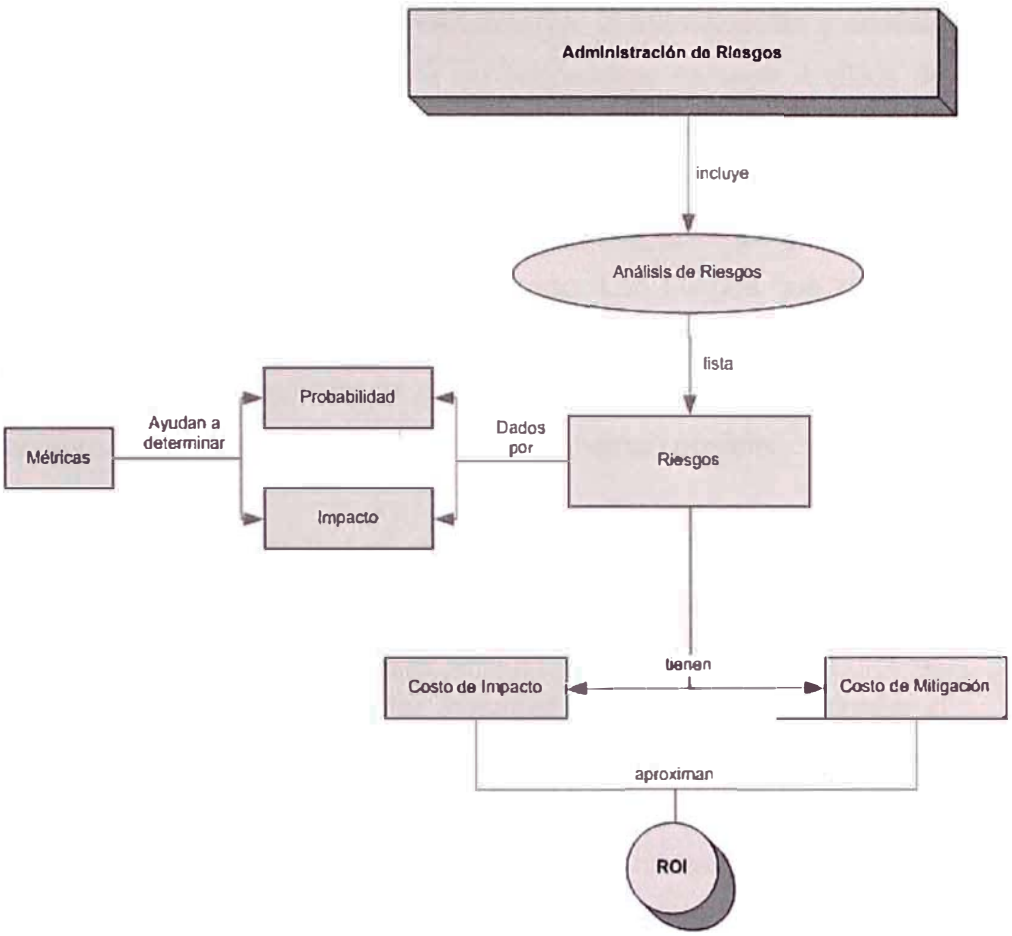


Figura 2-5. Modelo de Retorno de Inversión en Seguridad de Información

El modelo inicia con base en el proceso de Administración de Riesgos, que para las organizaciones, consiste en un proceso iterativo que consta de una secuencia de pasos, que al ser ejecutados, posibilitan una mejora continua en el proceso de toma de decisiones. Este proceso incluye la identificación de los riesgos a los que está expuesta la organización en un momento dado, y que en este caso, se refieren a riesgos de seguridad de la información. Adicionalmente luego de dicha identificación, este proceso permite analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados a la infraestructura de seguridad de la información.

Durante el proceso descrito anteriormente, la identificación y análisis de riesgos asociados, involucra un subproceso llamado Análisis de Riesgos, este proceso permite establecer una lista de riesgos clasificados según su nivel de criticidad, determinado por la probabilidad de ocurrencia y la magnitud del impacto que generaría la materialización de un riesgo determinado. Los riesgos que resultan ser más críticos, o con prioridad alta, involucran los activos más importantes y valiosos de la organización, por lo cual son los que primero deben ser mitigados, en el menor tiempo posible.

Para cuantificar tanto la probabilidad de ocurrencia como el impacto del riesgo, se pueden utilizar como herramientas, algunas métricas definidas para valorar, por ejemplo, la magnitud de dicho impacto. Estas métricas pueden estar basadas en estudios anteriores, o también pueden ser definidas según las necesidades.

Para lograr la estimación de la probabilidad o número de ocurrencias de los eventos no deseados, que para este modelo se tomarán en cuenta en períodos anuales, lo más deseable es contar con datos históricos de los eventos sucedidos en la organización, relacionados con el riesgo que se esté evaluando. De esta manera, se puede llegar a tener un estimado del número de ocurrencias anuales por cada amenaza que se materializaría en dicho riesgo. En caso de no tener registros de los eventos sucedidos en períodos anteriores que ayuden a estimar dicha probabilidad de ocurrencia, es posible basarse en historiales obtenidos de organizaciones de características similares, en cuanto a su tamaño, sector, ingresos anuales, número de clientes, entre otros aspectos. Sin embargo, es posible que estas organizaciones semejantes mantengan este tipo de información de manera confidencial, y por lo tanto habría que buscar otro medio para realizar dichas estimaciones. Es por esto que pueden ser de gran utilidad, las estadísticas que varios fabricantes de soluciones de

seguridad de información tienen a disposición del público, sobre los eventos de seguridad más relevantes de los últimos períodos.

La estimación del impacto que puede causar la ocurrencia de un evento no deseado, consistiría en calcular el costo de recuperación de los daños causados por dicho evento. Para ello, es necesario tener en cuenta el mayor número de aspectos implicados en la recuperación de los sistemas o activos afectados por la ocurrencia del evento. Algunos de estos factores que se deben tener en cuenta son: el número de horas de inactividad de la organización debido al evento ocurrido y el costo que esto implica, porcentaje de actividades paralizadas debido al evento, cantidad correspondiente en dinero que implica el porcentaje de inactividad del negocio, costo por hora de los empleados afectados y de los empleados que se requieren para el reestablecimiento de los sistemas afectados, tiempo estimado de recuperación, número de transacciones perdidas por hora, entre muchos otros aspectos que pueden variar dependiendo del tipo y actividad principal de la organización y del tipo de evento analizado.

Luego de tener la lista de los riesgos asociados a la infraestructura de seguridad de la organización, y de haber realizado el análisis de dichos riesgos, se contaría con el costo de impacto para cada uno de ellos, basado en la estimación del impacto, realizado en la valoración de cada uno de los riesgos.

Por otra parte, para cada uno de los riesgos se puede también calcular el costo de mitigación, es decir el costo de implementar y mantener una solución que permita disminuir la probabilidad de la ocurrencia del evento o eventos asociados a dichos riesgos; esto incluye, el costo de la inversión que implica la implementación de la solución, así como también, los costos de operación , que incluyen los costos de mantenimiento y soporte anual que requiere dicha

solución y que comúnmente son ofrecidos por los mismos fabricantes de las soluciones que proveen la implementación de las mismas.

El retorno de inversión se calcula dividiendo el costo de mitigar entre el costo de impacto y a este factor se multiplica doce. La diferencia de estos costos sería lo que la empresa ahorraría en caso de materializarse los riesgos.

2.7 METODOLOGÍA DE EVALUACIÓN DE SOLUCIONES

Se elabora criterios de Evaluación a fin de calificar las propuestas de los proveedores y el producto a adquirir. En la Tabla 2.5 se muestra los criterios de evaluación y los pesos asignados por grupo y de forma individual.

% Grupo	CRITERIOS A EVALUAR	% Ind.
35%	**Del producto (Funcional)**	
	Configuración de parámetros de Seguridad	30%
	Módulo de Reportes	20%
	Facilidad de administración	15%
	Alarmas	15%
	Escalable	15%
	Valor Agregado	5%
30%	**Del Proveedor**	
	Cumplimiento de Proyectos anteriores	30%
	Experiencias en soluciones similares	30%
	Experiencias tecnológica / Plataforma	20%
	Conocimiento del proceso	20%
35%	**De la Propuesta**	
	Consultaría	20%
	Tiempo de Implementación	15%
	Esfuerzo (Jornadas)	15%
	Soporte	10%
	Documentación / Entregable	5%
	Capacitación / Formación	5%
	Costo	30%

Tabla 2-5. Criterios de evaluación de proveedores

Cuantificación

a) Se solicita propuesta a los proveedores seleccionados, se revisa las propuestas y luego se cuantifica los valores de las alternativas sobre la base a la Tabla 2.6. Sólo se debe ingresar los valores en las celdas resaltadas de color amarillo. El calculó del Valor Máximo (Valor Max.) se detalla en el punto c).

% Grupo	CRITERIOS A EVALUAR		Alternativa 1 Proveedor A Enigma		Alternativa 2 Proveedor B ESM		Alternativa 3 Proveedor C Integrated Security		
		% Ind.	Ptje. 0 al 5	Valor %Ind. x ptje.	ptje. 0 al 5	Valor %Ind. x ptje.	ptje. 0 al 5	Valor %Ind. x ptje.	Valor Max.
35%	**Del producto - Funcional**								
	Configuración de parámetros de Seguridad	30%							1.5
	Módulo de Reportes	20%							1
	Facilidad de administración	15%							0.75
	Alarmas	15%							0.75
	Escalable	15%							0.75
	Valor Agregado	5%							0.25
	Puntaje SUBTOTAL	100%							5
	SUBTOTAL PONDERADO								
30%	**Del Proveedor**								
	Cumplimiento de Proyectos anteriores	30%							1.5
	Experiencias en soluciones similares	30%							1.5
	Experiencias tecnológica / Plataforma	20%							1
	Conocimiento del proceso	20%							1
	Puntaje SUBTOTAL	100%							5
	SUBTOTAL PONDERADO								
35%	**De la Propuesta**								
	Consultaría	20%							1
	Tiempo de Implementación	15%							0.75
	Esfuerzo (Jornadas)	15%							0.75
	Soporte	10%							0.5
	Documentación / Entregable	5%							0.25
	Capacitación / Formación	5%							0.25
	Costo	30%							1.50
	Puntaje SUBTOTAL	100%							5
	SUBTOTAL PONDERADO								

% Grupo	CRITERIOS A EVALUAR	Alternativa 1 Proveedor A Enigma	Alternativa 2 Proveedor B ESM	Alternativa 3 Proveedor C Integrated Security
35%	Del producto - Funcional..... (A)			
30%	Del Proveedor..... (B)			
35%	De la Propuesta.....(C)			
	TOTAL PONDERADO (A*0.35 + B*0.30 + C*0.35)			
	Puntaje Requerido para aprobación ..... > 69%			

Tabla 2-6. Plantilla de Evaluación de Proveedores

b) El puntaje de cada uno de los criterios es establecido de acuerdo a la Tabla 2.7.El cual varía desde 0 hasta el 5, asignándose el valor

de 0, cuando el criterio no se cumple y el valor de 5 cuando se cumple en su totalidad (al 100%).

Puntajes por criterio	% cumplimiento
0	No cumple (0%)
1	Cumple al 20%
2	Cumple al 40%
3	Cumple al 60%
4	Cumple al 80%
5	Cumple en su totalidad (100%)

Tabla 2-7. Puntajes por criterio de acuerdo a su nivel de cumplimiento

c) De acuerdo al %Individual del criterio (peso individual) se obtiene el valor del criterio, que resulta del factor:

Valor = % Ind. x Ptje.

Donde: %Ind. = %Individual
Ptje = Puntaje (0 al 5).
x: signo de multiplicación

Cuando el ptje. Es igual a 5 se obtiene el máximo valor a lo que en la Tabla 2.6. se indica como "Valor Max."

d) El Costo es un factor negativo, debido a que mayor costo menor puntaje total de la alternativa. Se cuantifica asignando el puntaje máximo (5) al menos costo y a través de comparación entre ellos se calcula el puntaje de las otras alternativas. Ejemplo. Se tiene los siguientes costos por alternativa:

	Alternativa1	Alternativa2	Alternativa3
Costos S/	75000	100000	50000

Tabla 2-8. Ejemplo de cuantificación de costos

Se asigna al de menos costo, en este caso la alternativa 3, el puntaje de 5, posteriormente se calcula los otros puntajes de la siguiente manera:

Puntaje Costos Alternativa3 = 2.5 x Puntaje Costos Alternativa2

Puntaje Costos Alternativa3 = 1.5 x Puntaje Costos Alternativa1

Donde 2.5 y 1.5 representan cuantas veces mejor es una alternativa comparada con la otra.

Entonces, se tiene:

Puntaje Costos Alternativa2= 5 / 2.5 = 2

Puntaje Costos Alternativa1= 5 / 1.5 = 3.3

	Alternativa 1	Alternativa 2	Alternativa 3
Costos S/	75,000	100,000	50,000
Puntaje costos	3.3	2	5

Tabla 2-9. Ejemplo de cuantificación y puntaje de costos

e) El puntaje SUBTOTAL de un grupo, resulta de la suma de los valores de todos los criterios que pertenecen al grupo.

Puntaje SUBTOTAL = valor_1 + valor_2 + ... valor_n

Donde:

n: número de criterios del grupo

f) El SUBTOTAL PONDERADO del grupo de una determinada alternativa se obtiene del siguiente factor:

$$= \frac{\text{(Puntaje SUBTOTAL de Alternativa1)}}{\text{(Puntaje SUBTOTAL del Valor Max)}}$$

Representa en porcentaje el nivel de cumplimiento de los criterios de un grupo en una determinada alternativa.

Donde:

Para nuestro caso el Puntaje SUBTOTAL del Valor Max = 5

g) El TOTAL PONDERADO resulta de la suma de los valores de SUBTOTAL PONDERADO multiplicados por su peso grupal
= (SUBTOTAL (1) x %Grupo(1) + SUBTOTAL (2) %Grupo(2) + ...SUBTOTAL (n) x %Grupo(n)) / 5

Donde: n: número de grupos de criterio
x: signo de multiplicación
%Grupo: Peso x grupo
Representa en porcentaje el nivel de cumplimiento del total de los criterios en una determinada alternativa.

h) La alternativa que tiene mayor valor en el TOTAL PONDERADO será la elegida, siempre y cuando sea mayor al 69%.

CAPÍTULO III

PROCESO DE TOMA DE DECISIONES

3.1 PLANTEAMIENTO DEL PROBLEMA

Identificación del Problema a resolver: Problemática

- 4 Casos de robo de información confidencial de la empresa, durante el periodo 2003 -2004.
- 2 denuncias legales por la no protección de información confidencial durante el año 2004.
- 12 casos reportados por usuarios de que su información ha sido eliminada o alterada, durante el año 2004.
- 2 casos de indisponibilidad del servidor de archivos en el periodo 2002.

Diagnóstico del Problema

Seguridad comprende varios aspectos: Seguridad Física, Seguridad del perímetro, Seguridad en la red, Seguridad del Servidor, Seguridad de las Aplicaciones, Seguridad de los Datos. ***El alcance del problema está referido al control de accesos en los servidores (plataformas de sistemas); los cuales, brindan servicios de repositorio de archivos, base de datos, aplicaciones y dominio para el ingreso a la red corporativa.***

Se revisa en el 2006 mediante la consultaría externa EY los niveles de seguridad de accesos en 32 servidores considerados por la empresa como los más críticos por la información que contienen, la medición fue realizada en base al cumplimiento de las buenas prácticas de control de accesos (ver Tabla 3-2 y 3-3), establecidos como estándar en la empresa. En la Tabla 3.1 se muestra la lista de 32 servidores.

Servidor	Sistema Operativo	Tipo de servidor	Servicio \ Información
FacturaLima	OPENVMS	Servidor de Aplicación y/o Base de Datos	Facturación de Telefonía Local Lima.
CobranzaLima	OPENVMS	Servidor de Aplicación y/o Base de Datos	Cobranza de Telefonía Local Lima
AClientesLima	OPENVMS	Servidor de Aplicación y/o Base de Datos	Atención al cliente de Telefonía Local
FacturaProv	UNIX	Servidor de Aplicación y/o Base de Datos	Facturación de Telefonía Local Provincias
CobranzaProv	UNIX	Servidor de Aplicación y/o Base de Datos	Cobranza de Telefonía Local Provincias
Empresas	UNIX	Servidor de Aplicación y/o Base de Datos	Facturación / Grandes Clientes / Cobranzas de Empresas
Cable	UNIX	Servidor de Aplicación y/o Base de Datos	Clientes/Cobranza/ Facturación/Marketing de Cable
Comercial	UNIX	Servidor de Aplicación y/o Base de Datos	Comercial
Instalaciones	UNIX	Servidor de Aplicación y/o Base de Datos	Alta / baja del servicio de instalaciones telefonía local
DataWareHouse	UNIX	Servidor de Aplicación y/o Base de Datos	Conceptos facturables, Movimiento abonados, Demanda y Gestión, trafico
Guias	UNIX	Servidor de Aplicación y/o Base de Datos	Cobranza/ Facturación de Guías
LargaDistancia	UNIX	Servidor de Aplicación y/o Base de Datos	Llamada Larga Distancia
RRHH	UNIX	Servidor de Aplicación y/o Base de Datos	Boletas de Pago del personal de la empresa.
SAPBD	UNIX	Servidor de Aplicación y/o Base de Datos	SAP Base datos
SAPContable	UNIX	Servidor de Aplicación y/o Base de Datos	SAP Aplicación Contable
TelefIntern	UNIX	Servidor de Aplicación y/o Base de Datos	Telefonía Internacional
Tups	UNIX	Servidor de Aplicación y/o Base de Datos	Cobranza Telefonía uso público
COBAN	UNIX	Servidor de Aplicación y/o Base de Datos	Cobranzas Interconectadas a Bancos

Cobros	W2K/NT	Servidor de Aplicación y/o Base de Datos	Recaudación de consumo de Telefonía Local, Móvil, Cable.
FileServerGrupal	W2K/NT	Servidor de Archivos	Directorios por Gerencia. Planes, estrategias gerenciales.
FileServerPersonal	W2K/NT	Servidor de Archivos	Directorios por persona Procedimientos, , Backup de usuario
RedCorpDomC1	W2K/NT	Servidor de Dominio de Red	Plataforma de cuentas de la red corporativa en Lima
RedCorpDomC2	W2K/NT	Servidor de Dominio de Red	Plataforma de cuentas de la red corporativa en Ayacucho, Huancavelica, Huancayo, Huanuco, Tarma
RedCorpDomN1	W2K/NT	Servidor de Dominio de Red	Plataforma de cuentas de la red corporativa en Piura, Cajamarca y Tumbes
RedCorpDomN2	W2K/NT	Servidor de Dominio de Red	Plataforma de cuentas de la red corporativa en Chiclayo, Chimbote, Trujillo y Huaraz
RedCorpDomO1	W2K/NT	Servidor de Dominio de Red	Plataforma de cuentas de la red corporativa en Iquitos, Pucallpa, Tarapoto
RedCorpDomS1	W2K/NT	Servidor de Dominio de Red	Plataforma de cuentas de la red corporativa en Arequipa, Cusco, Juliaca, Moquegua, Puno, Tacna
RedCorpDomS2	W2K/NT	Servidor de Dominio de Red	Plataforma de cuentas de la red corporativa en Chincha, Ica, Pisco
Correo	W2K/NT	Servidor Correo	Plataforma de Correo Lotus
AdminReport	W2K/NT	Servidor de Aplicación y/o Base de Datos	Report manager. Duplicado de Detalle de llamadas básica / móviles
AplicLotus	W2K/NT	Servidor de Aplicación y/o Base de Datos	Soporte BD y Aplicaciones Lotus
SIO	W2K/NT	Servidor de Aplicación y/o Base de Datos	Nuevas Oportunidades de Negocio

Tabla 3-1. Servidores / Plataformas de Sistemas

Se ha revisado 30 buenas prácticas agrupadas de la siguiente manera, para el periodo 2006:

1. Gestión de acceso de usuarios		22
1.1 Gestión de cuentas/identificadores de usuarios	5	
1.2 Gestión de contraseñas de usuarios	6	
1.3 Gestión de privilegios de usuarios	3	
1.4 Control de acceso al sistema operativo	6	
1.5 Revisión de los derechos de acceso de los usuarios	2	
2. Responsabilidad de los usuarios		8
2.1 Uso de cuentas	2	
2.2 Uso de contraseñas	3	
2.3 Equipo informático de usuario desatendido	2	
2.4 Uso de archivo y directorios	1	
TOTAL		30

Tabla 3-2 Grupo de buenas prácticas de control de Accesos en los Servidores al 2006

En la Tabla 3-3 se muestra cada una de las buenas prácticas referidas al control de accesos en los servidores.

1. Gestión de acceso de usuarios		
	1.1 Gestión de cuentas/identificadores de usuarios	
		Se debe tener procedimiento de creación/eliminación/modificación de cuentas de usuarios.
		Cada usuario debe tener su propio y único identificador, prohibiéndose que varios usuarios lo compartan.
		El propietario del servicio o información debe autorizar el acceso al usuario.
		Eliminar las cuentas de acceso de los usuarios que y no pertenezcan a la organización (personal cesado) o retirado.
		Eliminar las cuentas de acceso de los usuarios que se encuentran inactivos (sin uso) hace más de 60 días.
	1.2 Gestión de contraseñas de usuarios	
		Proporcionar inicialmente una contraseña temporal segura, que el sistema debe obligar al usuario cambiar inmediatamente después de inicio de sesión.
		El sistema no debe permitir asignar una contraseña menor a 6 caracteres.
		El sistema no debe permitir asignar una contraseña igual a las 6 últimas contraseñas.
		El sistema debe forzar cambiar la contraseña cada 35 días calendario.
		La contraseña no debe visualizarse en pantalla durante la introducción de la misma.

			Contraseña debe ser fácil de recordar y difícil de adivinar: contraseña no debe ser igual a Identificación del Usuario (con prefijo, sufijo), no debe ser igual a una de las palabras especificadas en un diccionario.
	1.3 Gestión de privilegios de usuarios		
			Identificar los privilegios asociados a cada elemento del sistema. Resaltar cuentas con privilegios de administración.
			Asignar privilegios según "necesidad de su uso" y "caso por caso" (asignar el permiso necesario para que pueda desempeñar su labor).
			Se debe tener procedimiento de creación/eliminación/modificación de cuentas con privilegio administrador.
	1.4 Control de acceso al sistema operativo		
			El sistema debe mostrar un mensaje al inicio de sesión que advierta la restricción de acceso al sistema sólo a usuarios autorizados.
			El sistema debe bloquear la cuenta por 5 intentos fallidos.
			Después de ocurrir el error en el ingreso al Sistema, la cuenta deberá permanecer inactiva por 30 minutos.
			Se recomienda que la opción de servicio de acceso remoto debe estar desactivada.
			Se debe tener actualizado los parches de sistemas operativos.
			Desactivar o retirar todas las facilidades basadas en software que no sean necesarios. No se debe tener servicios instalados que no han sido definidos como permisibles para el sistema.
	1.5 Revisión de los derechos de acceso de los usuarios		
			Revisar los derechos de accesos de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses).
			Revisar las cuentas privilegiadas periódicamente (se recomienda cada semana).
2. Responsabilidad de los usuarios			
	2.1 Uso de cuentas		
			Cada usuario debe ingresar con su propia "cuenta de usuario" y no debe compartirla. El usuario es responsable por todas las acciones que se realicen con su "cuenta".
			El usuario no deberá usar cuentas especiales o aprovechar fallas en la seguridad de los sistemas, para obtener un acceso no autorizado.
	2.2 Uso de contraseñas		
			Mantener la confidencialidad de las contraseñas. Evitar guardar registros (papel, archivos de software o dispositivos).
			Seleccionar contraseñas de buena calidad, con una longitud mínima caracteres que sean fáciles de recordar, no estén basas en algo que cualquiera pueda adivinar.
			Cambiar las contraseñas en intervalos de tiempo regulares (menor a 35 dias).
	2.3 Equipo informático de usuario desatendido		
			Bloquear su sesión o habilitar un protector de pantalla para evitar accesos no autorizados usando su cuenta. Desconectar (log-off) los servidores o los computadores centrales cuando se ha terminado la sesión
			Al término del trabajo diario, cierra todas las sesiones y apaga tu computadora antes de retirarte de la oficina.
	2.4 Uso de archivo y directorios		
			No compartir sus archivos o directorios por defecto. Este no debe quedar con acceso de control total y a su vez con permiso para todos los usuarios de la red corporativa.

Tabla 3-3. Buenas prácticas de control de Accesos en los Servidores al 2006

Problema

Se tiene que los 32 servidores no superan el 40 % (ver Tabla 3-4) de las recomendaciones de buenas prácticas de control de accesos en los servidores, establecido como estándar en la empresa (ver Tabla 3-3), siendo su política cumplir por lo menos con el 90 % de estas recomendaciones para tener un nivel adecuado de Seguridad de Información.

Cuantificación del problema

a) Por Servidor

En la Tabla 3.4 se muestra por cada servidor los niveles de seguridad (% de cumplimiento de buenas prácticas), en las cual se puede observar que ninguno supera el 40%, siendo el servidor de "Empresas" el de menor nivel, cumpliendo solamente con el 16.7% del total de prácticas revisadas. El nivel de seguridad promedio de todos lo servidores es 29.3%. La medición fue realizada por consultoría externa EY en el 2006.

Servidor	Nivel de Seguridad
FacturaLima	33.3%
CobranzaLima	30.0%
AClientesLima	20.0%
FacturaProv	26.7%
CobranzaProv	23.3%
Empresas	16.7%
Cable	23.3%
Comercial	30.0%
Instalaciones	26.7%
DataWareHouse	36.7%
Guías	20.0%
LargaDistancia	26.7%
RRHH	33.3%
SAPBD	26.7%
SAPContable	26.7%
TelefIntern	33.3%

Tups	40.0%
COBAN	30.0%
Cobros	26.7%
FileServerGrupal	23.3%
FileServerPersonal	26.7%
RedCorpDomC1	30.0%
RedCorpDomC2	33.3%
RedCorpDomN1	36.7%
RedCorpDomN2	33.3%
RedCorpDomO1	36.7%
RedCorpDomS1	33.3%
RedCorpDomS2	30.0%
Correo	33.3%
AdminReport	30.0%
AplicLotus	33.3%
SIO	26.7%
Nivel de seguridad PROMEDIO	29.3%

Tabla 3-4. Niveles de Seguridad de los Servidores calculado por consultoría externa EY en el 2006

En el Anexo A, al final de este informe, se adjunta la tabla de revisión de cumplimiento de buena práctica sobre el servidor FacturaLima.

b) Por buena práctica

En la Tabla 3.5 se muestra por cada buena práctica el porcentaje de cumplimiento medido sobre los 32 servidores, en la cual se puede observar que 2 buenas prácticas tienen un nivel de cumplimiento de 100%, el cual indica que se cumple en todos los servidores, asimismo, se tiene 6 buenas prácticas que tienen un nivel de cumplimiento de 0%, el cual indica que no se cumple en ningún servidor.

Buena Práctica de Control de Accesos \ Servidor	% Cumplimiento
1. Gestión de acceso de usuarios	
1.1 Gestión de cuentas/identificadores de usuarios	
Se debe tener procedimiento de creación/eliminación/modificación de cuentas de usuarios.	100.0%
Cada usuario debe tener su propio y único identificador, prohibiéndose que varios usuarios lo compartan.	18.8%
El propietario del servicio o información debe autorizar el acceso al usuario.	56.3%
Eliminar las cuentas de acceso de los usuarios que y no pertenezcan a la organización (personal cesado) o retirado.	0.0%
Eliminar las cuentas de acceso de los usuarios que se encuentran inactivos (sin uso) hace más de 60 días.	0.0%
1.2 Gestión de contraseñas de usuarios	
Proporcionar inicialmente una contraseña temporal segura, que el sistema debe obligar al usuario cambiar inmediatamente después de inicio de sesión.	90.6%
El sistema no debe permitir asignar una contraseña menor a 6 caracteres.	37.5%
El sistema no debe permitir asignar una contraseña igual a las 6 últimas contraseñas.	9.4%
El sistema debe forzar cambiar la contraseña cada 35 días calendario.	6.3%
La contraseña no debe visualizarse en pantalla durante la introducción de la misma.	100.0%
Contraseña debe ser fácil de recordar y dificil de adivinar: contraseña no debe ser igual a Identificación del Usuario (con prefijo, sufijo), no debe ser igual a una de las palabras especificadas en un diccionario.	6.3%
1.3 Gestión de privilegios de usuarios	
Identificar los privilegios asociados a cada elemento del sistema. Resaltar cuentas con privilegios de administración.	50.0%
Asignar privilegios según "necesidad de su uso" y "caso por caso" (asignar el permiso necesario para que pueda desempeñar su labor).	15.6%
Se debe tener procedimiento de creación/eliminación/modificación de cuentas con privilegio administrador.	0.0%
1.4 Control de acceso al sistema operativo	
El sistema debe mostrar un mensaje al inicio de sesión que advierta la restricción de acceso al sistema sólo a usuarios autorizados.	53.1%
El sistema debe bloquear la cuenta por 5 intentos fallidos.	6.3%
Después de ocurrir el error en el ingreso al Sistema, la cuenta deberá permanecer inactiva por 30 minutos.	6.3%
Se recomienda que la opción de servicio de acceso remoto debe estar desactivada.	81.3%
Se debe tener actualizado los parches de sistemas operativos.	37.5%
Desactivar o retirar todas las facilidades basadas en software que no sean necesarios. No se debe tener servicios instalados que no han sido definidos como permisibles para el sistema.	21.9%
1.5 Revisión de los derechos de acceso de los usuarios	
Revisar los derechos de accesos de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses).	0.0%
Revisar las cuentas privilegiadas periódicamente (se recomienda cada semana).	0.0%
2. Responsabilidad de los usuarios	
2.1 Uso de cuentas	
Cada usuario debe ingresar con su propia "cuenta de usuario" y no debe compartirla. El usuario es responsable por todas las acciones que se realicen con su "cuenta".	28.1%

	El usuario no debe usar cuentas especiales o aprovechar fallas en la seguridad de los sistemas, para obtener un acceso no autorizado.	46.9%
2.2 Uso de contraseñas		
	Mantener la confidencialidad de las contraseñas. Evitar guardar registros (papel, archivos de software o dispositivos).	40.6%
	Seleccionar contraseñas de buena calidad, con una longitud mínima caracteres que sean fáciles de recordar, no estén basas en algo que cualquiera pueda adivinar.	6.3%
	Cambiar las contraseñas en intervalos de tiempo regulares (menor a 35 días).	6.3%
2.3 Equipo informático de usuario desatendido		
	Bloquear su sesión o habilitar un protector de pantalla para evitar accesos no autorizados usando su cuenta. Desconectar (log-off) los servidores o los computadores centrales cuando se ha terminado la sesión	6.3%
	Al término del trabajo diario, cierra todas las sesiones y apaga tu computadora antes de retirarte de la oficina.	0.0%
2.4 Uso de archivo y directorios		
	No compartir sus archivos o directorios por defecto. Este no debe quedar con acceso de control total y a su vez con permiso para todos los usuarios de la red corporativa.	46.9%
Nivel de seguridad (% de cumplimiento de buenas prácticas)		29.3%

Tabla 3-5. Niveles de Seguridad por buena práctica calculada por consultoría externa EY en el 2006

3.2 OBJETIVO DEL PROYECTO

Mejorar los niveles de seguridad de los accesos a las 32 plataformas de sistemas o servidores que contienen información critica de la empresa, cumpliendo por lo menos con el 90% de buenas prácticas, establecido como estándar de control de accesos en los servidores de la empresa.

3.3 ALTERNATIVAS DE SOLUCIÓN

El personal interno de la empresa no tiene capacidad de dar solución al problema planteado presentándose robos de información, denuncias legales, entre otros, los cuales han generado perdidas financieras a las empresas del grupo de aproximadamente 800 mil soles anuales en promedio durante el 2003-2004, por ello la empresa avalúa la contratación de consultoría externa para que brinde asesoría en el cumplimiento de buenas prácticas en seguridad de información sobre el control de acceso en las plataformas de sistemas o servidores. También se requiere adquirir producto (software) desarrollado por terceros el cual debe apoyar en la labor administrativa de elaboración de reportes, configuraciones, control y evaluaciones del cumplimiento de configuraciones de parámetros de Seguridad de Información.

A partir de fuentes de las empresas del grupo se escoge como alternativas tres consultorías externas (proveedores) con un producto respectivo.

Alternativa 1: Proveedor A - Enigma
Alternativa 2: Proveedor B - ESM (Enterprise Security Manager)
Alternativa 3: Proveedor C - Integrated Security

3.4 EVALUACIÓN DE ALTERNATIVAS DE SOLUCIÓN

Se identifica las ventajas y desventajas de cada alternativa

Alternativa 1: Proveedor A - Enigma

Ventajas

- El producto emite alarmas a un número de celular cuando este detecta vulnerabilidades en los servidores, funcionalidad que no tienen los otros productos, cuyas alarmas son emitidos a través de correo electrónico.
- En la propuesta se considera un soporte personalizado de 24 horas para resolver incidencias generadas por el producto.

Desventajas

- El producto no permite realizar todas las configuraciones recomendadas en las mejores prácticas. Es posible configurar sólo a un 60%.
- En la propuesta no se ha incluido actividades de aprobación de entregables.

Alternativa 2: Proveedor B - ESM

Ventajas

- El producto, desde una consola, permite realizar todas las configuraciones de parámetros de seguridad de acceso recomendados en las mejores prácticas.
- El producto permite elaborar reportes personalizados para ejecutivos y administradores de Seguridad.
- El proveedor tiene conocimiento de la organización de la empresa, sus procesos, habiendo participado en 15 proyectos y

cumpliendo con el desarrollo de los mismos.

Desventajas

- En la propuesta se especifica un máximo de 80 horas de consultoría, mientras que la alternativa 1 y la alternativa 3, proponen 90 y 120 horas respectivamente.

Alternativa 3: Proveedor C - Integrated Security

Ventajas

- Dentro del valor agregado del producto se especifica que éste ejecuta correcciones automáticas en línea de acuerdo a reglas que en el se puede configurar, mientras que esta facilidad no lo tienen los otros productos.
- Se considera como tiempo de implementación 150 días útiles, mientras que la alternativa 1 y la alternativa 2, proponen 210 y 172 días calendario respectivamente.

Desventajas

- El producto no es compatible con todas las plataformas de sistemas (servidores) instalados en la empresa.
- El producto no permite realizar todas las configuraciones recomendadas en las mejores prácticas. Es posible configurar un 80%.
- El proveedor es nuevo en el mercado, tiene menos experiencia en soluciones similares comparado con los otros proveedores.

Se realiza la selección del Proveedor y su Producto a través de la metodología indicada en la sección 3.3

Cuantificación de Costos

El costo está relacionado a la consultoría del proveedor, adquisición de licencias y mantenimiento del producto.

El puntaje es calculado a través de la Metodología de Evaluación de Soluciones explicada en la sección 3.3 punto "d"

En la Tabla 3.6 se muestra la calificación y puntajes de costos de cada una de las alternativas.

	Alternativa 1	Alternativa 2	Alternativa 3
Costos S/	241,920	378,000	332,640
Consultoría Proveedor (80 horas mínimo)	45,000	76,000	60,000
Licencia del producto	170,000	260,000	240,000
Mantenimiento del producto	26,920	42,000	32,640
Puntaje costos	5	2.27	2.94

Tabla 3-6. Cuantificación y puntaje de costos de alternativas

Donde:

Puntaje Costos Alternativa1 = 2.2 x Puntaje Costos Alternativa2

Puntaje Costos Alternativa1 = 1.7 x Puntaje Costos Alternativa3

Calificación de Alternativas

En la Tabla 3.7 se muestra los valores cuantificados y la calificación total por cada alternativa, esto de acuerdo a la metodología descrita en la sección 2.6.

% Grupo	CRITERIOS A EVALUAR		Alternativa 1 Proveedor A Enigma		Alternativa 2 Proveedor B ESM		Alternativa 3 Proveedor C Integrated Security		Valor Max.
		% Ind.	Ptje. 0 al 5	Valor %Ind. x ptje.	Ptje. 0 al 5	Valor %Ind. x ptje.	Ptje. 0 al 5	Valor %Ind. x ptje.	
35%	**Del producto - Funcional**								
	Configuración de parámetros de Seguridad	30%	2	0.6	5	1.5	4	1.2	1.5
	Módulo de Reportes	20%	3	0.6	4	0.8	4	0.8	1
	Facilidad de administración	15%	3	0.5	4	0.6	4	0.6	0.75
	Alarmas	15%	5	0.8	4	0.6	4	0.6	0.75
	Escalable	15%	3	0.5	4	0.6	3	0.5	0.75
	Valor Agregado	5%	0	0.0	0	0.0	2	0.3	0.25
	Puntaje SUBTOTAL	100%		2.9		4.1		3.7	5
	SUBTOTAL PONDERADO			**57.0%**		**82.0%**		**73.0%**	
30%	**Del Proveedor**								
	Cumplimiento de Proyectos anteriores	30%	4	1.2	4	1.2	3	0.9	1.5
	Experiencias en soluciones similares	30%	3	0.9	4	1.2	1	0.3	1.5
	Experiencias tecnológica / Plataforma	20%	4	0.8	4	0.8	3	0.6	1
	Conocimiento del proceso	20%	3	0.6	4	0.8	3	0.6	1
	Puntaje SUBTOTAL	100%		3.5		4.0		2.4	5
	SUBTOTAL PONDERADO			**70%**		**80%**		**48%**	
35%	**De la Propuesta**								
	Consultaria	20%	3.75	0.8	3.3	0.7	5	1.0	1
	Tiempo de Implementación	15%	3.5	0.5	4.3	0.6	5	0.8	0.75
	Esfuerzo (Jornadas)	15%	3	0.5	3	0.5	3	0.5	0.75
	Soporte	10%	4	0.4	3	0.3	3	0.3	0.5
	Documentación / Entregable	5%	2	0.1	4	0.2	3	0.2	0.25
	Capacitación / Formación	5%	4	0.2	4	0.2	3	0.2	0.25
	Costo	30%	5	1.5	2.27	0.7	2.94	0.9	1.50
	Puntaje SUBTOTAL	100%		3.9		3.1		3.7	5
	SUBTOTAL PONDERADO			**78.5%**		**62.7%**		**73.6%**	

% Grupo	CRITERIOS A EVALUAR	Alternativa 1 Proveedor A Enigma	Alternativa 2 Proveedor B ESM	Alternativa 3 Proveedor C Integrated Security
35%	Del producto – Funcional..... (A)	57.0%	82.0%	73.0%
30%	Del Proveedor..... (B)	70.0%	80.0%	48.0%
35%	De la Propuesta.....(C)	78.5%	62.7%	73.6%
	TOTAL PONDERADO (A*0.35 + B*0.30 + C*0.35)	**68.4%**	**74.7%**	**65.7%**
	Puntaje Requerido para aprobación ..... > 69%	Desaprobado	Aprobado	Desaprobado

Tabla 3-7. Cuantificación y Calificación total de Alternativas

3.5 TOMA DE DECISIÓN

La alternativa 2: Proveedor B y Producto ESM es la elegida debido a que tiene mayor calificación de todas las alternativas con un 74.7 % y supera el mínimo requerido de 69%.

3.6 DESARROLLO DE LA SOLUCIÓN ELEGIDA

La estrategia se basa en el modelo PDCA: Planificar – Hacer – Verificar y Actuar como se muestra en la Figura 3.1 y explicada en la sección 2.4.

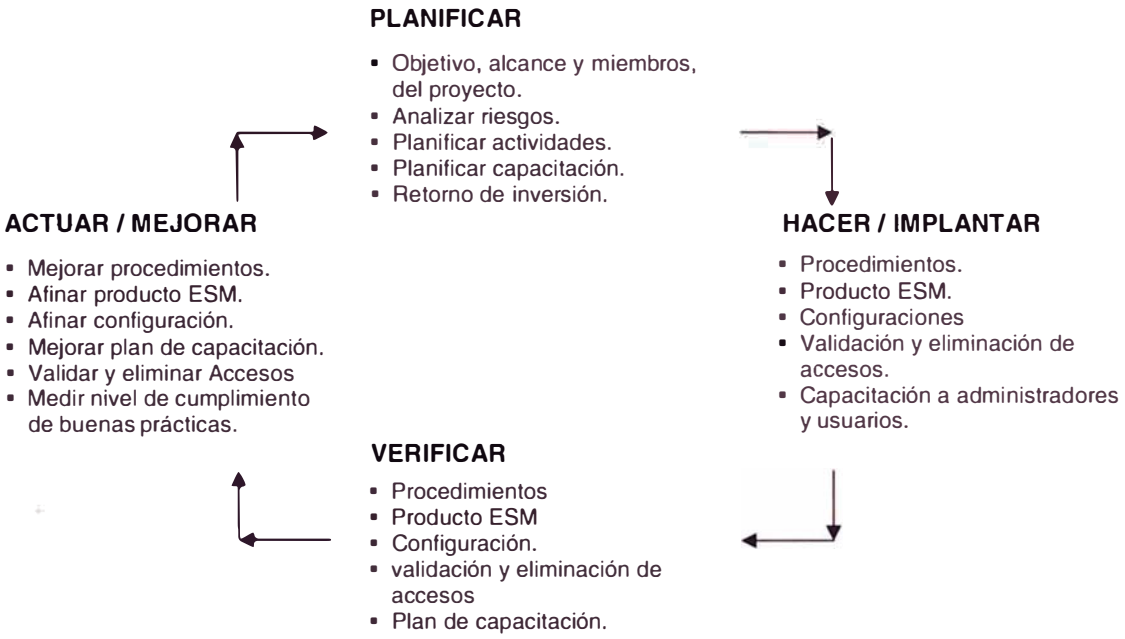


Figura 3-1. Desarrollo de la solución utilizando modelo Planificar-Hacer-Verificar-Actuar

3.6.1 Planificar

3.6.1.1 Alcance del proyecto

Mejorar los niveles de seguridad de los accesos a los 32 servidores, cumpliendo por lo menos con el 90% de buenas prácticas de control de accesos en la seguridad de información; implantando, verificando y mejorando: procedimientos, el producto ESM, configuraciones de

parámetros de seguridad en lo servidores, validaciones de cuentas de accesos y capacitaciones a los administradores y usuarios.

3.6.1.2 Miembros del proyecto

El equipo de trabajo está compuesto por 9 integrantes, distribuido de la siguiente manera:

a) Empresa (7 Personas)

- Un Jefe de Proyecto: Supervisor de Seguridad de Información y encargado de planificar conjuntamente con el Ingeniero (proveedor) de las actividades de mejora de los niveles de seguridad.
- Un Analista de Seguridad de Información: Responsable de validar accesos; elaborar reportes, procedimientos; coordinar con el personal de soporte y administradores de los servidores para la mejora de seguridad.
- Un Analista de Seguridad de Información: Encargado de la Inducción de seguridad de información al personal de la empresa.
- Cuatro administradores de servidores: Encargado de configura en el servidor los parámetros de seguridad y corregir las vulnerabilidades encontradas en los servidores. Compuesto por:
  - 1 Administrador de servidores UNIX
  - 1 Administrador de servidores OPENVMS
  - 1 Administrador de servidores WINDOW2K – Red y Correo
  - 1 Administrador de servidores WINDOW2K – Aplicaciones y Base de Datos

b) Proveedor (2 Personas)

- Un Ingeniero: Encargado de planificar y asesorar en lo concerniente a la mejoras prácticas de seguridad de acceso en los servidores. Debe aplicar su experiencia y compartir casos de éxitos.
- Una Persona de Soporte: Encargado de instalar y dar soporte operativo al producto ESM

3.6.1.3 Arquitectura de la Red Corporativa

Accesos Externos

En la Figura 3.2 se muestra las redes externas conectadas a la red interna, como es el caso de las contratas, agencias, Internet y redes de clientes a las que se les brinda servicios de red, correo y/o aplicaciones. Los tipos de conexiones son diversas, tales como: Línea dedicada, Speedy, Infovía, VPN.

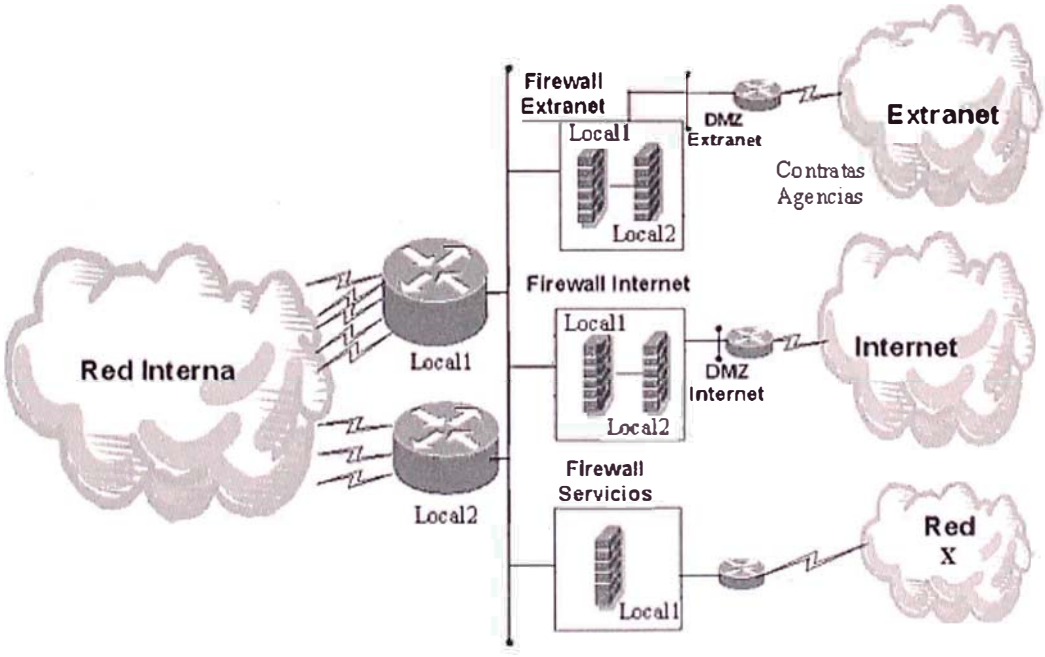


Figura 3-2. Arquitectura de la red externa

Red Interna

Se tiene 12523 usuarios de red distribuidos en cerca de 100 locales a nivel nacional, 10527 computadoras personales (estaciones de trabajo), 465 impresoras y 272 servidores como se muestra en la Figura 3.3.

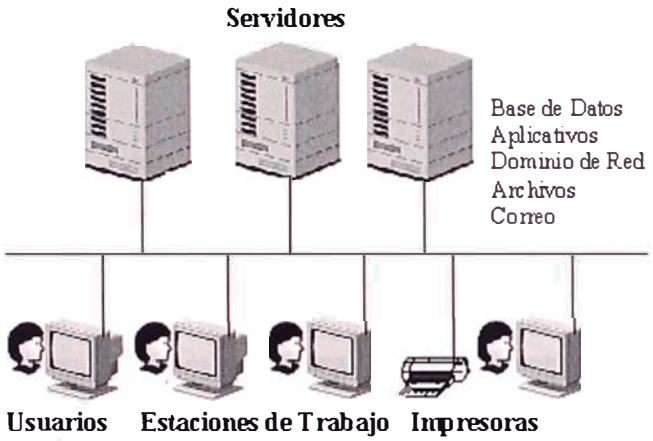


Figura 3-3. Arquitectura de la red interna

3.6.1.4 Análisis de Riesgos

Se realiza un análisis de riesgos, sobre la base de la metodología descrita en la sección 2.5.

a) Vulnerabilidades

Las vulnerabilidades identificadas son:

- No se sigue las normas de seguridad en la gestión de cuentas en los servidores:

  a) Se han creado cuentas de acceso no personalizados, algunas de estas cuentas posee privilegio de administrador. Las malas prácticas en la gestión de cuentas de acceso aumenta el riesgo de que personas no autorizados conozcan las contraseñas. b) Se ha identificado cuentas de usuarios que han sido creados sin autorización del propietario de la información. c) La Dirección de Recursos Humanos no comunica al área de Seguridad de información sobre las personas cesadas de las empresas del grupo, permaneciendo sus cuentas activas, lo cual puede generar represalia por parte del trabajador o que sus cuentas sean usadas por personas no autorizadas. d) Existen cuentas de acceso que no deberían existir ya que están en desuso.
- Contraseñas fáciles de adivinar:

  a) En la creación de la cuenta no se asigna una contraseña segura y/o no se configura en el sistema para que obligue al usuario cambiar su contraseña después de iniciar su primera sesión. b) No se tienen configurado las políticas de contraseñas de acuerdo a lo especificado en la normativa corporativa de Seguridad de Información: longitud mínima de contraseña, vigencia máxima de contraseña, historial de contraseña, complejidad de contraseña.

- No se sigue las normas de seguridad en gestión de privilegios de cuentas en los servidores:

  a) No existe documento donde se indique los privilegios y perfiles existentes en los servidores. b) Existen cuentas de usuarios que tienen más privilegios de los debidos. c) El administrador crea/elimina/modifica las cuentas sin seguir un estándar debidamente documentado.
- Configuración inadecuada de acceso en el sistema operativo:

  a) No bloquea cuentas por intentos fallidos, la opción de acceso remoto se encuentra activada, no se tiene implementado en el servidor la opción de mostrar un mensaje que advierta la restricción de acceso solo a usuarios autorizados. b) No se tiene actualizado los parches de sistemas operativos. c) Existen softwares o programas no autorizados.
- No se revisa periódicamente las cuentas de accesos a lo servidores:

  a) No se identifica evidencia de revisión de las cuentas de accesos, existen usuarios que ya no deben tener cuentas de acceso porque cambiaron de función o cesaron. b) Existe una excesiva cantidad de cuentas de acceso con privilegio de administrador en los servidores. Asismismo, existen cuentas de desarrolladores del sistema que mantienen acceso al computador de producción del Sistema, concentrándose accesos críticos e incompatibles en una sola persona con lo que se podrían modificar datos del negocio sin estar controlados.
- Falta de conocimiento y capacitación de los usuarios sobre su responsabilidad en la seguridad de información: confidencialidad de contraseña, información crítica, entre otros. En visita al centro de cómputo se observó que los terminales de los servidores se encontraban desbloqueados, pudiendo ser manipulados por personas cuya función no le corresponde. Tambien se ha identificado servidores que tiene información con acceso

compartido de acceso público (Permiso de escritura y borrado sobre información y para todos los usuarios de la red corporativa).

b) Amenazas

Se ha identificado las amenazas a partir de datos históricos.

- Robo de información: Ejemplo: Lanzamiento de nuevos productos, planes estratégicos de la empresa.
- Denegación del Servicio a toda la red corporativa, imposibilitando acceder a los recursos de la red corporativa (impresoras, servidores de archivos, computadoras personales) además del correo y aplicaciones corporativas.
- Eliminación o Modificación de Información Confidencial almacenadas en los servidores de la red corporativa.
- Infección con Virus
- Divulgación de información confidencial. Ejemplos: Detalle de llamadas, Datos de Clientes VIP.

c) Riesgos

Se define la tabla de riesgos a partir de las vulnerabilidades y amenazas determinadas en los pasos anteriores.

Identificación de Riesgo	Vulnerabilidad	Amenaza
R1	- Contraseñas fáciles de adivinar. - No se sigue las normas de seguridad conrespecto a la gestión de privilegios de cuentas en los servidores. Se asigna a las cuentas de usuarios más privilegios de los debidos.	Robo de información.
R2	- No se revisa periódicamente las cuentas de accesos a lo servidores. Existen cuentas que ya no deberían tener acceso a las plataforma de sistemas: administradores que dejaron de laborar en la empresa, personas que desarrollaron el sistema, entre otros.	Denegación del Servicio a toda la red corporativa.
R3	- No se sigue las normas de seguridad en lo que respecta a la gestión de cuentas en los servidores: se crean cuentas no personalizadas, no autorizadas; y no se eliminan cuentas correspondiente a personal cesado y las que están en desuso.	Eliminación o Modificación de Información Confidencial
R4	- Configuración inadecuada de acceso en el sistema operativo: Parches no actualizados, Sotware no autorizados.	Infección con Virus
R5	- Falta de conocimiento y capacitación de los usuarios sobre su responsabilidad en la seguridad de información: confidencialidad de contraseña e información crítica, entre otros.	Divulgación de información confidencial.

Tabla 3-8 Riesgos identificados

d) Determinación del Número de Ocurrencias (Frecuencia)

La siguiente tabla muestra el número de ocurrencias anuales de los riesgos identificados anteriormente.

Identificación de Riesgo	Número de Ocurrencias Anuales (NOA)
R1	2
R2	0.4 horas al año. (2 horas sin servicio en 5 años)
R3	12
R4	3
R5	2

Tabla 3-9. Número de Ocurrencias Anuales (NOA)

Asimismo, se determinaron los siguientes cuadros de criticidad del NOA, para cada uno de los riesgos identificados

R1

Rango NOA	Criticidad NOA
$0 \leq x < 1$	Bajo
$1 \leq x < 2$	Medio
$X \geq 2$	Alto

Tabla 3-10. NOA R1

R2

Rango NOA	Criticidad NOA
$0 \leq x < 0.25$	Bajo
$0.25 \leq x < 1$	Medio
$X \geq 1$ (Hora)	Alto

Tabla 3-11. NOA R2

R3

Rango NOA	Criticidad NOA
$0 \leq x < 3$	Bajo
$3 \leq x < 6$	Medio
$X \geq 6$	Alto

Tabla 3-12. NOA R3

R4

Rango NOA	Criticidad NOA
$0 \leq x < 3$	Bajo
$3 \leq x < 6$	Medio
$X \geq 6$	Alto

Tabla 3-13. NOA R4

R5

Rango NOA	Criticidad NOA
$0 \leq x < 1$	Bajo
$1 \leq x < 2$	Medio
$X \geq 2$	Alto

Tabla 3-14. NOA R4

Dado los rangos anteriores, la criticidad de ocurrencias Anuales (NOA) de los riesgos queda de la siguiente manera.

Identificación de Riesgo	Criticidad NOA
R1	Alto
R2	Medio
R3	Alto
R4	Medio
R5	Alto

Tabla 3-15. Criticidad de NOA

e) Determinación del Impacto

Se presentan para cada uno de los riesgos, los factores del impacto relacionados y el costo unitario del impacto (CUI) por cada factor, así como el total del costo unitario del impacto del riesgo. En el caso de R2, el costo unitario es por una hora.

R1

Factor de impacto	Cálculo	Total (S/)
Robo de información que genera perdidas financieras a la empresa	Caso. Información de resultados esperados por lanzamiento de producto. 400 clientes, S/ 20 x cliente x 12 meses	96,000
Total CUI		96,000

Tabla 3-16. Costo Unitario del Impacto (CUI) R1

R2

Factor de impacto	Cálculo	Total (S/)
Paralización de actividades de usuarios por hora	Promedio de salarios/hora x Cantidad de Personas (S/ 1500 / 176 horas) x 12523	106,730
Perdidas financieras por hora	850'000,000 Promedio utilidad Anual / (12 meses/año x 22 días/mes x 8 horas/día)	402,462
Tiempo de personal de sistemas para reponer el servicio por hora	Promedio de salarios/hora x cantidad de personas (administradores y gestores) (S/ 5000 / 176 horas) x 20	568
Total CUI		509,760

Tabla 3-17. CUI R2

R3

Factor de impacto	Cálculo	Total (S/)
Tiempo de Personal de sistemas para restaurar ultima versión de la información borrada	Tiempo afectado en días x Promedio de salarios/día x cantidad de personas 2 x (5000 /22) x 2	909
Tiempo de Usuarios en rehacer	Tiempo en días x Promedio de salarios/día x cantidad de personas 7 x (2500 /22) x 6	4,772
Total CUI		5,681

Tabla 3-18. CUI R3

R4

Factor de impacto	Cálculo	Total (S/)
Tiempo de personal de sistemas para restauración del sistema afectado	Tiempo afectado en días x Promedio de salarios/día x cantidad de personas 2 x (5000 /22) x 2	909
Perdida financiera	Caso. Acceso y captura de clave de cuenta bancaria por terceras personas.	45,000
Total CUI		45,909

Tabla 3-19. CUI R4

R5

Factor de impacto	Cálculo	Total (S/)
Demandas judiciales de información a causa de divulgación de información	Basado en casos	100,000
Perdida de Imagen	(Ingresos/cliente) x Cantidad de	25000

Organizacional	clientes retirados S/ 50 x 500	
Total CUI		125,000

Tabla 3-20. CUI R5

Se tiene los siguientes rangos de valor, para la clasificación del nivel de criticidad CUI

Rango CUI (S/)	Criticidad CUI
$0 \leq x < 45000$	Bajo
$45000 \leq x < 135000$	Medio
$X \geq 135000$	Alto

Tabla 3-21. Rango de CUI

El costo unitario de impacto (CUI) y grado de criticidad CUI, para cada uno de los riesgos identificados queda de la siguiente manera.

Identificación de Riesgo	CUI (S/)	Criticidad CUI
R1	96,000	Medio
R2	509,760	Alto
R3	5,681	Bajo
R4	50,909	Medio
R5	125,000	Medio

Tabla 3-22. Costo y Criticidad de CUI

f) Determinación del Nivel de Riesgo

Se muestra el nivel de riesgo en base a la "Relación de criticidad NOA - CUI"

Criticidad NOA	Criticidad CUI		
	Bajo	**Medio**	**Alto**
Alto	Medio	Medio – Alto	Alto
Medio	Bajo	Medio	Medio - Alto
Bajo	Bajo	Bajo	Medio

Tabla 3-23. Relación Criticidad NOA - CUI

Con base a la Tabla 3.23 El Nivel de criticidad de cada uno de los riesgos son los siguientes:

Identificación de Riesgo	Criticidad NOA	Criticidad CUI	Criticidad del Riesgo
R1	Alto	Medio	Medio – Alto
R2	Medio	Alto	Medio – Alto
R3	Alto	Bajo	Medio
R4	Medio	Medio	Medio
R5	Alto	Medio	Medio – Alto

Tabla 3-24. Criticidad de Riesgos

Se calcula Costo Anual para cada uno de los riesgos, con base en su NOA y CUI cuantitativos, calculando un costo anual total de S/. 851,803.

Identificación de Riesgo	NOA	CUI	Criticidad del Riesgo	(S/) (NOA x CUI)
R1	2	96,000	Medio	192,000
R2	0.4 (horas)	509,760	Medio – Alto	203,904
R3	12	5,681	Medio	68,172
R4	3	45,909	Medio	137,727
R5	2	125,000	Medio – Alto	250,000
Total				**851,803**

Tabla 3-25. Costo Anual de Riesgos

g) Controles

Por cada uno de los riesgos se presenta los siguientes controles.

Identificación de Riesgo:	R1
Amenaza:	Robo de información
Vulnerabilidad:	Contraseñas fáciles de adivinar. a) En la creación de la cuenta no se asigna una contraseña segura y/o no se configura en el sistema para que obligue al usuario cambiar su contraseña después de iniciar su primera sesión. b) No se tiene configurado las políticas de contraseñas de acuerdo a lo especificado en la normativa corporativa de Seguridad de Información: longitud mínima de contraseña, vigencia máxima de contraseña, historial de contraseña, complejidad de contraseña. No se sigue las normas de seguridad en la gestión de privilegios de cuentas en los servidores.a) No existe documento donde se indique los privilegios y perfiles existentes en los servidores. b) Existen cuentas de usuarios que tienen más privilegios de los debidos. c) El administrador crea/elimina/modifica las cuentas sin seguir un

	estándar debidamente documentado.
Control:	Sobre las contraseñas fáciles de adivinar: a) Hacer cumplir el procedimiento de creación de cuentas de usuarios en la asignación de una contraseña temporal segura y la configuración en el sistema para que obligue al usuario cambiarla cuando inicie su primera sesión. b) Configurar en los servidores las políticas de contraseñas: longitud mínima de contraseña igual a 6, vigencia máxima de contraseña igual a 35 días, historial de contraseña igual a 6 y complejidad de contraseña donde ésta no debe ser igual a: cuenta o identificación usuario, identificación de usuario más un prefijo o sufijo, palabras especificadas en un diccionario. Identificar, solicitar al usuario cambio de contraseña (comunicar tips de asignación de contraseñas fácil de recordar y difícil de adivinar). Sobre la gestión de privilegios: a) Elaborar documento donde se indique los privilegios y perfiles existentes en los servidores. b) Hacer cumplir el procedimiento de creación/modificación de cuentas de usuarios en la habilitación solamente de los privilegios necesarios. c) Elaborar procedimiento de creación/eliminación/modificación de cuentas con privilegio administrador.

Tabla 3-26. Control de R1

Identificación de Riesgo:	R2
Amenaza:	Denegación del Servicio a toda la red corporativa.
Vulnerabilidad:	No se revisa periódicamente las cuentas de accesos a lo servidores. a) No se identifican evidencia de revisión de las cuentas de accesos, existen usuarios que ya no deben tener cuentas de acceso debido a que estos cambiaron de función o se encuentra cesado. b) Existe una excesiva cantidad de cuentas de acceso con privilegio de administrador en los servidores. Asismismo, existen cuentas de desarrolladores del sistema que mantienen acceso al computador de producción del Sistema, concentrándose accesos criticos e incompatibles en una sola persona, con lo que se podrían modificar datos del negocio sin estar controlados.
Control:	a) Se debe revisar las cuentas de accesos con el propietario de la información por lo menos cada 6 meses, para ello es necesario la elaboración del procedimiento de revisión de cuentas. Validar las cuentas existentes con el propietario. b) Los administradores del equipo deberán ser los únicos que tengan privilegios de administrador, Asimismo, la cantidad de administradores deberá ser mínima, para ello es necesario la elaboración del procedimiento de revisión de cuentas privilegiadas. Validar cuentas administradores.

Tabla 3-27. Control de R2

Identificación de Riesgo:	R3
Amenaza:	Eliminación o Modificación de Información Confidencial
Vulnerabilidad:	No se sigue las normas de seguridad en la gestión de cuentas en los servidores. a) Se han creado cuentas de acceso no personalizados, algunas de estas cuentas posee privilegio de administrador. Las malas

	prácticas en la gestión de cuentas de acceso aumenta el riesgo de que personas no autorizados conozcan las contraseñas. b) Se ha identificado cuentas de usuarios que han sido creado sin autorización del propietario de la información. c) La Dirección de Recursos Humanos no comunica al área de Seguridad de información las personas cesadas de las empresas del grupo, permaneciendo sus cuentas activas, el cual puede generar represalia por parte del trabajador o que sus cuentas sean usadas por personas no autorizadas. d) Existen cuentas de acceso que no deberían existir ya que están en desuso.
Control:	a) Tal como lo indica la norma de seguridad, se deberá crear cuentas de acceso personalizadas, sobre todo para cada uno de los administradores, para ello en necesario cumplir con el procedimiento de "creación de cuentas de usuarios" asignando cuentas personalizadas por cada usuario. Identificar, validar y de ser el caso eliminar cuentas no personalizadas. b) Se debe hacer cumplir en el procedimiento de creación/modificación de cuentas de usuarios en la que toda creación de cuenta debe estar autorizado por el propietario del servicio. Identificar, validar y de ser el caso eliminar cuentas no autorizadas. c) Elaboración conjuntamente con la dirección de Recursos Humanos del procedimiento de eliminación de cuentas de acceso de las personas cesadas. Eliminar cuentas de Personas cesadas. d) Elaboración del procedimiento de eliminación de cuentas de acceso sin uso hace más de 60 días. Eliminar las cuentas de acceso que no se utilicen en un tiempo mayor a 60 días, tal como lo indica la normativa de seguridad.

Tabla 3-28. Control de R3

Identificación de Riesgo:	R4
Amenaza:	Infección con Virus
Vulnerabilidad:	Configuración inadecuada de acceso en el sistema operativo: a) no bloquea cuentas por intentos fallidos, la opción de acceso remoto se encuentra activada, No se tiene implementado en el servidor la opción de mostrar un mensaje que advierta la restricción de acceso solo a usuarios autorizados. b) No se tiene actualizado los parches de sistemas operativos. c) Existen softwares o programas no autorizados.
Control:	a) Configurar en los servidores la opción: bloquear la cuenta por 5 intentos fallidos, después de ocurrir el error en el ingreso al Sistema, la cuenta debe permanecer inactiva por 30 minutos, mostrar un mensaje al inicio de sesión que advierta la restricción de acceso al sistema sólo a usuarios autorizados. b) Elaborar procedimiento de Instalación de parches en el sistema operativo. Actualizar los parches a los servdores que no lo tienen. Actualizar los parches. c) Elaborar procedimiento de software no autorizados. Validar / desinstalar software no autorizados.

Tabla 3-29. Control de R4

Identificación de Riesgo:	R5
Amenaza:	Divulgación de información confidencial.
Vulnerabilidad:	Falta de conocimiento y capacitación de los usuarios sobre su responsabilidad en la seguridad de información: confidencialidad de contraseña, información crítica, entre otros. En visita al centro de cómputo se observó que los terminales de los servidores se encontraban desbloqueados, pudiendo ser manipulados por personas cuya función no le corresponde. Tambien se ha identificado servidores que tiene información con acceso compartido de acceso público (Permiso de escritura y borrado sobre directorios / archivos con acceso para todos los usuarios de la red corporativa).
Control:	Definir un plan de capacitación para usuarios finales y administradores (incluyendo oficiales de seguridad) sobre actualización de nuevas tecnologías de seguridad. Validar información que tienen compartido de acceso público y comunicar al usuario / administrador compartir de forma privada.

Tabla 3-30. Control de R5

3.6.1.5 Planificar Actividades

El proyecto completo tiene una duración de 6 meses calendario o 132 días útiles, teniendo como fecha de fin programada el 06/09/2006, tal como se muestra en la Tabla 3.31. En el Anexo B, al final de este informe, se adjunta a mayor detalle las de tareas del proyecto.

Nombre de Tarea	Duración	Fecha Inicio	Fecha Fin
PROYECTO Mejora de Nivel de Seguridad	**132 días**	**07/03/2006**	**06/09/2006**
PLANIFICAR	**12 días**	**07/03/2006**	**22/03/2006**
Coordinar: objetivo, miembros, alcance del proyecto	2 días	07/03/2006	08/03/2006
Analizar riesgos	4 días	09/03/2006	14/03/2006
Elaborar plan de capacitación	2 días	15/03/2006	16/03/2006
Elaborar plan de actividades	2 días	17/03/2006	20/03/2006
Retorno de Inversión	2 días	21/03/2006	22/03/2006
IMPLANTAR	**96 días**	**23/03/2006**	**03/08/2006**
Procedimientos	30 días	23/03/2006	03/05/2006
Producto ESM	27 días	23/03/2006	28/04/2006
Configurar	7 días	20/04/2006	28/04/2006
Validar y eliminar accesos	52 días	04/05/2006	14/07/2006
Capacitar administradores y usuarios	66 días	04/05/2006	03/08/2006
REVISAR	**9 días**	**04/08/2006**	**16/08/2006**
Revisar procedimientos	2 días	04/08/2006	07/08/2006
Revisar producto ESM	1 día	08/08/2006	08/08/2006
Revisar configuración	1 día	09/08/2006	09/08/2006
Revisar validación y eliminación de accesos	3 días	10/08/2006	14/08/2006
Revisar plan de capacitación	2 días	15/08/2006	16/08/2006
MEJORA Y CORRECCION	**11 días**	**17/08/2006**	**31/08/2006**
Coordinar y definir acciones correctivas	1 día	17/08/2006	17/08/2006
Mejorar procedimientos	2 días	18/08/2006	21/08/2006
Afinar configuración	1 día	22/08/2006	22/08/2006
Mejorar plan de capacitación	2 días	23/08/2006	24/08/2006
Validar y eliminar accesos	3 días	25/08/2006	29/08/2006
Medir nivel de cumplimiento de buenas practicas	2 días	30/08/2006	31/08/2006
CIERRE	**4 días**	**01/09/2006**	**06/09/2006**
Evaluar resultados	2 días	01/09/2006	04/09/2006
Elaborar informe ejecutivo	2 días	05/09/2006	06/09/2006

Tabla 3-31. Calendario de Actividades del Proyecto

El esfuerzo del proyecto es de 1208 horas / hombre compuesto por 2 consultores externo y 7 miembros de la empresa, tal como se indica en la Tabla 3.32

Personal	Hora/Hombre	Total
Proveedor		80
2 consultores externos: 1 Ingeniero y Personal de Soporte		
Personal Empresa		1128
1 Jefe de Proyecto (Supervisor de Seguridad de Información)	192	
1 Analista (Seguridad de Información)	528	
1 Administrador Plataforma UNIX	160	
1 Administrador Plataforma OpenVMS	80	
1 Administrador de WINDOW2K – Red y Correo.	112	
1 Administrador de WINDOW2K – Aplic. y B. de Datos.	56	
TOTAL de Horas/Hombre		**1208**

Tabla 3-32. Total de Horas / Hombre del Proyecto

3.6.1.6 Planificar Capacitación

Objetivo General: Concientizar al personal en: política, normativa y procedimientos de seguridad de la Información.

Alcance: Todo el personal de la empresa que posea una cuenta de usuario de acceso en las plataformas de sistemas: Administradores de sistemas y Usuarios finales.

Estrategia: Las estrategias a emplear son:

- Metodología de exposición – diálogo.
- Realizar Charlas de Inducción.
- Dar recomendaciones de seguridad a través de pantallas de inicio de sesión y / o correo electrónico en forma masiva a todos los usuarios.

Modalidad

* Formación: Su propósito es impartir a los usuarios finales conocimientos básicos orientados a proporcionar una visión general y amplia con relación a la seguridad de Información

* Actualización / Especialización: Se orienta a los administradores y personal del área de Seguridad de Información a fin de proporcionar conocimientos y experiencias derivados de recientes avances científico -tecnológicos concernientes a la seguridad de Información.

Actividades a desarrollar

	04May-03Jun	04Jun-03jul	04Jul-03Ago
Temas			
Administradores / Personal de Seguridad			
Capacitación	X	X	X
Usuarios Finales			
Charlas de Inducción	X	X	X
Pantallazos al inicio de sesión en la PC	X	X	X
Correos masivo al personal adjuntando boletín	X	X	X
Articulo en la revista "ABCvip"			X

Tabla 3-33. Plan de Actividades de Capacitación

Recursos

La capacitación de los administradores y personal de seguridad a cargo de Empresas Externas.

Para el caso de charlas de inducción así como la difusión a través de inicio de sesión, correo electrónico o revistas lo realiza consultor de Seguridad de Información de la empresa.

3.6.1.8 Retorno de Inversión del proyecto

a) Inversión del Proyecto

Descripción	Unidad	Importe unitario (Nuevo soles)	Importe Total (Nuevo soles)
Producto / Software			302,000
Licencia del producto	1	260,000	260,000
Mantenimiento del producto	1	42,000	42,000
Proveedor			76,000
Consultoría Proveedor	1	76,000	
Personal Empresa			63,736
1 Jefe de Proyecto (Supervisor de Seguridad de Información)	192 horas	55	10,560
1 Analista Gestión de Accesos de Seguridad de Información	528 horas	42	22,176
1 Analista de Inducción de Seguridad de Información	272 horas	48	13,056
1 Administrador UNIX	160 horas	44	7,040
1 Administrador OpenVMS	80 horas	46	3,680
1 Administrador W2K – Red, Correo	112 horas	43	4,816
1 Administrador de W2K. Aplicación y Base de Datos	56 horas	43	2,408
Hardware			18,200
Servidor	1	11,200	11,200
Consolas de monitoreo	2	3,500	7,000
Capacitación y Campañas Seguridad			138,000
Infraestructura / Materiales	40	400	16,000
Bolsas de viajes	15	2,000	30,000
Premios	40	50	2,000
Cursos Administradores	12	7500	90,000
Total (Nuevos soles)			597,936

Tabla 3-34. Inversión del proyecto

b) Costo

Referido al impacto económico en nuevo soles si es que sucediera los riesgos que en suma es S/. 851,803 anuales, tal como se muestra en la Tabla 3.25.

c) Retorno de Inversión

El tiempo de Retorno de la Inversión es aproximadamente ocho meses y medio, lo cual es muy conveniente para la empresa, además

se tendría un ahorro anual de S/. 271,867

Descripción	(Nuevo soles) S/.
Valor de Inversión	597,936
Total Costos anuales	851,803
Retorno de Inversión *	**8.4 meses**
Ahorro anual	**271,867**

Tabla 3-35. Retorno de Inversión del proyecto

* El retorno de inversión del proyecto se calcula del factor (Valor de Inversión) / (Total Costos anuales) multiplicado por 12 meses.

3.6.2 Implantar

3.6.2.1 Implantar Procedimientos

Se revisa los procedimientos existentes para el cumplimiento de las buenas prácticas encontrando solamente implementado y documentado el procedimiento de Creación/eliminación/modificación de cuentas de usuarios.

Se coordina con áreas involucradas: Soporte Usuarios e Infraestructura y Tecnología para elaborar los procedimientos de:

- Eliminación de cuentas de acceso de las personas cesadas.
- Eliminación de cuentas de acceso sin uso hace más de 60 días.
- Creación/eliminación/modificación de cuentas con privilegio administrador.
- Instalación de parches en el sistema operativo.
- Revisión con el propietario de la información de las cuentas y sus privilegios.
- Revisión de cuentas privilegiada.
- Revisión de software o programas no autorizados.

Actualizar los procedimientos de:

- Creación de cuentas de usuarios: En la que se especifica que la asignación de cuentas deben ser únicas o personalizadas por cada usuario.
- Creación/modificación de cuentas de usuarios: Resaltando que la asignación de cuentas, siempre y cuando haya sido autorizado por el propietario del servicio.
- Creación de cuentas de usuarios: En la que se agregue pasos para la asignación de una contraseña temporal segura y la configuración en el sistema para que obligue al usuario cambiar la contraseña cuando inicie su primera sesión.
- Creación/modificación de cuentas de usuarios: especificando que la asignación de privilegios deben ser los necesarios, no se debe asignar más de lo debido.

Se aprueba los procedimientos por parte de la Gerencia General, Dirección de Tecnologías y Sistemas de Información.

Se publica en un repositorio único sobre el servidor de archivos y se difunde los nuevos procedimientos a los administradores y personal de Seguridad.

3.6.2.2 Implantar el Producto

a) Del Producto

Funciones:

Las principales funciones son:

- Configura parámetros de seguridad de acceso en cada plataforma de sistema.
- Genera reportes que permiten evaluar el nivel de Seguridad que ofrece cada sistema.
- Administra todos los sistemas desde una única consola.
- Revisa vulnerabilidades de sistemas y recomienda las acciones a seguir.
- Notifica vía E-mail en forma resumida el estado de seguridad de los sistemas.

Arquitectura

Involucra tres componentes principales, tal como se muestra en la Figura 3.4

- El Agente ESM
- El Manager ESM
- La consola de ESM

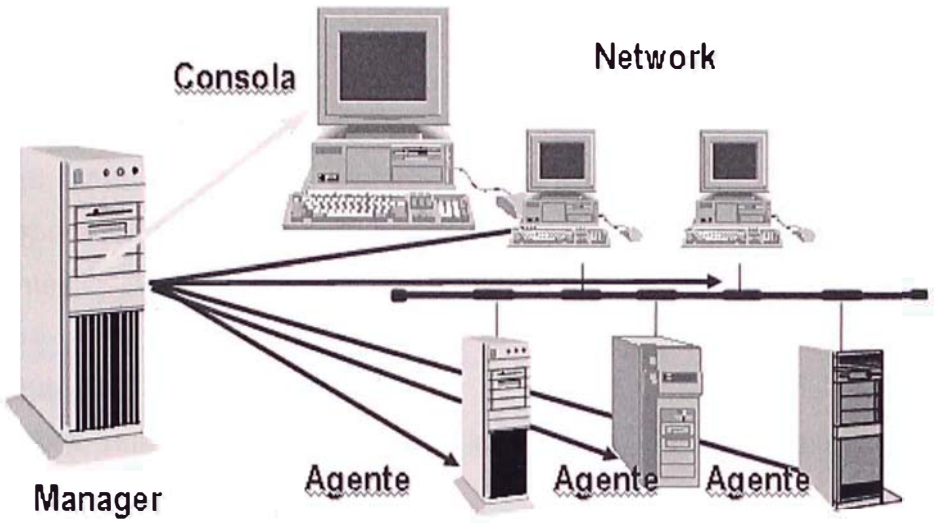


Figura 3-4. Arquitectura del producto ESM

Agentes: Los Agentes ESM son instalados en cada servidor y/o estación de trabajo y se encargan de interpretar la información relativa a la seguridad de los sistemas. El Agente de ESM realiza este análisis ante un requerimiento de ejecución de parte de un "Manager" de ESM. Los módulos de seguridad en el Agente analizan la estación de trabajo, el servidor o la máquina donde el Agente reside. Una vez terminado el análisis, los resultados son enviados al "Manager" de ESM que inició el requerimiento de ejecución. El "Manager" responde actualizando los respectivos archivos en su base de datos.

Manager: Almacena información de seguridad de los Agentes y envía dicha información a la Consola de ESM.

Consola: La consola de ESM es uno de los componentes principales de ESM. A través de la consola se recibe las entradas de datos y se envía requerimientos a otros componentes. En base a la información recibida, la consola formatea los datos para mostrar la información detallada y sumarizada. Además, crea reportes, gráficos tipo pie,

barras y otros objetos visuales que permiten un rápido análisis del nivel de cumplimiento de seguridad en el Sistema. La Figura 3.5 ilustra la Consola de ESM

La arquitectura Manager / Agente permite que el ESM sea escalable, de tal forma que nuevas plataformas de sistemas sean fácilmente incorporados al esquema de seguridad de la empresa en forma de agentes.

Módulos de Seguridad

Contiene tres áreas claves en lo que los sistemas son vulnerables:

Cuentas de usuario y autorizaciones.

- Información de Cuentas
- Integridad de las cuentas
- Parámetros de Ingreso al sistema
- Características de las Contraseñas

Cuentas de Redes y Servidores

- Integridad a nivel Redes
- Parches del Sistema Operativo
- Archivos de Inicio
- Auditoria de los Sistemas

Archivos y Directorios del Sistema.

- Acceso a Archivos
- Atributos de Archivos
- Registro

Políticas de Seguridad del ESM

Una política de Seguridad contiene un conjunto de módulo de Seguridad. Una política define la configuración que el sistema debe tener para satisfacer los estándares de seguridad dentro de la empresa.

b) Actividades

Coordinar

Se realiza una reunión entre la empresa y el proveedor para coordinar las acciones a desarrollar en la implementación de ESM. Se acuerda una distribución preliminar de los Managers y Agentes de ESM a instalar por plataforma y servidores.

Capacitar

Se realiza la presentación del producto ESM a los Administradores. Durante la presentación se describió los alcances del producto y los objetivos básicos que se busca con la implementación del ESM. Se discutió varios aspectos relacionados a la seguridad de los ambientes y el consumo de recursos.

Instalar

Ambiente de Pruebas

En esta fase la empresa define los servidores sobre los cuales se va instalar, se realiza la instalación, Se revisa la evaluación de ESM sobre los Servidores pilotos y no se reportan problemas acerca de la ejecución de Políticas.

Producción

En esta fase se coordina la instalación del ESM y ubicación de los Managers, asimismo, se instala el producto en los 32 servidores críticos (3 Open Vms, 15 Unix y 14 Windows).

Se configura producto ESM y se ejecuta revisión de Seguridad sobre los Servidores instalados, encontrando las siguientes observaciones:

- Excesivas cuentas con privilegio de administrador. De un total de 357 cuentas se tiene más de 130 cuentas en la red de Windows.
- Se tiene 532 cuentas no personalizadas de los cuales 355 pertenecen a cuentas de usuarios de ingreso a la red de

Windows.

- Existen 285 cuentas pertenecientes a personal cesado
- 153 usuarios que comparten sus cuentas
- 856 cuentas sin uso hace más de 60 días
- 652 contraseñas fáciles de adivinar
- 161 usuarios que comparten su directorio o archivos de forma pública
- En promedio por servidor se tiene 18 parches no instalados. En 12 servidores se tiene actualizado todos los parches recomendados.
- En promedio por servidor se tiene 4 servicios instalados que no son identificados como autorizados por la empresa. En 7 servidores se tiene que todos los servicios están permitidos.
- Configuración inadecuada de acceso en el sistema operativo: no bloquea cuentas por intentos fallidos, permite asignar contraseñas menor a 6 caracteres o las 6 ultimas contraseñas, la opción de acceso remoto se encuentra activada. Se tienen 72 de 256 configuracones de políticas de cuentas y contraseña en todos los servidores.

3.6.2.3 Configuraciones

Se agrupa por tipo de plataforma de servidores UNIX, OpenVMS, y Windows, este último separado en dos subgrupos: a) por servidores de la red y b) aplicaciones y base de datos

Se coordina con los responsables de los grupos de plataformas las configuraciones a realizar sobre los parámetros de seguridad.

Los administradores configuran en todos los servidores las siguientes opciones:

- No permitir asignar una contraseña menor a 6 caracteres.
- No permitir asignar una contraseña igual a las 6 últimas contraseñas.
- Contraseña debe expirar cada 35 días.
- Contraseña no debe ser igual a identificación usuario, ni identificación de usuario más un prefijo o sufijo, ni palabras especificadas en un diccionario.
- Bloquear la cuenta por 5 intentos fallidos
- Después de ocurrir el error en el ingreso al Sistema, la cuenta permanecerá inactiva por 30 minutos.
- Se desactiva el servicio de acceso remoto.
- Se muestra un mensaje al inicio de sesión que advierta la restricción de acceso al sistema sólo a usuarios autorizados.

3.6.2.4 Validación y eliminación accesos

Se valida y elimina los accesos de acuerdo a las vulnerabilidades identificadas en el punto "a" de la sección 3.5.1.5 (Análisis de Riesgos), así como los reportados por el producto ESM.

a) Cuenta / Identificador de Usuario

Valida las cuentas existentes con el propietario: Se elabora reporte de cuentas del sistema y se comunica esta relación vía correo electrónico al propietario de la información del sistema. Se da un plazo de 5 días para que este responda. Los accesos no validados por el propietario se proceden a eliminar y los demás se registran como autorizados y se guarda la infomación para fines de auditoría en la empresa.

Valida cuentas administradores: Se elabora reporte de cuentas con privilegio de administrador y se comunica vía correo electrónico a los

administradores del sistema, según corresponda a fin de que validen si estas cuentas deben permanecer. El analista de Seguridad procede a retirar privilegios de aquellos que no los requieren o elimina cuentas por falta de uso o que pertenecían a personal cesado de la empresa.

Valida y/o elimina cuentas no personalizadas: Se elabora reportes de cuentas no personalizadas o denominadas tambien cuentas genericas, las cuales tienen nombres no comunes, asimismo no se tiene identificado al responsable, tales como: lima01, multiservicio. Normalmente estas cuentas suelen ser usadas para accesos no autorizados. Se valida con el administrador las cuentas de sistemas debido a que estos puedes ser utilizados por un servicio o software que requiere el sistema para su correcto funcionamiento. Estas cuentas no son consideradas para la depuración y se registra al responsable de la cuenta y se guarda la información para fines de auditoria. De las cuentas restantes se procede a validar los accesos con los usuarios. Para el caso de las cuentas de red, debido a que se encontraron aproximadamente 350 usuarios se comunica via pantalla de inicio de sesión a todos los usuarios de la red que tienen dies días utiles para reportar el uso y responsable de las cuentas, cumplido este plazo se procede a eliminar las cuentas. Para el caso de las cuentas que fueron reportadas en uso, se gestiona el cambio a cuentas personalizadas.

***Elimina cuentas de Personas cesadas*:** Se identifica las cuentas de personas cesadas cruzando la información de cuentas versus la relación de personal cesado registrado en el sistema de Recursos Humanos, luego se procede al bloqueo de las cuentas y tres días después se elimina definitivamente del sistema.

Elimina las cuentas de acceso sin uso: Se identifica las cuentas que no se utilizan por un tiempo mayor a 60 días, se exceptua las cuentas de usuarios con licencia u otras inasistencias jutificadas. Las cuentas restantes son bloqueadas y tres dias despues eliminadas.

b) Contraseña de usuario

Se identifica los usuarios que tienen contraseñas fáciles de adivinar. El producto reporta como contraseña fácil de adivinar cuando es igual a identificación usuario, identificación de usuario más un prefijo o sufijo o palabras especificadas en un diccionario.

Se solicita a los usuarios cambio de sus contraseñas, para ello se les envia un correo electrónico personalizado donde se oriente como realizar el cambio, asimismo se adjunta boletin con tips de asignación de contraseñas fácil de recordar y dificil de adivinar.

c) Programa \ Software

Actualiza los parches: Se identifica los parches no actualizados por el sistema. El administrador revisa estos, parches y, de ser el caso procede a actualizar en el sistema, previamente revisa en maquinas de prueba,que los parches no afecten la disponiblidad del sistema o recursos de los mismos y que a su vez sea util para las funciones o servicios del servidor.

Valida / desinstala programas no autorizados: Se identifica los programas o softwares no autorizados. El producto ESM revisa los programas autorizados comparando con su base de datos de programas autorizados y al no encontrarlos, emite una alerta y reporta como vulnerabilidad de programa no autorizado, para ello el administrador revisa y valida estos programas. Desintala aquellos programas no autorizados, caso contrario registra en la Base de datos como programas autorizados.

d) Archivo y directorio del sistema

Descomparte archivos y directorios que se tiene compartido con acceso público: Se identifica todos los archivos y directorios compartidos para todo los usuarios y con acceso total, el cual puede

ser accesado de forma casual o intencional para obtener información no autorizada, tambien puede ser modificada o eliminada, además estos directorios son apovechados por los virus para instalarse en el sistema. Se comunica a los administradores o usuaro (propietario o responsable del archivo o directorio) a fin de que asignen los permisos puntualmente a los usuarios que necesitan acceder a la información, así como el acceso minimo necesario (lectura, cambio, listado, entre otros). En caso de no tener respuesta a los 5 días y si las carpetas continuan desprotegidos, se descomparte los archivos y directorios a fin de prevenir, como se comento al inicio, de accesos no autorizados.

3.6.2.5 Capacitación y Charlas de Seguridad

Comprende:

- actualizar / especializar administradores y personal de seguridad en cursos de seguridad de información y administración de las plataformas de sistemas.
- Capacitar a usuarios finales mediante charlas y difusión de boletines de consejos prácticos de seguridad de información.

a) Capacitar a administradores y personal de Seguridad:

Se capacitan en los siguientes cursos a través de instituciones educativas especializadas en la materia.

Diplomado en Seguridad Informática: Este diplomado da a conocer las bases teóricas y tecnológicas que permitan al participante conocer los principios internacionalmente aceptados y dar los elementos para poner en práctica la arquitectura de seguridad en las empresas, identificando los servicios y mecanismos en los diferentes niveles de los sistemas informáticos y su ambiente operativo en el manejo seguro de la información. 2 participantes.

Especialista en Seguridad de Información. Este curso dio a conocer detalladamente los requerimiento de los lineamientos de la ISO y el cual permitirían de una forma exitosa y efectiva llevar a cabo la implantación de este sistema de gestión de seguridad como también adecuar las funciones de auditoria en un ambiente empresarial. Este permite a través del conocimiento adquirido, reducir los riesgos de Seguridad, incrementar el cumplimiento de leyes y regulaciones y lograr en la organización la confianza en su efectividad de los niveles de protección de la información y otros activos críticos. 4 Participantes

Seguridad Avanzada en UNIX: Este curso teórico-práctico muestra con un alto grado de profundidad los aspectos más relevantes de la seguridad en sistemas operativos de Tipo Unix. El curso se presento en dos escenarios: el primero de ellos muestra las técnicas de ataque que pueden ser utilizadas para infiltrar un servidor con este tipo de sistema operativo, y el segundo muestra las estrategias de corrección y aseguramiento que permiten mitigar los riesgos de Seguridad de la Información presentados inicialmente. 2 Participantes

Diseño de Seguridad para Redes Windows: Este curso proporciona los conocimientos y habilidades para diseñar una infraestructura de red segura. Los temas incluyen el análisis, diseño de la red, y el análisis de riesgos de seguridad con el fin de satisfacer las necesidades del negocio para asegurar las computadoras en un entorno de red. 4 participantes

Inversión aproximada S/ 90,000.

b) Capacitar usuarios finales

Se realizan las siguientes actividades

Charlas

Se realizan un total de 40 Charlas. 27 de ellas en Lima y 13 en Provincias (Huancayo, Piura, Cajamarca, Tumbes, Chiclayo, Iquitos, Arequipa, Cusco, Moquegua, Puno, Tacna, Ica y Pisco). Participan 856 trabajadores.

El objetivo de esta presentación es dar a conocer las responsabilidades de todos los empleados para proteger la información que maneja la empresa a nivel informático y así reducir los riesgos a los que está expuesta. Los temas tratados fueron:

- ¿Donde está la información?
- Principios de Seguridad de Información
- Servicios de Seguridad de Información
- Normativa de cuentas de accesos de usuarios
- Recomendaciones para uso de cuentas de Acceso, para crear una contraseña, de bloqueo de estación de trabajo, no compartir su carpeta sin restricción.
- No caer en Ingeniería social

Se hace entrega de encuesta sobre la utilidad de la charla.
Se premia a los participantes con usbs, polos, lapiceros que acierten con preguntas realizadas por el expositor.

Pantallazos al inicio de sesión en la PC

Se realiza prestación de pantallas al inicio de sesión de la red Windows mostrando presentaciones con contenidos de interés para

los empleados.

Las presentaciones realizadas son:

- No compartir cuentas de usuario
- Recomendación de contraseñas
- Bloqueo de Estación
- Carpetas Compartidas
- Ingeniería Social
- Virus Informático
- Software No Autorizado
- Test de Seguridad

Cada una de ellas se presenta durante todos los días por una semana. En el Anexo C, al final de este informe, se adjunta la presentación de bloqueo de estación.

Correos masivo al personal adjuntando boletín

Se envía a todo el personal que tiene un correo corporativo en la empresa boletines de las buenas prácticas de seguridad de información. Estos boletines tienen el mismo contenido que las presentaciones. En el Anexo D, al final de este informe, se adjunta boletín de Recomendación de contraseñas

Articulo en la revista "ABCvip"

Se contacta con el área de prensa de la revistas ABCvip y se coordina la publicación de importancia de seguridad de información en la empresa, cuyo usuario son los directivos de la empresas del grupo.

3.6.3 Verificar

Se revisa que lo definido este siendo ejecutado en la realidad.

3.6.3.1 Procedimientos

Se define 11 procedimientos por implantar: 7 procedimientos por elaborar y 4 por actualizar, de los cuales, se tiene que 9 procedimientos se han implantado quedando 2 procedimientos pendientes de aprobación por la gerencia.

- Creación/eliminación/modificación de cuentas con privilegio administrador
- Revisión de software o programas no autorizados

Se revisa cumplimiento de procedimiento implementados a través de auditoria interna, encontrando que los administradores conocen y aplica los procedimientos al 95%.

Se ha documentado para todas las plataformas de sistemas, la descripción de los privilegios o perfiles del sistema.

3.6.3.2 Producto ESM

Se define la instalación del producto: 2 Consolas, 1 Manager, 32 Agentes, de los cuales se revisa que se han instalado al 100%.

3.6.3.3 Configuración

Se revisa la configuración de accesos en los servidores a través de reportes ESM

Sobre la configuración de opciones de cuentas y contraseña se tiene que en 30 de 32 servidores se ha realizado de acuerdo a las mejores

prácticas, quedando solamente pendientes configurar las siguientes opciones en las plataformas de CobranzaLima y CobranzaProv:

- El sistema no debe permitir asignar una contraseña igual a las 6 últimas contraseñas.
- El sistema debe forzar cambiar la contraseña cada 35 días calendario.
- No se debe asignar contraseña fácil de adivinar: contraseña no debe ser igual a Identificación del Usuario (con prefijo, sufijo), o no debe ser igual a una de las palabras especificadas en un diccionario.
- El sistema debe bloquear la cuenta por 5 intentos fallidos.
- Después de ocurrir el error en el ingreso al Sistema, la cuenta deberá permanecer inactiva por 30 minutos.

Se configura la opción de que muestre al inicio de sesión un mensaje que advierta la restricción de acceso al sistema sólo a usuarios autorizados sobre los 14 servidores faltantes, cumpliendo al 100 % esta práctica.

Se identifica que no se tienen actualizado o validado todos los parches en los servidores DataWareHouse, LargaDistancia, TelefIntern, FileServerGrupal, FileServerPersonal

Se identifica que aun no se ha desactivado o retirado todas las facilidades basadas en software que no sean necesarios, sobre los servidores de: Instalaciones, RedCorpDomN1, RedCorpDomN2, RedCorpDomO1, RedCorpDomS1 y RedCorpDomS2, Correo.

3.6.3.4 Validación y eliminación de cuentas de accesos

Se revisa el estado de cuentas reportados por el ESM encontrando lo siguiente

- Existen cuentas no personalizadas en las plataformas de sistemas de cable, red corporativa y correo. En el primer caso no se tiene avance al respecto, en los siguientes casos se tiene un avance de 89 % y 87 % respectivamente.
- Existen cuentas sin uso hace más de 60 días en las plataformas de COBAN, SAP y red corporativa. En el primer caso y segundo no se tiene avance al respecto y en el tercero se tiene un avance al 80%
- Sobre las cuentas con privilegio de administrador esta pendiente la revisión de los administradores de las plataformas FacturaLima, CobranzaLima y AClientesLima.

3.6.3.4 Plan de capacitación

Sobre capacitación a los administradores y personal de Seguridad de Información se revisa los cuestionarios de evaluación de cursos llevados, encontrando que se cumplió en un 92% con las expectativas de los asistentes.

Sobre las charlas se ha contado con una participación de 83% de los usuarios programados.

Se revisa el grado de responsabilidad de usuarios sobre la seguridad de información

- Cuentas: Se elabora reporte de uso de cuenta en más de dos estaciones de trabajo encontrando 28 usuarios comparten su cuenta.
- Contraseñas: Mediante reporte ESM, se identifica 153 contraseñas fáciles de adivinar.
- Escritorios: Con el apoyo de vigilancia de los locales se identifica 2 usuarios que tienen sus contraseñas escritas en posit.
- Archivo y Directorios: Se elabora reporte de archivos y directorios encontrando 28 de ellos compartido para todos los usuarios y con permiso de control total.

3.6.4 Mejorar

Se comunica a todos los miembros del proyecto las revisiones realizadas en la sección 3.5.3, en la que define las siguientes acciones:

El Jefe de Proyecto debe coordinar con la dirección de Tecnología y Sistemas de Información la aprobación de los procedimientos que aun no se han aprobado.

Los administradores de las plataformas deben:

- Configurar en los servidores faltantes las opciones de cuentas y contraseñas según las mejores prácticas.
- Revisar cuentas con privilegios de administrador y eliminar cuentas que no son necesarias.
- Actualizar y/o validar los parches.
- Desactivar programas o servicios que no son necesarios.

El analista de Seguridad debe:

- Coordinar con el propietario de la información la revisión de las cuentas y sus privilegios.
- Sobre los servidores faltantes de revisión de accesos, se deben: validar y eliminar cuentas no personalizadas, eliminar cuentas sin uso.
- Revisar periódicamente cumplimiento de procedimientos

El analista de Inducción de Seguridad debe:

- Continuar con las charlas y difusiones de boletines sobre seguridad de información.
- Emitir reportes a la Jefaturas de los usuarios que incumplen la norma de seguridad de información

CAPÍTULO IV

EVALUACIÓN DE RESULTADOS

En el mes de setiembre del 2006, posterior a las mejoras realizadas, se mide los niveles de seguridad en los 32 servidores, el cual se obtiene de acuerdo a revisiones de cumplimiento de buenas prácticas de controles de accesos, referido a gestión de de acceso y responsabilidad de usuarios sobre la seguridad de información en las plataformas de sistemas.

Por Servidor

En la Tabla 4.1 se muestra por cada servidor los niveles de seguridad (% de cumplimiento de buenas prácticas), en la cual se puede observar que 28 de 32 servidores tienen un nivel de cumplimiento de seguridad mayor al 90%. El nivel de seguridad promedio de todos lo servidores es 91.6%

Servidor	Nivel de Seguridad
FacturaLima	90.2%
CobranzaLima	79.8%
AClientesLima	79.9%
FacturaProv	90.4%
CobranzaProv	82.7%
Empresas	92.9%
Cable	87.0%
Comercial	92.4%
Instalaciones	92.0%
DataWareHouse	90.8%
Guías	91.9%
LargaDistancia	91.5%
RRHH	92.9%
SAPBD	96.2%
SAPContable	96.4%
TelefIntern	90.6%
Tups	95.0%
COBAN	90.7%
Cobros	95.8%
FileServerGrupal	91.9%
FileServerPersonal	91.9%
RedCorpDomC1	91.5%
RedCorpDomC2	95.5%
RedCorpDomN1	92.5%
RedCorpDomN2	92.1%
RedCorpDomO1	92.7%
RedCorpDomS1	93.4%
RedCorpDomS2	91.9%
Correo	90.1%
AdminReport	96.5%
AplicLotus	98.4%
SIO	92.5%
Nivel de seguridad PROMEDIO	91.6%

Tabla 4-1. Resultados de Niveles de Seguridad de los Servidores

Por buena práctica

En la Tabla 4.2 se muestra por cada buena práctica el porcentaje de cumplimiento medido sobre los 32 servidores, en la cual se puede observar que 21 de 30 buenas prácticas tienen un nivel de cumplimiento mayor al 90%.

Buena Práctica de Control de Accesos \ Servidor	% Cumplimiento
1. Gestión de acceso de usuarios	
1.1 Gestión de cuentas/identificadores de usuarios	
Se debe tener procedimiento de creación/eliminación/modificación de cuentas de usuarios.	100.0%
Cada usuario debe tener su propio y único identificador, prohibiéndose que varios usuarios lo compartan.	93.4%
El propietario del servicio o información debe autorizar el acceso al usuario.	100.0%
Eliminar las cuentas de acceso de los usuarios que y no pertenezcan a la organización (personal cesado) o retirado.	100.0%
Eliminar las cuentas de acceso de los usuarios que se encuentran inactivos (sin uso) hace más de 60 días.	93.1%
1.2 Gestión de contraseñas de usuarios	
Proporcionar inicialmente una contraseña temporal segura, que el sistema debe obligar al usuario cambiar inmediatamente después de inicio de sesión.	100.0%
El sistema no debe permitir asignar una contraseña menor a 6 caracteres.	100.0%
El sistema no debe permitir asignar una contraseña igual a las 6 últimas contraseñas.	100.0%
El sistema debe forzar cambiar la contraseña cada 35 días calendario.	100.0%
La contraseña no debe visualizarse en pantalla durante la introducción de la misma.	100.0%
Contraseña debe ser fácil de recordar y difícil de adivinar: contraseña no debe ser igual a Identificación del Usuario (con prefijo, sufijo), no debe ser igual a una de las palabras especificadas en un diccionario.	100.0%
1.3 Gestión de privilegios de usuarios	
Identificar los privilegios asociados a cada elemento del sistema. Resaltar cuentas con privilegios de administración.	100.0%
Asignar privilegios según "necesidad de su uso" y "caso por caso" (asignar el permiso necesario para que pueda desempeñar su labor).	90.6%
Se debe tener procedimiento de creación/eliminación/modificación de cuentas con privilegio administrador.	72.0%
1.4 Control de acceso al sistema operativo	
El sistema debe mostrar un mensaje al inicio de sesión que advierta la restricción de acceso al sistema sólo a usuarios autorizados.	96.9%
El sistema debe bloquear la cuenta por 5 intentos fallidos.	93.8%
Después de ocurrir el error en el ingreso al Sistema, la cuenta deberá permanecer inactiva por 30 minutos.	93.8%
Se recomienda que la opción de servicio de acceso remoto debe estar desactivada.	81.3%
Se debe tener actualizado los parches de sistemas operativos.	84.4%
Desactivar o retirar todas las facilidades basadas en software que no sean necesarios. No se debe tener servicios instalados que no han sido definidos como permisibles para el sistema.	78.1%
1.5 Revisión de los derechos de acceso de los usuarios	
Revisar los derechos de accesos de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses).	74.8%
Revisar las cuentas privilegiadas periódicamente (se recomienda cada semana).	90.6%
2. Responsabilidad de los usuarios	
2.1 Uso de cuentas	
Cada usuario debe ingresar con su propia "cuenta de usuario" y no debe compartirla. El usuario es responsable por todas las acciones que se realicen con su "cuenta".	81.7%

		El usuario no debe usar cuentas especiales o aprovechar fallas en la seguridad de los sistemas, para obtener un acceso no autorizado.	94.7%
	2.2 Uso de contraseñas		
		Mantener la confidencialidad de las contraseñas. Evitar guardar registros (papel, archivos de software o dispositivos).	93.3%
		Seleccionar contraseñas de buena calidad, con una longitud mínima caracteres que sean fáciles de recordar, no estén basas en algo que cualquiera pueda adivinar.	76.5%
		Cambiar las contraseñas en intervalos de tiempo regulares (menor a 35 días).	100.0%
	2.3 Equipo informático de usuario desatendido		
		Bloquear su sesión o habilitar un protector de pantalla para evitar accesos no autorizados usando su cuenta. Desconectar (log-off) los servidores o los computadores centrales cuando se ha terminado la sesión	93.7%
		Al término del trabajo diario, cierra todas las sesiones y apaga tu computadora antes de retirarte de la oficina.	77.4%
	2.4 Uso de archivo y directorios		
		No compartir sus archivos o directorios por defecto. Este no debe quedar con acceso de control total y a su vez con permiso para todos los usuarios de la red corporativa.	83.9%
Nivel de seguridad (% de cumplimiento de buenas prácticas)			91.6%

Tabla 4-2. Resultados de Niveles de Seguridad por buena práctica

En la Tabla 4.3 se muestra indicadores de gestión de accesos y responsabilidad de usuarios que se usa para medir el cumplimiento de buenas practicas en las 32 plataformas de sistemas.

Área	Medición	Objetivo	Inicio Proy. 07/03/06	Fin Proy. 06/09/06	% Cumplimiento
Gestión de acceso de usuarios	Procedimiento				
	Procedimientos implementados	11	1	9	81.8%
	Verificación de cumplimiento de procedimientos	> 90%	-	95%	95.0%
	Documentos de descripción de privilegios en los sistemas	32	16	32	100.0%
	Sistema Operativo				
	Configuración de políticas de cuentas y contraseñas	256	72	246	96.1%
	Instalación del producto ESM	100%	-	100%	100.0%
	Actualización de parches en servidores	32	12	27	84.4%
	Desinstalación de programas no autorizados en servidores	32	7	25	78.1%
	Validación/ Eliminación de accesos				
	Cuentas administradores	< 35	357	34	90.4%
	Cuentas no personalizadas	< 53	532	36	93.2%
	Cuentas de Personas cesadas	< 28	285	0	100.0%
	Cuentas sin uso	< 85	856	59	93.1%
Responsabilidad de usuarios	Administradores y personal de Seguridad				
	Encuestas de satisfacción	> 90%	-	-	95%
	Usuarios				
	Asistencia a Charlas	> 90%	-	83%	85.0%
	Carpetas compartidas con acceso público	< 16	161	25	84.5%
	Cuentas compartidas	< 15	153	28	81.7%
	Contraseñas fáciles de adivinar	< 65	652	153	76.5%
	Bloqueo de pantallas	< 5	50	3	94.0%
	Escritorios limpio	< 3	30	2	93.3%

Tabla 4-3. Indicadores de gestión de acceso y concientización y responsabilidad de usuarios

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. Se tiene que 28 de 32 plataformas de sistemas (87.5%) superan el cumplimiento del 90% de recomendaciones de buenas prácticas de control de accesos, porcentaje mínimo establecido en la política de la empresa para tener un nivel adecuado de Seguridad de Información al 2006.

2. Se mejora los niveles de seguridad de información. En promedio para todas las plataformas se tiene un nivel de seguridad de 91.6% a setiembre del 2006, mejorando en un 62.3% comparado con la medición realizada en marzo del 2006.

3. Los socios, los accionistas, el personal y los clientes confían en la seguridad de la empresa debido a la importancia que ésta brinda a la protección de la información.

4. El producto ESM permite ahorrar 192 horas de trabajo en la elaboración de reportes.

5. El presente informe aporta al área de seguridad de información de los sistemas conocimientos y experiencias en metodología de evaluación de soluciones, análisis de riesgos, retorno a la inversión en seguridad de información y uso del modelo PDCA.

   - La metodología de evaluación de soluciones permite cuantificar y ponderar los criterios de evaluación a fin de tomar una decisión en base al que tiene mayor calificación, siempre y cuando este cumpla con el 69% de los criterios establecidos. Las ponderaciones y criterios pueden variar de acuerdo a las características de cada empresa.
   - El análisis de riesgos permite identificar, analizar, evaluar y tratar los riesgos en base a las vulnerabilidades y amenazas identificadas sobre los activos de la empresa. De este análisis se tiene que el impacto económico es S/.851,803 anuales y la inversión para mitigarlos es de S/.597,936.
   - El modelo de retorno de la inversión en seguridad de información se usa para estimar en cuanto tiempo retorna la inversión en seguridad de información. El modelo empleado calcula el retorno de inversión dividiendo el costo de tratar los riesgos entre el costo del impacto anual y a este resultado se multiplica doce. Para el proyecto se tiene un retorno de inversión en ocho meses y medio y un ahorro de S/ 271,867 anuales.
   - El modelo PDCA se usa para implementar, mantener y administrar un sistema de gestión de la seguridad de información. En este caso se emplea para planificar, implantar, revisar y mejorar procesos en las áreas de gestión de accesos y concientización y responsabilidad de usuarios en las plataformas de sistemas de acuerdo a estándares acordadas.

Recomendaciones:

1. Realizar una mejora continua en los procesos de gestión de seguridad de información ya que la tecnología avanza apareciendo nuevas técnicas para fines delictivos.

2. Continuar con las charlas y difusiones de boletines sobre seguridad de información, capacitar a los administradores y oficiales de seguridad.

3. Obtener una certificación ISO /IEC 27001 que permita a la empresa garantizar que ante eventuales riesgos presentes o futuros tiene implementado un sistema de seguridad para la protección de su información, asimismo ofrezca una imagen de calidad y solidez en su mercado. En un inicio se puede empezar con los procesos de: gestión de accesos de usuarios y gestión de incidencias. teniendo en cuenta que es más sencillo crecer de un núcleo que hacerlo todo desde cero.

GLOSARIO DE TÉRMINOS

Activo: Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Aplicación: Un programa que lleva a cabo una función directamente para un usuario.

Archivo: Es un grupo de datos estructurados que son almacenados en algún medio y pueden ser usados por las aplicaciones.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Base de Datos: Conjunto estructurado de datos para permitir su almacenamiento, consulta y actualización en un sistema informático.

Carpeta: Agrupación de archivos de datos, atendiendo a su contenido, a su propósito o a cualquier criterio que decida el usuario. Sirven para organizar mejor los archivos en un disco de almacenamiento.

Confidencialidad: Acceso a la información por parte únicamente de

quienes estén autorizados. Característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Configurar: Significa elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado.

Contraseña: Conjunto de letras, números y símbolos, o incluso frases, utilizadas para autenticar usuarios en un sistema informático. Para que el uso de contraseñas sea efectivo es necesario escogerlas de manera que sean difíciles de adivinar para un atacante.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Cuenta: Cadena de caracteres que se utiliza para identificar a un usuario en la entrada a un sistema, como un sistema operativo, una red, aplicación. Generalmente el nombre de usuario va acompañado de una contraseña única para éste.

Denegación de servicio: Ataque informático que, sin afectar a la información contenida en un sistema, lo deja incapacitado para prestar servicio. La denegación puede conseguirse mediante la saturación o el bloqueo de las máquinas.

Directorio: Véase: Carpeta

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Dominio: Es un grupo lógico de máquinas que comparten cuentas de usuarios y seguridad de los recursos.

Empresas del grupo: Todas las unidades de negocio del Grupo ABC.

ESM: Enterprise Security Manager. Producto o software que da

soporte a la labor administrativa

FODA: Fortaleza Oportunidades Debilidades y Amenazas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: El costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidencia: Inadecuado funcionamiento detectado en los equipos, servicios y sistemas informáticos.

Incidencia Masiva: Falla que afecta a varios Clientes teniendo una misma causa.

Incidente de Seguridad: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Ingeniería social: Técnicas que intentan atacar la seguridad de los sistemas informáticos engañando a sus usuarios y administradores. La mayoría de las técnicas de ingeniería social son similares a los timos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Propiedad/característica de salvaguardar la exactitud y completitud de los activos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.

Modelo: Representación de la realidad por medio de abstracciones. Los modelos enfocan ciertas partes importantes de un sistema (por lo menos, aquella que le interesan a un tipo de modelo específico), restándole importancia a otras.

PDCA: Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), hacer (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Plataforma de Sistema: Cualquier computador de una red que pone los servicios de red, archivos, aplicación, Base de Datos a disposición de otras estaciones de la red

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Intención y dirección general expresada formalmente por la Dirección.

Problema: Cuando el estado actual del sistema no es igual al estado esperado del sistema.

Problemática: Conjunto de problemas pertenecientes a una actividad determinada, el cual es percibida a nivel gerencial.

Proveedores: Compañías que proporciona servicios de consultoría y/o software (aplicaciones) a la empresa.

Requerimiento: Pedido de algún servicio informático que se desea obtener.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Combinación de la probabilidad de un evento y sus consecuencias.

ROSI es el Retorno Sobre la Inversión de Seguridad, derivado del conocido indicador financiero ROI, Retorno Sobre la Inversión

Sarbanes-Oxley: Ley de Reforma de la Contabilidad de Compañías Públicas y Protección de los Inversores aplicada en EEUU desde 2002. Crea un consejo de supervisión independiente para supervisar

a los auditores de compañías públicas y le permite a este consejo establecer normas de contabilidad así como investigar y disciplinar a los contables. También obliga a los responsables de las empresas a garantizar la seguridad de la información financiera.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Servidor: Véase: Plataforma de Sistema

Servidor de Aplicación: Tipo de servidor que permite el procesamiento de datos de una aplicación de cliente.

Servidor de Archivos: Tipo de servidor que almacena varios tipos de archivos y los distribuye a otros clientes de la red. Ordenador conectado a la red que permite el acceso de los usuarios a una colección de ficheros en él almacenados

Servidor de base de datos: Tipo de servidor que provee servicios de base de datos a otros programas u otras computadoras.

Servidor de correo: Tipo de servidor almacena, envía, recibe, encamina y realiza operaciones relacionadas a los emails de otros clientes de la red.

Servidor de dominio administra las cuentas y recursos del dominio en cuestión, y/o servidores y /o estaciones de trabajo. Los usuarios de un mismo dominio tendrán un inicio de sesión único en el servidor del dominio para acceder a los recursos de cualquier parte de la red, una cuenta única para acceder a las máquinas del dominio.

SGSI: Sistema de Gestión de la Seguridad de la Información. Parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Tratamiento de riesgos: Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de riesgos: Proceso completo de análisis y evaluación de riesgos.

Virus: El tipo más conocido de código malicioso. Programa que se copia dentro de otros programas e intenta reproducirse el mayor número de veces posible. Aunque no siempre es así, la mayoría de las veces el virus, además de copiarse, altera o destruye la información de los sistemas en los que se ejecuta.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

W2k: Sistema Operativo Windows 2000

BIBLIOGRAFÍA

[ALSI05] ACADEMIA LATINOAMERICANA DE SEGURIDAD INFORMÁTICA. Unidad 1: Introducción a la Seguridad de la Información. Unidad 2: Concepto de Análisis de Riesgo. Microsoft Technet. 2005.

[ALSI05-2] ACADEMIA LATINOAMERICANA DE SEGURIDAD INFORMÁTICA. Christian Linacre. Módulo 1. Microsoft TechNet. 2005. Disponible en: http://www2.ing.puc.cl/~dmery/Academia%20de%20 eguridad%20Modulo%201%20PUC.ppt

[AZNZS] AS/NZS 4360:1999 Estándar Australiano: Administración de Riesgos. Segunda Edición. Australia. 2003.

[BRIN95b] BRINKLEY, Donald L. y SCHELL, Roger R. Information Security: An Integrated Collection of Essays: Essay 2 Concepts and Terminology for Computer Security. California, Estados Unidos de América. ACSAC. 995. Disponible en: http://www.acsac.org/secshelf/book001/02.pdf

[CHAR05] Charles Davis, Eric Lakin, "Hasta las pymes son hacheadas", Exposición en el congreso Internacional en Seguridad TI Informática H@cker Halted. 2005.

[GASS88] GASSER, Morrie. Building a Secure Computer System. Nueva York, Estados Unidos de América. Library of Congreso. 1988. Disponible en: http://www.acsac.org/secshelf/book002.html

[HARR03] HARRIS, Shon. CISSP Certification: All-in-one Exam Guide. Second Edition. Emerville, California, Estados Unidos de América. McGraw Hill. 2004.

[MAGE**01**] MAGERIT versión 1.0, Consejo Superior de Informática Análisis y Gestón de Riesgos. Guía de procedimientos.

[NIST95] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12. Washington, Estados Unidos de América. 1995. Disponible en: http://www.csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

[OUD05] OUD, Ernst Jan. The value to IT of using Internacional Standards. En: Information Systems Control Journal. Vol. 3. (2005); p. 35-39.

[ROBO05] Robotiker, Cristina Martínez Martínez, Forosec: Guía de Implantación de Sistemas de Gestión de la Seguridad de la Información. 2005.

[ROSI07] ROSI, Retorno sobre la inversión de Seguridad de información Definición. Septiembre de 2007. Disponible en: http://seguridad-informacion.blogspot.com/2007/09/ro_i-retorno-obre-la-inversin-de.html

[STON01] STONEBURNER, Gary. NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security. Gaithersburg, Estados Unidos de América. National Institute of Standards and Technology (NIST), 2001. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

[WILS03] WILSON, Marcia J. Calculating security ROI is tricky business. Estados Unidos de América. ComputerWorld. 2003. Disponible en: http://www.computerworld.com/securitytopics/security/story/0,10801,83207,00.html?SKC=securi ty-83207

ANEXOS

ANEXO A
Cumplimiento de buena Práctica de Control de Accesos del Servidor FacturaLima

Buena Práctica de Control de Accesos \ Servidor	FacturaLima
1. Gestión de acceso de usuarios	
1.1 Gestión de cuentas/identificadores de usuarios	
Se debe tener procedimiento de creación/eliminación/modificación de cuentas de usuarios.	SI
Cada usuario debe tener su propio y único identificador, prohibiéndose que varios usuarios lo compartan.	NO
El propietario del servicio o información debe autorizar el acceso al usuario.	SI
Eliminar las cuentas de acceso de los usuarios que y no pertenezcan a la organización (personal cesado) o retirado.	NO
Eliminar las cuentas de acceso de los usuarios que se encuentran inactivos (sin uso) hace más de 60 días.	NO
1.2 Gestión de contraseñas de usuarios	
Proporcionar inicialmente una contraseña temporal segura, que el sistema debe obligar al usuario cambiar inmediatamente después de inicio de sesión.	SI
El sistema no debe permitir asignar una contraseña menor a 6 caracteres.	NO
El sistema no debe permitir asignar una contraseña igual a las 6 últimas contraseñas.	NO
El sistema debe forzar cambiar la contraseña cada 35 días calendario.	NO
La contraseña no debe visualizarse en pantalla durante la introducción de la misma.	SI
Contraseña debe ser fácil de recordar y difícil de adivinar: contraseña no debe ser igual a Identificación del Usuario (con prefijo, sufijo), no debe ser igual a una de las palabras especificadas en un diccionario.	NO
1.3 Gestión de privilegios de usuarios	
Identificar los privilegios asociados a cada elemento del sistema. Resaltar cuentas con privilegios de administración.	NO
Asignar privilegios según "necesidad de su uso" y "caso por caso" (asignar el permiso necesario para que pueda desempeñar su labor).	NO
Se debe tener procedimiento de creación/eliminación/modificación de cuentas con privilegio administrador.	NO
1.4 Control de acceso al sistema operativo	
El sistema debe mostrar un mensaje al inicio de sesión que advierta la restricción de acceso al sistema sólo a usuarios autorizados.	SI
El sistema debe bloquear la cuenta por 5 intentos fallidos.	NO
Después de ocurrir el error en el ingreso al Sistema, la cuenta deberá permanecer inactiva por 30 minutos.	NO
Se recomienda que la opción de servicio de acceso remoto debe estar desactivada.	SI
Se debe tener actualizado los parches de sistemas operativos.	SI
Desactivar o retirar todas las facilidades basadas en software que no sean necesarios. No se debe tener servicios instalados que no han sido definidos como permisibles para el sistema.	NO
1.5 Revisión de los derechos de acceso de los usuarios	
Revisar los derechos de accesos de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses).	NO
Revisar las cuentas privilegiadas periódicamente (se recomienda cada semana).	NO
2. Responsabilidad de los usuarios	
2.1 Uso de cuentas	
Cada usuario debe ingresar con su propia "cuenta de usuario" y no debe compartirla. El usuario es responsable por todas las acciones que se realicen con su "cuenta".	NO
El usuario no debe usar cuentas especiales o aprovechar fallas en la seguridad de los sistemas, para obtener un acceso no autorizado.	SI
2.2 Uso de contraseñas	
Mantener la confidencialidad de las contraseñas. Evitar guardar registros (papel, archivos de software o dispositivos).	SI
Seleccionar contraseñas de buena calidad, con una longitud mínima caracteres que sean fáciles de recordar, no estén basas en algo que cualquiera pueda adivinar.	NO
Cambiar las contraseñas en intervalos de tiempo regulares (menor a 35 días).	NO

	2.3 Equipo informático de usuario desatendido	
	Bloquear su sesión o habilitar un protector de pantalla para evitar accesos no autorizados usando su cuenta. Desconectar (log-off) los servidores o los computadores centrales cuando se ha terminado la sesión	NO
	Al término del trabajo diario, cierra todas las sesiones y apaga tu computadora antes de retirarte de la oficina.	NO
	2.4 Uso de archivo y directorios	
	No compartir sus archivos o directorios por defecto. Este no debe quedar con acceso de control total y a su vez con permiso para todos los usuarios de la red corporativa.	SI
Nivel de seguridad (% de cumplimiento de buenas prácticas)		33.3%

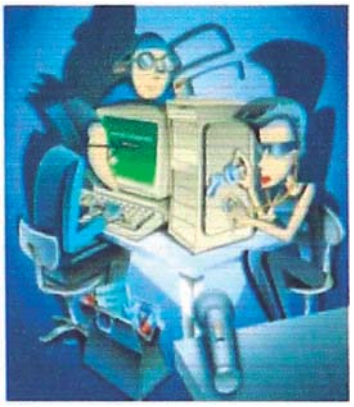
ANEXO B
Cronograma de Actividades del Proyecto

Item	Nombre de Tarea	Duración	Fecha Inicio	Fecha Fin	Predecesoras
1	**PROYECTO Mejora de Nivel de Seguridad**	**132 días**	**07/03/2006**	**06/09/2006**	
2	**PLANIFICAR**	**12 días**	**07/03/2006**	**22/03/2006**	
3	Coordinar: objetivo, miembros, alcance del proyecto	2 días	07/03/2006	08/03/2006	
4	Analizar riesgos	4 días	09/03/2006	14/03/2006	3
5	Elaborar plan de capacitación	2 días	15/03/2006	16/03/2006	4
6	Elaborar plan de actividades	2 días	17/03/2006	20/03/2006	5
7	Retorno de Inversión	2 días	21/03/2006	22/03/2006	6
8	**IMPLANTAR**	**96 días**	**23/03/2006**	**03/08/2006**	**2**
9	**Procedimientos**	**30 días**	**23/03/2006**	**03/05/2006**	
10	Revisar procedimientos existente	3 días	23/03/2006	27/03/2006	
11	Coordinar con las áreas involucradas	2 días	28/03/2006	29/03/2006	10
12	Elaborar y/o actualizar procedimientos	20 días	30/03/2006	26/04/2006	11
13	Coordinar la aprobación de procedimientos	2 días	27/04/2006	28/04/2006	12
14	Comunicar procedimientos	3 días	01/05/2006	03/05/2006	13
15	**Producto ESM**	**27 días**	**23/03/2006**	**28/04/2006**	
16	**Capacitar**	**2 días**	**23/03/2006**	**24/03/2006**	
17	Capacitar responsables/usuarios en el uso del producto	2 días	23/03/2006	24/03/2006	
18	**Instalar**	**18 días**	**27/03/2006**	**19/04/2006**	**16**
19	**Ambiente de Pruebas**	**5 días**	**27/03/2006**	**31/03/2006**	
20	Coordinar y definir servidores a instalar	1 día	27/03/2006	27/03/2006	4
21	Instalar	1 día	28/03/2006	28/03/2006	20
22	Evaluar performance	2 días	29/03/2006	30/03/2006	21
23	Elaborar informe	1 día	31/03/2006	31/03/2006	22
24	**Producción**	**13 días**	**03/04/2006**	**19/04/2006**	**19**
25	Coordinar y definir servidores a instalar	1 día	03/04/2006	03/04/2006	
26	Instalar plataformas UNIX	5 días	04/04/2006	10/04/2006	25
27	Instalar plataformas W2K	3 días	04/04/2006	06/04/2006	25
28	Instalar plataformas OPENVMS	2 días	04/04/2006	05/04/2006	25
29	Evaluar performance	3 días	11/04/2006	13/04/2006	26,27,28
30	Ejecutar revisión de accesos	2 días	14/04/2006	17/04/2006	29
31	Elaborar informe	2 días	18/04/2006	19/04/2006	30
32	**Configurar**	**7 días**	**20/04/2006**	**28/04/2006**	**18**
33	Coordinar con responsables de plataformas	2 días	20/04/2006	21/04/2006	
34	Configurar	5 días	24/04/2006	28/04/2006	33
35	**Validar y eliminar accesos**	**52 días**	**04/05/2006**	**14/07/2006**	**9,15**
36	Validar y eliminar cuentas	20 días	04/05/2006	31/05/2006	
37	Asignar contraseñas difíciles de adivinar	15 días	01/06/2006	21/06/2006	36
38	Descompartir carpetas con acceso público	5 días	22/06/2006	28/06/2006	37
39	Desinstalar softwares no autorizados	7 días	29/06/2006	07/07/2006	38
40	Actualizar parches del sistema operativo	5 días	10/07/2006	14/07/2006	39
41	Elaborar informe	2 días	04/05/2006	05/05/2006	
42	**Capacitar administradores y usuarios**	**66 días**	**04/05/2006**	**03/08/2006**	**9,15**
43	**Capacitar administradores**	**66 días**	**04/05/2006**	**03/08/2006**	
44	Capacitar	65 días	04/05/2006	02/08/2006	
45	Elaborar informe	1 día	03/08/2006	03/08/2006	44
46	**Capacitar usuarios**	**66 días**	**04/05/2006**	**03/08/2006**	
47	Charlas	64 días	04/05/2006	01/08/2006	

48	Campañas	64 días	04/05/2006	01/08/2006	
49	Elaborar informe	2 días	02/08/2006	03/08/2006	47,48
50	**REVISAR**	**9 días**	**04/08/2006**	**16/08/2006**	**8**
51	Procedimientos	2 días	04/08/2006	07/08/2006	
52	Producto ESM	1 dia	08/08/2006	08/08/2006	51
53	Configuración	1 dia	09/08/2006	09/08/2006	52
54	Validación y eliminación de accesos	3 días	10/08/2006	14/08/2006	53
55	Plan de capacitación	2 días	15/08/2006	16/08/2006	54
56	**MEJORA Y CORRECCION**	**11 días**	**17/08/2006**	**31/08/2006**	**50**
57	Coordinar y definir acciones correctivas	1 día	17/08/2006	17/08/2006	
58	Mejorar procedimientos	2 días	18/08/2006	21/08/2006	57
59	Afinar configuración	1 día	22/08/2006	22/08/2006	58
60	Mejorar plan de capacitación	2 días	23/08/2006	24/08/2006	59
61	Validar y eliminar accesos	3 días	25/08/2006	29/08/2006	60
62	Medir nivel de cumplimiento de buenas practicas	2 días	30/08/2006	31/08/2006	61
63	**CIERRE**	**4 días**	**01/09/2006**	**06/09/2006**	**56**
64	Evaluar resultados	2 días	01/09/2006	04/09/2006	
65	Elaborar informe ejecutivo, conclusiones y recomendaciones	2 días	05/09/2006	06/09/2006	64

ANEXO C
Presentación de Bloqueo de Estación de Trabajo

¿Bloqueas tu estación de Trabajo?

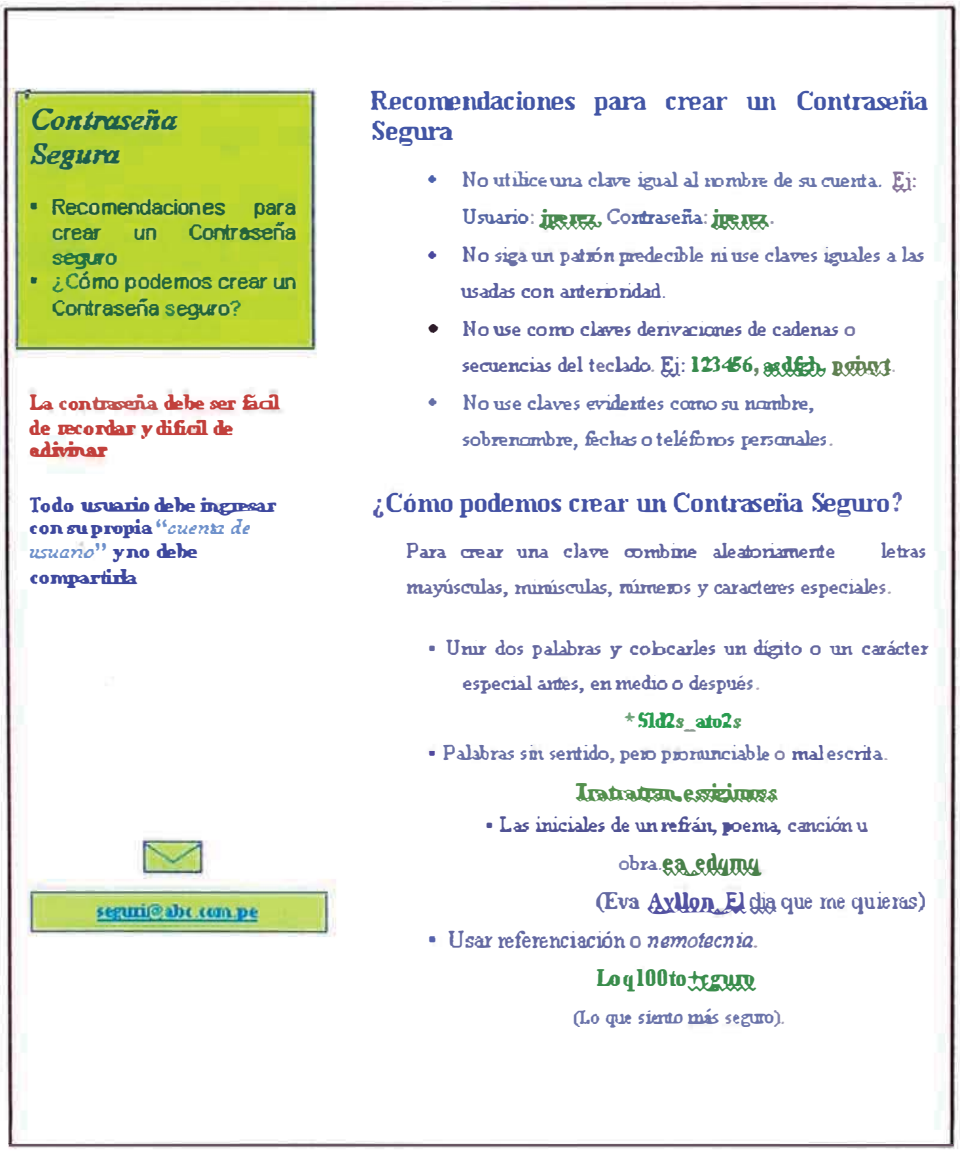


¿Por qué hacerlo?
¿Cuándo?
¿Para qué?

Debes bloquear tu estación cuando la dejes **desatendida** para **impedir el acceso de terceros** a tus archivos y datos personales, de esta manera estarás **protegiendo** la información que la **empresa te confía**.

"LA SEGURIDAD DE LA INFORMACION ES TAREA DE TODOS"

ANEXO D
Boletín de Recomendación de contraseñas



Contraseña Segura

- Recomendaciones para crear un Contraseña seguro
- ¿Cómo podemos crear un Contraseña seguro?

La contraseña debe ser fácil de recordar y difícil de edivinar

Todo usuario debe ingresar con su propia *"cuenta de usuario"* **y no debe compartirla**

seguri@abc.com.pe

Recomendaciones para crear un Contraseña Segura

- No utilice una clave igual al nombre de su cuenta. Ej: Usuario: jperez, Contraseña: jperez.
- No siga un patrón predecible ni use claves iguales a las usadas con anterioridad.
- No use como claves derivaciones de cadenas o secuencias del teclado. Ej: 123456, asdfgh, poiuyt.
- No use claves evidentes como su nombre, sobrenombre, fechas o teléfonos personales.

¿Cómo podemos crear un Contraseña Seguro?

Para crear una clave combine aleatoriamente letras mayúsculas, munúsculas, números y caracteres especiales.

- Unir dos palabras y colocarles un dígito o un carácter especial antes, en medio o después.

  *51d2s_ato2s

- Palabras sin sentido, pero pronunciable o mal escrita.

  Iratratran.esiximos

- Las iniciales de un refrán, poema, canción u obra.ea edumy

  (Eva Ayllon, El dia que me quieras)

- Usar referenciación o *nemotecnia*.

  Loq100to+seguro

  (Lo que siento más seguro).