CAPITULO III

PROPUESTA DE POLÍTICAS, ESTANDARES Y PROCEDIMIENTOS DE SEGURIDAD PARA LA EMPRESA ANDINATEL S.A.

Con esta propuesta de políticas, estándares y procedimientos de seguridad para la Empresa de Telecomunicaciones ANDINATEL S.A. se pueden alcanzar medidas de seguridad, reduciendo así el acceso a información sensitiva o privilegiada acerca de los datos, procesos de negocio, personal o infraestructura. Necesaria para minimizar los peores escenarios posibles que implican grandes pérdidas en la compañía.

3.1 OBJETIVOS DE LA PROPUESTA.

OBJETIVO GENERAL.

- Normar, estandarizar y establecer políticas de seguridad, en lo referente a hardware, software, infraestructura, personal, niveles de acceso y procedimientos en la Red Corporativa de Datos de ANDINATEL S.A.

OBJETIVOS ESPECÍFICOS.

- Proteger y proceder a una previsión de ataques con un conjunto de pasos que ayudara a reducir al mínimo la cantidad de puntos vulnerables existentes.
- Determinar responsabilidades a los encargados de los servicios y recursos informáticos del Área de Tecnología de la Vicepresidencia de Sistemas de ANDINATEL S.A..
- Brindar una estructura estable sujeta a cambios organizacionales revelantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

3.2 OBSERVACIONES Y RECOMENDACIONES TÉCNICAS EN LA ORGANIZACIÓN.

Concluida la etapa de inspección física de los componentes de infraestructura y detección de vulnerabilidades mediante la utilización de software de escaneo, se presenta a continuación observaciones y recomendaciones complementarias.

Las recomendaciones a continuación se dan de manera independiente de marcas de fabricantes, proveedores y productos específicos.

Constituyen únicamente un aporte en el proceso de selección a realizar por ANDINATEL S.A., considerando que el seguimiento a estas sugerencias disminuirá el tiempo de identificación de productos, desarrollo de laboratorios de pruebas, calificación de fabricantes, dado que se considera son la buena alternativa para ANDINATEL S.A.

3.2.1 CENTRO DE COMPUTO.

3.2.1.1 Re-ordenamiento de sistemas de cableado (eléctrico, voz, datos, video seguridad, y otros). No se cuenta con una documentación técnica apropiada, completa y actualizada. Se han realizado trabajos parciales, contratados para solucionar problemas puntuales. A la fecha, varios continúan pendientes de contratación y realización.

Recomendaciones

- Es necesario contratar el desarrollo de planos eléctricos de redes de alta tensión y de las de distribución (Centro de Cómputo,

edificios en Quito y oficinas a nivel nacional). El trabajo debe actualizarse a medida que se realicen cambios en los sitios indicados. Con especial énfasis en la alimentación de energía para equipos de computación.

- Definir a la brevedad posible las directrices que se deben seguir para la realización de los trabajos eléctricos en las nuevas instalaciones y en las adecuaciones a las ya existentes; en estas se deben especificar las normas y estándares de referencia, marca y características de materiales a utilizar, criterios de pruebas y aceptación, contenido de las documentaciones tanto gráfica, como texto, formato de recepción y responsable de las actualizaciones.
- Mejoras para evitar daños por presencia de roedores que ingresan desde el exterior, dado que hay acceso próximo a la planta baja desde cañerías externas de desagüe y alcantarillas. Pueden ocasionar problemas por mordida de cables, además de los relacionados con ataques a personas. Se debe como mínimo fumigar e instalar trampas para roedores bajo el piso falso, complementada con la instalación de equipos para ahuyentar estos animales por la emisión de sonidos a frecuencias pre-determinadas.

- No se debería dar como terminado y aceptado por parte de ANDINATEL S. A., ningún trabajo que no cumpla con las directrices y estándares de seguridad. Por otro lado también se debería revisar detalladamente en el área del Centro de Informática los contenidos y rutas de las canaletas del sistema eléctrico, para garantizar que no sean utilizadas para la transportación de otros tipos de cables. Además, todas las canaletas y tuberías que se utilicen, deben estar pintadas y marcadas exteriormente, de acuerdo a los colores que dictan las normas internacionales respectivas (por ejemplo: naranja para datos, azul para eléctrico, etc.).

3.2.1.2 Referente a los UPS, aire acondicionado, sistemas contra incendios y de control de acceso y seguridad.

Recomendación

- Comprobar los procedimientos de verificación y comprobación de dichos equipos, así como los cambios y ajustes realizados.
- Incorporar herramientas de administración y monitoreo para los UPS, en lo que corresponde a facilidades pro-activas para predecir la posibilidad de fallas, carga soportada versus esperada.

3.2.1.3 ANDINATEL S.A. a normalizado una sola marca de servidores, utilizan equipos marca IBM (aunque aun existen equipos Compaq, varios modelos y configuraciones).

Recomendación

- Estandarizar servidores con procesadores: RISC (RS/6000) y CISC (Intel). Todos los nuevos equipos son marca IBM y del tipo apilable en gabinete (también llamado; rackable). Ahorro de espacio, mejor ordenamiento, facilidad de crecimiento, relación con proveedor de nivel mundial con alto nivel de soporte local. Mejoras en las condiciones de negociación.

3.2.1.4 En su distribución, no existe una sectorización de manera que las personas que requieran trabajar en su interior, no tengan facilidades de acceso a equipos restringidos de las áreas periféricas.

Recomendación

- Utilizar divisiones interiores restringidas por puertas de acceso.

3.2.2 CABLEADO DE DATOS.

3.2.2.1 A la fecha la instalación de nuevos puntos, se realiza respetando las normas EIA/TIA 568 y 569. Además se etiquetan e identifican estos puntos, finalmente, se certifican con equipo electrónico apropiado.

Recomendaciones

- Realizar la documentación integral y detallada de las rutas de transportación, tanto del back-bone como de distribución (planos y diagramas). Completando con el pintado e identificación de canaletas y tuberías de distribución de acuerdo a los estándares establecidos. Con una adecuada planificación se podría determinar una meta a 1 ó 2 años para cumplir con esta recomendación.
- Enviar a cursos de certificación al personal interno asignado a las tareas de instalación de puntos de cableado estructurado. Actualmente estas tareas se realizan utilizando buenos materiales pero malas prácticas. No están adecuadamente identificados a ambos extremos, ni su transportación en medios seguros (claramente identificados) y con aislamiento eléctrico.

- Es importante expresar, que la instalación de cualquier sistema de cableado (eléctrico, voz, datos, seguridad, entre otros), debe ser planificado para períodos no menores de 10 años, dado que su instalación es una tarea que demanda muchos recursos técnicos y económicos y que son difícil de cambiar ó modificar

3.2.2.2 Certificar todos los puntos de datos, con una planificación de 1 a 2 años, para corregir errores o para validar buenos trabajos.

Recomendación

- Esto debe hacerse extensivo a los tramos en que se utiliza Fibra Óptica.

3.2.3 REDES

3.2.3.1 Estandarizar en todos los dispositivos CISCO, el nombre de la comunidad SNMP (Simple Network Management Protocol), cambiando el de omisión **public** por uno con longitud y nivel de complejidad apropiado (es una conocida vulnerabilidad, protocolo SNMP con comunidad de omisión).

Recomendación

- A futuro, de ser necesario se lo puede subir a este servicio, pero con las consideraciones de seguridad ya tomadas para el caso de los dispositivos Cisco.

3.2.3.2 Optimización de uso de los canales de dstribución (red amplia), en este punto se han aumentado la capacidad de los enlaces con los sitios remotos (tanto en la ciudad de Quito, como en las ciudades que tiene cobertura). La mayoría de estos enlaces son de orden de 2 Kbps. Mejorando significativamente los tiempos de respuesta de las aplicaciones y servicios informáticos.

Recomendación

- Adquirir un equipo especializado para establecer prioridades de tráfico en los enlaces, de esta manera se podrán mantener excelentes tiempos de respuesta en las aplicaciones y restringir/controlar el uso del canal por aplicaciones no sensibles al tiempo (por ejemplo: Correo electrónico). Seria aconsejable que este equipo tenga potencialidad de compresión de datos. Una

opción son los fabricados por Packerteer. Esta consideración también podría utilizarse para el enlace a Internet.

3.2.3.3 Para etiquetar de una manera visible, codificada y unificada, cada dispositivo de red, es posible utilizar un código como continuación se recomienda.

Recomendación.

- Es posible utilizar un código como por ejemplo:

3CSWDORUIO001095

Donde:

3C → Fabricante (3C = 3Com, CS = Cisco, AS = Asante, HP = Hewlett Packard, ...)

SW → Tipo equipos (SW = Switch, HB = Hub no adm, HM = Hub administrable,...)

DOR → Edificio (DOR = Edif. Doral, TEC= Edif. Tecnología, ADM= Edif. Administrativo,....)

UIO → Ciudad (UIO = Quito, GYE = Guayaquil, etc....)

001 → Dirección IP (3er octeto)

095 → Dirección IP (4to octeto)

Es decir, el equipo del ejemplo, es marca 3Com, switch, está ubicado en el edificio Doral, de la ciudad de Quito, y su dirección IP es 172.17.1.95.

3.2.3.4 La configuración de la comunidad SNMP seleccionada, debe ser solo de lectura (Read only). Definiendo una dirección de equipo de administración (o consola).

Recomendación.

- Para de esta manera lograr que los equipos administrados solo respondan a los requerimientos de su comunidad y a las direcciones definidas. Los equipos que tienen conexión hacia el exterior (firewall, router externo y servidores), no deben tener habilitado el servicio SNMP.

3.2.4 SERVIDORES.

3.2.4.1 Servidores IBM RS/6000, la versión del sistema operativo AIX en producción es la v. 4.3.3, porque no es soportada por IBM desde el 31 de Diciembre de 2003. Esto ocasiona que no se tengan desarrollos y mejoras sobre este producto.

Recomendaciones

- Debe desarrollarse un plan de migración a la versión AIX 5.x relacionado con la también necesaria migración de la base de datos Oracle 8i Versión 8.1.7.4.0 a la Oracle 9+. El tema de la migración de las versiones de ambos productos es un tema muy delicado, pero que debe desarrollarse a la brevedad posible, de lo contrario la brecha tecnológica será mucho mayor.
- En los servidores IBM RS/6000 que ejecutan el sistema operativo IBM AIX configurar el servicio SNMP para que no utilice el nombre de comunidad por omisión (public), sujeta ataques desde la red, que a través de la cual podrían obtener datos de la configuración y características internas de los servidores y posteriormente llegar a una escala contra la seguridad.

3.2.4.2 Servidores basados en Intel, realizar la instalación de todos los parches que faltan (seguridad, mejoras y solución de problemas) que Microsoft ha liberado (trabajos manuales de distribución e instalación; no se tiene una herramienta automatizada para el efecto).

Recomendacione s

- Eliminar los programas no utilizados o viablemente peligrosos, detener (STOP), los servicios instalados por omisión y potencialmente utilizados para ataques contra estos equipos. Los administradores de estos equipos, deben ser instruidos de la metodología a seguir para la aplicación de estos parches.
- Servidores basados en Intel, detener y bajar los servicios del sistema operativo Alerter, Messenger, Remote Registry, Remote Registry, entre otros. Servicios levantados innecesariamente, ocasionan consumo de valiosos recursos del sistema, así como, riesgos de seguridad contra la estabilidad del equipo, facilidad para acceso remoto no autorizado a los archivos de configuración de los servidores motivo suficiente para que estos deban ser deshabilitados o eliminados.
- Que estos potencialmente pueden ser utilizados para un ataque basado en ingeniería social.

3.2.4.3 La instalación del sistema operativo en servidores de misión critica, se lo realiza siguiendo las instrucciones del CD de carga del programa.

Recomendación.

- Complementar dichas instalaciones con una optimización y monitoreo constantes de las variables de eficiencia del equipo, debido a que no es posible dejar abiertas puertas de seguridad o servicios vulnerables.

3.2.4.4 Banners (Letreros), los banners que se despliegan cuando se da una conexión a ese puerto (servicio), publican la información de servicios y versiones de los mismos.

Recomendación

- Modificar la configuración de los servidores de manera que no publiquen la información de servicios y versiones, que el equipo esta ejecutando. Esto dificulta las tareas de exploración NO autorizadas. Los cambios deben ser realizados en los archivos de configuración de cada servicio.

3.2.4.5 Analizar los numerosos puertos, TCP y UDP, que están disponibles en los servidores.

Recomendación.

- Eliminar los puertos no necesarios, para evitar malos funcionamientos ó potenciales fallas de seguridad.

3.2.5 ESTACIONES DE TRABAJO.

3.2.5.1 Estaciones de trabajo, no se han instalado las ultimas versiones de programas que se utilizan en las estaciones de trabajo, como por ejemplo: Adobe Reader v6.0.1+, WinZip, y otros que controlan vulnerabilidades de dichos programas. Tampoco se han instalado los parches en los programas Microsoft como Office, Visio, Project y otros. Estos programas presentan vulnerabilidades que pueden ser explotadas.

Recomendaciones

- La solución es instalar todos los parches indicados, y realizar una revisión periódica (por ejemplo: 1 vez al mes), buscando nuevas versiones de parches y paquetes de servicio (SP Service Packs).
- Con lo referente al proceso de actualización de parches para el programa MS-Office 97/2000/2002 se hará uso de la opción

Office Update, que se presentara interactivamente, y en forma personalizada (individualizada por cada equipo), revisara automáticamente los parches instalados y notificara los que faltan, este trabajo indicado debe realizarse mensualmente en cada equipo, de lo contrario la red no estará protegida de la explotación de vulnerabilidades de programas que son reportadas mundialmente a pesar de que se tengan seguridades perimetrales como el firewall y locales como antivirus.

- Se sugiere que ANDINATEL S.A., adquiera una aplicación automatizada para el control y distribución de parches de programa dado la gran cantidad de horas/hombre necesarias para realizar estos trabajos repetitivos de forma manual. Debe incluir capacidades para generación de reportes, bitácoras de eventos, controles por nivel de usuario/supervisor. Una opción de programas es Novell ZenWoks, otra la suite de productos de Altiris. Ambos programas incluyen otras opciones como: inventario automático de equipos y programas, control remoto de estaciones para tareas de soporte a usuario, y un esquema de apoyo para la administración de estaciones y perfiles de usuarios. ANDINATEL S.A., debe decidir cual es el apropiado para sus necesidades.

3.2.6 SEGURIDAD PERIMETRAL.

3.2.6.1 Seguridad perimetral (hacia Internet); a la fecha se encuentran instalados todos los parches (seguridad, mejoras y solución de problemas) del firewall que CheckPoint ha liberado. El firewall tiene definido un conjunto de reglas que administran el entorno, son apropiadas y constantemente revisadas por su Administrador.

Recomendaciones

- Se debe contar con un esquema de Alta Disponibilidad, en el que exista por lo menos 2 firewall funcionando simultáneamente, de manera que si uno de estos cae el otro continuara funcionando. Además, es posible utilizarlos para balanceo de carga, función muy importante en especial para ambientes transaccionales en Internet y servidores de correo electrónico con altas cargas de trabajo. Si no es posible tener esta opción de respaldo y contingencia en línea, es necesario desarrollar un esquema de protección manual, por medio de un equipo secundario configurado como el primario, esperando en sitio de forma que si

falla el principal manualmente se cambia de equipos y continua la operación.

- Es necesario desarrollar una capacitación orientada a una conciencia de seguridad informática en caso de un incidente de seguridad en la conexión Internet. Además de potenciar el alcance que un evento de este tipo tendría contra la imagen de ANDINATEL S.A..

3.2.6.2 Seguridad perimetral (red interna), existen rangos de dirección IP asignados por localidad con la finalidad de identificar origen/destino de tráficos.

Recomendación

- Se recomienda analizar un proyecto de rediseño (redistribución) de los rangos de las direcciones IP utilizados. Actualmente existen rangos muy amplios con desperdicio de manejo.

3.2.6.3 Seguridad perimetral (red interna), usuarios no autorizado podría realizar exploraciones (scanning) maliciosas a los servidores y dispositivos de red ubicados en el edificio de tecnología (donde

funciona la Vice-presidencia de Informática), en donde residen los servidores del negocio.

Recomendación

- Para evitarlo, se puede incorporar un firewall entre la red del Centro de Cómputo y los usuarios de la red local del edificio, así como con los usuarios remotos. Filtrando puertos, limitando exploraciones, generando registros en las bitácoras para identificar origen de este tipo de acciones.

3.2.6.4 Seguridad perimetral (red interna), aunque los atacantes no puedan tener acceso a los datos de los clientes, podrían sacar de servicio a un servidor, con técnicas tan simples como asignar la dirección IP del equipo que se desea atacar a otra computadora del mismo rango IP, obteniendo lo buscado por DIRECCION IP DUPLICADA.

Recomendación

- Desarrollar esquemas de seguridad que eviten ataques que podrían sacar de servicio por un tiempo a los servidores

principales del negocio, debido a que los daños podrían ser mayores si se duplica la dirección IP del Gateway principal de la red.

3.2.6.5 Seguridad perimetral (red interna), complementando el punto anterior es la segmentación de la red local (incluso por medio de redes virtuales - VLAN).

Recomendación

- Para esto se deben realizar trabajos de configuración en los equipos Cisco (centrales y de distribución).

3.2.6.6 Detector de intrusos (IDS), es el de identificar y bloquear intentos de ataques desde Internet a los servidores.

Recomendación

- Implementar una aplicación que trabaje en conjunto con el ferewall y otros productos de protección perimetral, como recomendación ISS Real Source.

3.2.6.7 Seguridad acceso remoto (dial-up), fueron encontrados instalados MODEM en equipos en la red local, estos equipos rompen el control perimetral ejercido por el firewall. Como estos usuarios se conectan por la tarjeta de red que representan un MODEM (incluso con dirección IP propia) estos controles son pasados.

Recomendaciones

- Remover los modem`s instalados en la red e implementar salidas a través de RAS (Remote Access Server) con las seguridades correspondientes (por ejemplo, un control bajo una aplicación por medio del protocolo Radius). En los casos en que no se pueda implementar esta medida, configurar sin directorios compartidos, parches instalados y de ser posible activar un firewall personal (incluido en MS-windows XP).

3.2.7 CUENTAS DOMINIO DE RED.

3.2.7.1 Cuentas dominio de red, de la depuración de cuentas, a partir del informe generado, el Administrador de la red, comprobó que existían cuentas que estaban creadas y que nunca habían sido

utilizadas. Se solicito a Recursos Humanos un listado de los empleados de ANDINATEL S.A. (contratación directa o por medio de tercerizadora), no se recibió esta información.

Recomendaciones

- Se recomienda bloquear estas cuentas por un tiempo determinado, después preceder a eliminarlas. Activar bloqueos de cuentas después de 3 intentos errados para identificarse.

3.2.7.2 Cuentas dominio de red, se establecen los motivos por las cuales las cuentas no han sido depuradas:

- Cuentas de usuarios que ya no trabajan en la empresa.
- Cuentas de usuarios que se encuentran con permiso y no están asistiendo a laborar.
- Cuentas de usuarios que no utilizan su propia identificación para acceso a la red, es decir utilizan cuentas genéricas o de otros usuarios autorizados.
- Cuentas de usuarios que ya terminaron los trabajos temporales para los cuales fueron contratados.

- Cuentas con formatos antiguos, que no han sido eliminadas después que fueron normalizadas el estándar en uso.
- Cuentas de prueba y temporales que no fueron depuradas a tiempo.

Recomendación

- Insistir en la utilización de mecanismos formales a través de los cuales Recursos Humanos solicite la alta/baja de una cuenta por ingreso/salida de empleados. De lo contrario, a mediano plazo se perderá el trabajo de depuración realizado en cuentas para acceso a los recursos informáticos de ANDINATEL S.A.
- Adicionalmente, es necesario insistir con las personas autorizadas para solicitar cuentas para el personal a su cargo, que se deben crear estas cuentas, solo si es estrictamente necesario que se lo haga.
- En el caso que las personas aún laborarán en ANDINATEL S.A. y no ha utilizado la cuenta que fue creada para su uso, evaluar si es necesario que tengan cuenta, en caso contrario proceder a eliminarlas.
- Para las cuentas creadas en trabajos temporales o terceros, investigar si no son necesarias y eliminarlas.

3.2.8 SEGURIDAD CONEXIONES CON TERCEROS.

3.2.8.1 Seguridades conexiones con terceros, se tiene implementados mecanismos de seguridad en varias de las conexiones con terceros (Ejemplo: bancos, servipagos, etc.).

Recomendación

- Aumentar las seguridades en los canales de la conexión, incluyendo otros mecanismos para preservar la confidencialidad de la información transmitida. A la fecha, la transferencia de archivos se realiza a través de niveles bajo de identificación y control de integridad. Se recomienda utilizar FTP sobre SSH/SSL. Otro cambio es utilizar telnet (información viaja en forma de texto, que es expuesto), cambiándolo a SSH. Complementario a la incorporación de otros puntos del firewall para estos sitios externos.

3.2.9 BASE DE DATOS.

3.2.9.1 Base de Datos (MS SQL Server), se han presentado los siguientes problemas: inicialmente se tenía el usuario sa (System Administrator) sin clave, y claves levantadas por defecto, problema

de seguridad en el puerto 1433, en los servidores que se ejecuta SQL Server, aún aparecen mensajes que no están instalados los Service Pack (SP) correspondientes. El probable origen de esta situación, es que se aplicaron parches sin seguir la secuencia sugerida por el fabricante SP1,SP2,SP3, SP4...

Recomendaciones

- Cerrar estas vulnerabilidades existentes en servidores que ejecutan este producto, cambiar todas las claves por defecto, modificar los casos en que usuario y clave eran iguales.
- Cambiar el puerto 1433 utilizado por omisión por MS SQL Server. Esto se debe a que ciertos virus en el ambiente MS-Windows (como el SQL Worm), exploran la red buscando dicho puerto para tratar de alcanzar control sobre la BD.
- Seguir esta secuencia de Service Pack como sus fabricantes lo demandan, esto es, en orden ascendente: SP1, SP2, SP3 y SP4.
- Instalar los últimos parches disponibles para mejorar el ambiente (eficiencia, estabilidad y seguridad) de las BD MS SQL Server.

3.2.9.2 Base de Datos (Oracle), cambiar las claves de usuarios de cuentas (ampliamente conocida por la comunidad hacker), del

sistema que estaban aun con el conjunto usuario/clave, que se instala por omisión ("default"), utilizando esta cuentas un usuario no autorizado podría ganar derechos en el sistema y tener acceso. Así como también sus roles, permisos y usuarios.

Recomendaciones

- Activar bloqueos de cuentas después de tres intentos errados para identificarse.
- Modificar el parámetro OS_REMOTE-OS-ROLE a FALSE, lo cual impide que la base de datos confié en el sistema operativo para autentificar roles. Su seguridad se suma a la seguridad autónoma del sistema operativo (IBM AIX).
- Depurar los roles y usuarios que tienen altos privilegios (SUPER PRIVILEGIOS), y modificar todos aquellos que tengan la opción Admin_Option TRUE a FALSE, para que no puedan heredar sus privilegios a terceros.
- Implementar una aplicación que revise e identifique las potenciales vulnerabilidades en la base de datos Oracle. Esto aumentara el nivel de seguridad de los datos de las aplicaciones del negocio. Para el efecto se sugiere AppDetective for Oracle.

Base de Datos (TODAS)

Para el mantenimiento de las pistas de auditoria correspondientes, además de guardar versiones sucesivas de estas y que las mismas estén claramente identificadas.

Recomendaciones

- Incluir procedimientos de auditoría (basados en triggers) para control de excepción sobre procesos de la base de datos, considerando que esto es una alternativa más viable que levantar las opciones de auditoría en la misma, por la penalización a los tiempos de respuesta que estos ocasiona.
- Continuar con la depuración de roles, permisos y usuarios en las aplicaciones desarrolladas en ANDINATEL S.A..

3.2.10 IMPLEMENTACION DE UN DIRECTORIO UNIFICADO.

3.2.10.1 Implementación de un directorio unificado, a la fecha se tienen grupos de recursos, como por ejemplo: Microsoft Active Directory, que utilizan el directorio LDAP pero enfocado principalmente a los servicios Microsoft Windows. Pero aislados a

los recursos de los servidores IBM RS/6000, base de datos Oracle 8, y las aplicaciones del negocio, no se tiene un Metadirectorio que unifique los directorios, siguiendo el estándar LDAP v3.+.

Un directorio es un mecanismo distribuido de almacenamiento y recuperación de la información. Tiene algunas de las características de una base de datos, un sistema de procesamiento transaccional y un sistema de archivos. Un directorio es un lugar en el cual se administra información de manera que los sistemas operativos múltiples o múltiples instancias de un sistema operativo, puedan usarlo.

Los directorios pueden contener casi de todo: descripciones de personas y sus direcciones electrónicas (e-mail), ubicaciones de servicios vitales en la red, datos de configuración, datos definidos por el usuario y más.

El protocolo de acceso a direcciones livianos LDAP (Lightweight Directory Access Protocol) es un estándar que permite el acceso a los servicios de directorio, multiplataforma, actualmente en su versión 3.0. Este protocolo y su API han sido implementados en una amplia gama de directorios y otros productos. Sobre esta base se

puede pasar a otros proyectos como: seguridad unificada (SSO – Single Sign On), autentificación y encriptación.

3.2.11 CONTROL DE BITÁCORAS

Para una recuperación ante incidentes de seguridad, detecciones de comportamiento inusual, resolver problemas, evidencia legal e información acerca de eventos relacionados en los sistemas y centro de computo.

Recomendación

- Implementar una aplicación para análisis de eventos registrados en las bitácoras de sistema operativo, base de datos, firewall, acceso a servidores, etc. Es necesario, revisar por excepción de la red y sus servicios, para tomar medidas defensivas a la seguridad informática de recursos.

3.2.12 IMPRESORAS DE RED.

Por el hecho de estar conectadas en red, pues estas aceptaran comandos, además pocos técnicos controlan el tráfico de las impresoras, pudiendo ser estas utilizadas, como puente hacia la zona interna de la empresa.

Recomendaciones

- Actualizar el firmware a la última versión disponible.
- Levantar claves para acceso a los menús de configuración de opciones (protección contra intrusos).

3.3 RECOMENDACIONES FINALES.

3.3.1 CENTRO DE COMPUTO:

Considerar en el diseño de su distribución y de sus áreas aledañas, las recomendaciones del Comité ANSI/EIA/TIA-942 (actualmente en estado de Borrador de Discusión), que consideran los estándares para la construcción de Centros de Datos (por ejemplo: la ubicación de los racks y gabinetes, para crear corredores de aire fríos y calientes. Para el ruteo de cables de señal y de alimentación eléctrica, respectivamente). El estándar comprende más que la infraestructura de comunicaciones. Más de la mitad de la norma trata de las especificaciones de construcción. Se espera su aprobación a mediados del año 2004.

3.3.2 EQUIPO MEDICIÓN / CERTIFICACIÓN CABLEADO:

Actualizar el equipo existente (de ser posible o en su defecto adquirir uno nuevo), para certificaciones EIA/TIA 568 B1-2.1, Categoría 6 y que pueda actualizarse a futuro (por medio de software). Se sugiere Fluke DSP-4300 o superior, incluir medios UTP y Fibra Óptica (Multimodo).

3.3.3 PROGRAMA DE MONITOREO DE NIVELES DE SERVICIO (SLA):

Incorporar una aplicación automatizada para control de niveles de servicio y de servicio de servidores y equipos de red. Es necesario generar estadísticas de tiempos de respuesta, porcentajes de carga sobre servidores, memoria RAM, disco duros y otros indicadores de eficiencia necesaria para desarrollar Planificación de Capacidad (Capacity Planning).

Sobre esta base se puede decidir sobre potenciales crecimientos de configuraciones y cambios/adquisiciones/mejoras en equipos. Una alternativa inicial es utilizar un programa Open Source llamado JFF NMS **(**http://jffnms.sourceforge.net/**)**, que utiliza una Base de Datos

para almacenar las estadísticas obtenidas (instalación de bajo costo, debido a que es un producto de libre distribución). Se Sugiere instalarlo sobre un servidor que ejecute el sistema operativo Linux (preferible Red Hat ó SUSE). A futuro se puede tener varios equipos con funciones especializadas, por ejemplo: una para los servidores red LAN, otro para equipos red WAN y otro para las instancias de Base de Datos.

Para su instalación debe activarse y configurarse con el nombre comunidad SNMP que utiliza ANDINATEL S.A. a partir de esta experiencia se podría evaluar la posibilidad de adquirir una aplicación para estos trabajos.

3.3.4 PROCESOS CONTINUOS DE INSTALACIÓN DE PARCHES

Es imprescindible que se mantengan estos procesos para mantener los niveles de seguridad actuales, y a futuro aumentarlos. De lo contrario, la posición de seguridad se perdería siendo vulnerables a todo tipo de riesgos informáticos.

Se Recomienda que los ejecutivos tecnológicos de alto nivel apoyen estas medidas.

3.3.5 SEGURIDAD PERIMETRAL (HACIA INTERNET):

Certificar a los técnicos encargados de Administración del Firewall, por medio de cursos y los respectivos exámenes. Consideremos que es crítico para la seguridad informática de ANDINATEL S.A. que sus técnicos estén capacitados para diseñar, administrar y operar, soluciones de seguridad sobre el Firewall. Los cursos deben ser dictados en centro de capacitación autorizados por el fabricante.

3.3.6 BASE DE DATOS:

Realizar revisiones técnicas de manera periódica por medio de terceros especializados, para identificar potenciales puntos de ruptura de seguridad, depuración de usuarios y optimización de la configuración de los ambientes, dado que son dinámicos. De lo contrario no se podría garantizar que el trabajo realizado haya tenido la continuidad apropiada.

También se debería incorporarse una herramienta que permita controlar los cambios a las versiones de programas, además de guardar las versiones sucesivas de estas. Es necesario que los cambios sean claramente identificados antes de ser pasados a producción, mantenie ndo las pistas de auditoría correspondientes.

3.3.7 CAPACITACIÓN:

Comunicar a los usuarios sus responsabilidades sobre la utilización de cuenta y clave, para el acceso a los servicios y aplicaciones. Hacer énfasis en las medidas por mal uso de las mismas.

Se deberá certificar a los técnicos asignados a manejo de productos utilizados como estándar en ANDINATEL S.A, como los fabricados por Microsoft, IBM y Cisco, por medio de cursos dictados por el fabricante. Esto mejoraría la capacidad interna en respuesta a necesidades de soporte técnico.

Por último, insistir con los usuarios sobre el tema de compartir directorios, especialmente en los que no tienen clave. Esta práctica es un potencial punto de ruptura de las seguridades perimetrales. Además de la posibilidad de obtener datos reservados del negocio como personales.

Durante el desarrollo de la identificación de vulnerabilidades, se realizo pruebas de exploración de directorios compartidos, pudiendo obtener fácilmente información técnica, comercial y financiera de ANDINATEL S.A.

3.3.8 PERSONAL:

Existen empleados contratados por medio de una empresa tercerizadora, que son responsables de procesos críticos en las áreas de informática de ANDINATEL S.A., están capacitados y tienen un buen nivel de experiencia técnica, pero que podrían ser despedidos por motivos administrativos, sin considerar lo indicado. Se sugiere identificarlos y evaluar su contratación y vinculación directa a ANDINATEL S.A.

Definir la función de un jefe de seguridad informática (CSO – Chief Security Oficcer), responsable de todos los aspectos técnicos de la seguridad de ANDINATEL S.A. Se recomienda a la brevedad posible se implemente el rol de CSO; con un nivel ejecutivo alto sobre los responsables técnicos de las áreas informáticas.

3.4 ESTANDARES Y NORMAS PARA LA ADQUISICIÓN O IMPLEMENTACION DE EQUIPOS EN LA ORGANIZACIÓN.

3.4.1 NORMAS Y ESTANDARES PARA EL CABLEADO ESTRUCTURADO.

Para permitir una administración sencilla y sistemática de las mudanzas y cambios de ubicación de personas y equipos. Tales como el sistema

de cableado de telecomunicaciones para edificios que presentan como característica saliente de ser general, el soportar una amplia gama de productos de telecomunicaciones, como es el caso de la empresa ANDINATEL S.A.

Estas normas garantizan que los sistemas que se ejecuten de acuerdo a ella soportarán todas las aplicaciones de telecomunicaciones presentes y futuras por un lapso de al menos 10 años. Esta afirmación puede parecer excesiva, pero si se tiene en cuenta que entre los autores de la norma están precisamente los fabricantes de estas aplicaciones.

1. ANSI/TIA/EIA-568-A_Commercial Building Telecommunications Cabling Standard (October 1995). "Norma para la construcción comercial de cableado de telecomunicaciones".

   Esta norma fue desarrollada y aprobada por comités del Instituto Nacional Americano de Normas (ANSI) Asociación de Industria de Telecomunicaciones (TIA), y la Asociación de la Industria Electrónica, (EIA).

   La norma establece criterios técnicos y de rendimiento para diversos componentes y configuraciones de sistemas. Además, hay un número de normas relacionadas que deben seguirse con apego.

Consiste en 7 subsistemas funcionales:

a.) Instalación de entrada, o acometida, el punto donde la instalación exterior y dispositivos asociados entran al edificio. Este punto puede estar utilizado por servicios de redes públicas, redes privadas del cliente, o ambas; están ubicados los dispositivos de protección para sobrecargas de voltaje.

b.) Sala de máquinas o equipos, un espacio centralizado para el equipo de telecomunicaciones que da servicio a los usuarios en el edificio

c.) El eje de cableado central, proporciona interconexión entre los gabinetes de telecomunicaciones Consiste de cables centrales, interconexiones principales e intermedias, terminaciones mecánicas, y puentes de interconexión.

d.) Gabinete de telecomunicaciones, es donde terminan en sus conectores compatibles, los cables de distribución horizontal.

e.) El cableado horizontal consiste en el medio físico usado para conectar cada toma o salida a un gabinete. Se pueden usar varios tipos de cable para la distribución horizontal.

f.) El área de trabajo, sus componentes llevan las telecomunicaciones desde la unión de la toma o salida y su conector donde termina el sistema de cableado horizontal, al equipo o estación de trabajo del usuario.

g.) Cableado de backbone, el propósito es proveer interconexión entre edificio sala de equipo y closet de telecomunicaciones y además incluye los medios de transmisión, intermediario y terminaciones mecánica, utiliza una estructura convencional tipo estrella.

2. ANSI/EIA/TIA-569_Commercial Building Standards for Telecommunications Pathways and Spaces (October 1990). Norma de construcción para vías y espacios de telecomunicaciones.

El contenido de esta norma, incluye y proporciona estándares para conformar ubicaciones, conductos, áreas, pasos y espacios

necesarios a través de las cuales se instalan los equipos y sistemas estandarizados de telecomunicaciones.

3. ANSI/EIA/TIA-570_Residential and Light Commercial Telecommunications Wiring Standard (June 1991). Norma para la instalación de Sistemas de Telecomunicaciones en áreas residenciales y comerciales de baja densidad.

   En este estándar están los requerimientos para tecnología existente y tecnología emergente. Especificaciones de cableado para voz, video, datos, automatización del hogar, multimedia, seguridad y audio están disponibles en este estándar. Este estándar es para nuevas construcciones, adiciones y remodelamientos en edificios residenciales.

4. ANSI/TIA/EIA-606_The Administration Standard for the Telecommunications Infrastructure of Commercial building (February 1993). Norma de administración para la infraestructura de telecomunicaciones en edificios comerciales.

   Proporciona normas para la codificación de colores, etiquetado, y documentación de un sistema de cableado instalado. Seguir esta

norma, permite una mejor administración de una red, creando un método de seguimiento de los traslados, cambios y adiciones. Facilita además la localización de fallas, detallando cada cable tendido por características.

5. ANSI/TIA/EIA-607_Commercial Building Grounding and Bonding Requirements for Telecommunications (August 1994). Requisitos de aterrizado y protección para telecomunicaciones en edificios comerciales.

   Regula las especificaciones para instalar sistemas de aterrizado que aseguren un nivel confiable de referencia a tierra eléctrica, para todos los equipos.

6. TIA/EIA TSB-67_Transmission Performance Specifications for Field Testing of Unshielded Twisted-Pair Cabling Systems - Draft (September 1995). Regula las especificaciones de equipos para la prueba, medición y certificación de sistemas de cableado estructurado.

7. TIA/EIA TSB-72_Centralized Optical Fiber Cabling Guidelines - Draft (September 1995). Regula la instalación de sistemas centralizados de fibra óptica.

8. TIA/EIA TSB-75_Additional Horizontal Cabling Practices for Open Offices - Draft (June 1996). Regula lo concerniente a espacios de oficinas abiertos u oficinas con mucho movimiento de personal.

3.4.2 ESTANDAR PARA LA SEGURIDAD DE LA INFORMACIÓN.

ISO / IEC 17799:2000(E) Information Technology – Code of practice for information security management. (Tecnología de la Información – Código de práctica para el manejo de seguridad informática).

En la actualidad las empresas son concientes de la gran importancia que tienen para el desarrollo de sus actividades el hecho de proteger de forma adecuada la información que poseen y especialmente aquella que les sirve para realizar correctamente su actividad de negocio.

El poder gestionar bien la seguridad de la información que manejan no sólo permitirá garantizar, de cara a la propia organización, que sus recursos están protegidos (asegurando la confidencialidad, integridad y disponibilidad de los mismos) sino que de cara a los posibles clientes les aportará un grado de confianza superior al que puedan ofrecer sus competidores, convirtiéndose en un factor más de distinción en el competitivo mercado en el que comercia la empresa.

Esta norma es aplicable a cualquier empresa, sea cual sea el tamaño, la actividad de negocio o el volumen del mismo, esto es lo que se denomina el principio de proporcionalidad de la norma, es decir que todos los aspectos que aparecen en la normativa deben ser contemplados y tenidos en cuenta por todas las organizaciones a la hora de proteger sus activos, y la diferencia radicará en que una gran organización tendrá que utilizar más recursos para proteger activos similares a los que puede poseer una pequeña organización.

De la misma forma, dos organizaciones que tengan actividades de negocio muy diferentes, no dedicarán los mismos esfuerzos a proteger los mismos activos/informaciones. En pocas palabras, esta norma debe tenerse como guía de los aspectos que deben tener controlados y no quiere decir que todos los aspectos que en ella aparecen tienen que ser

implementados con los últimos avances, eso dependerá de la naturaleza de la propia organización.

Como conclusión se puede decir que la normativa ISO/IEC 17799:2000 debe ser utilizada como un índice de los puntos que pueden provocar algún tipo de incidente de seguridad en una organización para que éstas se puedan proteger de los mismos, sin olvidarse aquellos que puedan parecer más sencillos de controlar hasta llegar a los que pueden suponer un mayor dispendio de recursos a las organizaciones.

CLAUSULAS ISO/IEC 17799	OBJETIVOS DE CONTROL
1. POLÍTICA DE SEGURIDAD	• Documento de política de seguridad. • Revisión y evaluación del documento de política de seguridad.

CLAUSULAS ISO/IEC 17799	OBJETIVOS DE CONTROL
2. ORGANIZACIÓN DE LA SEGURIDAD	• Infraestructura de organización de la seguridad. • Foro de gestión de seguridad de la información. • Coordinación de seguridad de la información. • Asignación de responsabilidades de seguridad de información. • Proceso de la autorización para información que procesa los medios. • Consejo especializado de seguridad de información. • Cooperación entre la organización. • Revisión independiente de seguridad de la información. • SEGURIDAD EN ACCESO DE TERCERAS PARTES. • Identificación de riesgos en los enlaces a terceros. • Requerimientos de seguridad en los enlaces con terceros. • (OUTSOURCING) EXTERNALIZACIÓN. • Requisitos de seguridad en los contratos de outsourcing.
3. CLASIFICACIÓN Y CONTROL DE ACTIVOS	• LA RESPONSABILIDAD PARA LOS ACTIVOS. • Inventario de activos. • CLASIFICACIÓN DE LA INFORMACIÓN. • Pautas de la clasificación. • Nivelación y manejo de la información.

CLAUSULAS ISO/IEC 17799	OBJETIVOS DE CONTROL

4. SEGURIDAD DEL PERSONAL	• SEGURIDAD EN LA DEFINICIÓN DE LOS PUESTOS Y EN LA CAPTACIÓN DE PERSONAL.
	  • Formación de los usuarios en educación de seguridad.
	  • Respuesta ante incidentes de seguridad.
	  • Condiciones de empleo.
	  • Acuerdos de confidencialidad.
	• RESPONDIENDO A LAS CASUALIDADES DE SEGURIDAD Y FUNCIONAMIENTOS DEFECTUOSOS.
	  • Casualidades de seguridad de información.
	  • Debilidades de la seguridad de información.
	  • Mal funcionamiento del software informático.
	  • Aprendiendo de los incidentes.
	  • Proceso disciplinario.
	• SEGURIDAD FÍSICA Y MEDIO AMBIENTAL.
	• ÁREAS SEGURAS.
	  • Perímetro de seguridad físico.
	  • Mandos de entrada físicos.
	  • Oficinas, cuartos y medios.
	  • Trabajando en las áreas de seguridad.
	  • Entrega aislada y las áreas cargantes.
	• SEGURIDAD DEL EQUIPO.
	  • Envio de equipo y protección.
	  • Suministros de poder.
	  • Seguridad del cableado.
	  • Mantenimiento del equipo.
	  • Seguridad fuera de premisas del equipamiento.
	  • Disposición segura o re-usada de equipo.
	• LOS CONTROLES GENERALES.
	  • Escritorio claro y la política de la pantalla clara.

CLAUSULAS ISO/IEC 17799	OBJETIVOS DE CONTROL

5.LAS COMUNICACIONES Y DIRECCIÓN DE LAS OPERACIONES.	• PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES.
	  • Documentando los procedimientos operacionales.
	  • Control de cambio operacional.
	  • Incidentes en los procedimientos de dirección.
	  • Segregación de deberes.
	  • Desarrollo de separación y los medios operacionales.
	  • Manejo de medios externos.
	• SISTEMA DE PLANEACIÒN Y ACEPTACIÓN.
	  • Capacidad de planificación.
	  • Aceptación del sistema.
	• PROTECCIÓN CONTRA EL SOFTWARE MALÉVOLO.
	  • Controles contra el software malévolo.
	• HOUSEKEEPING ().
	  • Copia de Seguridad de la información.
	  • Operador de logs.
	  • Fallas en las Logins.
	• DIRECCION DE RED.
	  • Controles de red.
	• MEDIOS DE COMUNICACIÓN Y SEGURIDAD.
	  • Dirección para los medios de comunicación de computadoras portátiles.
	  • Disposición de medios de comunicación.
	  • Información que se ocupa de procedimientos.
	  • Seguridad de documentación del sistema.
	• INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE.
	  • Información y acuerdos de intercambio de software.

CLAUSULAS ISO/IEC 17799	OBJETIVOS DE CONTROL
	• Seguridad en el transito de los medios de comunicación. • Seguridad del comercio electrónico. • Seguridad del correo electrónico. • Seguridad en los sistemas de oficina electrónicos. • Sistemas públicamente disponibles.
6. CONTROL DE ACCESO.	• REQUISITO COMERCIAL PARA EL CONTROL DE ACCESO. • Política del control de acceso. • DIRECCIÓN DE ACCESO DE USUARIO. • Registro del usuario. • Dirección de privilegio. • Dirección de contraseña de usuario. • Revisión de derechos de acceso de usuario. • USO DE LAS RESPONSABILIDADES. • Uso de la contraseña. • Equipamiento del usuario desatendido. • CONTROL DE ACCESO A LA RED. • Política de uso de servidores des de red. • Bloqueos de Camino • Autentificación de usuario para conexiones externas. • Autentificación del nodo. • Control de conexión a red. • Red que derrota el control. • Seguridad de servicios de la red. • CONTROL DE ACCESO DEL SISTEMA OPARATIVO. • La identificación terminal automática. • Procedimientos terminales log-on Identificación de usuario y autentificación. • Contraseñas de inicio de sistema. • Uso de utilidades del sistema.

CLAUSULAS ISO/IEC 17799	OBJETIVOS DE CONTROL

7.DESARROLLO DE LOS SISTEMAS Y MANTENIMIENTO.	• REQUISITOS DE SEGURIDAD DE SISTEMAS.
	  • Análisis de requisitos de seguridad y especificación.
	• SEGURIDAD DE LOS SISTEMAS DE APLICACIÓN.
	  • Aprobación de datos de entrada.
	  • Control de proceso interior.
	  • Autentificación del mensaje.
	  • Aprobación de datos de rendimiento.
	• CONTROLES DE ENCRIPTACIÓN.
	  • Políticas en el uso de controles de encriptación y (criptografía / encriptografía).
	  • Firmas digitales.
	  • Servicios de no-repudiación.
	  • Dirección importante.
	• SEGURIDAD DE ARCHIVOS DEL SISTEMA.
	  • Control de software operacional.
	  • Protección de datos de prueba de sistema.
	  • Control de acceso para programar la biblioteca fuente.
	• LA SEGURIDAD EN EL DESARROLLO Y PROCESOS DE APOYO.
	  • Procedimientos de control de cambio.
	  • Revisión técnica de cambios del sistema operativo.
	  • Restricciones a los cambios a ,los paquetes de software.
	  • Canales de conversión y códigos troyanos.
	  • Desarrollo de software de realizado..
	  • Alarma de coacción para salvaguardar a los usuarios.
	  • Terminales fuera de tiempo.
	  • Limitación de tiempo de conexión.

CLAUSULAS ISO/IEC 17799	OBJETIVOS DE CONTROL

	• CONTROL DE ACCESO DE APLICACIÓN.
	  • Restricciones de acceso de información.
	  • Aislamiento del sistema sensible.
	• SUPERVISANDO EL ACCESO AL SISTEMA Y SU USO.
	  • Eventos logging.
	  • Supervisando el uso del sistema.
	  • Sincronización del reloj.
	• INFORMÁTICA MOVIL Y TELEWORKING.
	  • Informática móvil.
	  • Teleworking.

8. DIRECCIÓN DE CONTINUIDAD COMERCIAL.	• ASPECTOS DE DIRECCIÓN DE CONTINUIDAD COMERCIAL.
	  • Proceso de dirección de continuidad comercial.
	  • Continuidad comercial y análisis de impacto.
	  • Continuidad comercial que planea el armazón.
	  • Probando, mientras manteniendo y re-valuando los planes de continuidad comerciales.

9. CONFORMIDAD.	• LA CONFORMIDAD CON LOS REQUISITOS LEGALES.
	  • Identificación de legislación aplicable.
	  • Propiedad intelectual (IPR).
	  • Salvaguardando los archivos orgánicos.
	  • Protección de los datos y retiro de información personal.
	  • Prevención de mal uso de información que procesa los medios.
	  • Regulación de controles de criptografía.
	  • Colección de evidencia.

CLAUSULAS ISO/IEC 17799	OBJETIVOS DE CONTROL

	• REVISIONES DE POLÍTICA DE SEGURIDAD Y LA CONFORMIDAD TÉCNICA.
	  • Conformidad con la política de seguridad.
	  • Comprobación de conformidad técnica.
	• LAS CONSIDERACIONES DE AUDITORIA DE SISTEMA.
	  • Los controles de auditoria de sistema.
	  • Protección de herramientas de auditoria de sistema.

Tabla 23: Cláusulas de la norma ISO/IEC 17799 y sus respectivos objetivos de control.

3.4.3 TIA/EIA 942. ESTÁNDAR PARA LA SOLUCIÓN EN CENTROS DE DATOS.

El término centro de datos engloba diferentes significados. Hay quienes argumentarán que el centro de datos es el cuarto donde se almacenan los servidores. Otros visualizarán una perspectiva radicalmente diferente. Es verdad que en cierto momento, el centro de datos era más pequeño que el cuarto protegido de servidores. Sin embargo, con los avances tecnológicos y los negocios actuales de centrales de información el término mejor expresado sería "Centro de Datos de Misión Crítica". Los modelos de negocios han pasado por un ciclo completo de ser sitios de datos centralizados a descentralizados y nuevamente centralizados. Los negocios

están tomando conciencia de que los datos son su valor más poderoso y que se deben hacer enormes esfuerzos para asegurar su disponibilidad, seguridad y redundancia.

TIA/EIA-942 The Telecommunic ations Infrastructure Standard for Data Centers. (Estándar de Infraestructura de Telecomunicaciones para Centros de Datos) norma se encuentra en el proceso de certificación, trata acerca de la infraestructura y los componentes de un centro de datos, ya sea que una compañía implemente todos los aspectos que contemplen este documento o parte de estos componentes. Con el objetivo, en el ser capaz de responder al crecimiento y cambios en equipo, normas y demandas, al mismo tiempo que deberá mantenerse administrable y por supuesto confiable.

Algunos puntos que aborda este norma son:

- Infraestructura de cómputo y redes (cableado, fibra y electrónicos).
- Comunicaciones y monitoreo.
- Sistemas eléctricos de distribución, generación y acondicionamiento – UPS, generador es.
- Seguridad física y prevención de control de acceso, permisos y logging.
- Protección de circuitos.

- Iluminación apropiada.
- Altura mínima de techo.
- Tierra física.
- Racks y gabinetes para equipo.
- Canalizaciones: Piso falso y bandejas en techo.
- Circuitos y equipo de carriers
- Equipo de telecomunicaciones.
- Separaciones alrededor del equipo y terminaciones en paneles y racks.
- Dispositivos de almacenaje.
- Sistemas abiertos basados en normas.
- Convergencia con factores de crecimiento incorporados.

3.5 ESTANDARES Y NORMAS PARA POLÍTICAS EN LA COMPANIA.

Se muestra en el anexo # 17 la propuesta de política para la Empresa.

A continuación una parte de ellas:

3.5.1 ADMINISTRACIÓN Y POLITICAS DE CLAVES (PASSWORDS).

1 PROPÓSITOS

- Normar una estructura de referencia organizacional para evitar el manejo indebido de claves usadas en las diferentes aplicaciones y recursos informáticos de ANDINATEL S.A. como parte del trabajo diario de sus funcionarios y empleados.

2 ALCANCE

Esta política es aplicable para todas las dependencias de ANDINATEL S.A.

3 NORMAS

El cumplimiento de la política de Uso de Claves estará a cargo de:

Usuarios Finales y deberán cumplir las siguientes normas:

- Los usuarios asignados a las diferentes aplicaciones y recursos informáticos, así como sus claves NO serán compartidos y su uso es personal, confidencial e intransferible.
- Cuando el Administrador Nacional de Red cree un nuevo usuario o reinicie una clave existente, el usuario obligatoriamente debe considerar que:

  - La clave debe ser personalizada inmediatamente.
  - La clave debe tener mínimo 6 caracteres estos pueden ser numéricos o alfanuméricos.
  - La clave no debe ser de fácil acceso, ni seguir la secuencia del teclado.
  - La clave debe ser actualizada cada 3 meses.
  - La nueva clave no deberá haberse utilizado en ocasiones anteriores.

- Cuando el usuario deba salir del Sistema Operativo Windows 2000 deberá hacer uso de la cerradura con clave al momento de abandonar el sitio de trabajo temporal o definitivamente.
- Los códigos del usuario y sus claves serán manejadas por el usuario como información confidencial de ANDINATEL S.A. la

divulgación de las claves de acceso a terceras personas esta prohibida.

- El usuario dueño de una clave es responsable absoluto de todas y cada una de las operaciones que se realicen con dicha clave.

Gerentes o Jefes

El Gerente o Jefe a más de observar y cumplir y hacer cumplir las normas referidas para los usuarios finales deberán tomar en cuenta en el ejercicio de sus funciones las siguientes consideraciones:

- Asegurar el conocimiento, la ejecución y difusión de la política para el uso de claves entre los empleados.
- Informar formalmente y de inmediato al área de Servidores cuando un funcionario, empleado o terceras partes que le reporta, finaliza su prestación de servicios en la institución, o se ausenta temporalmente.
- Definir el periodo de inicio y de expiración de las claves correspondientes a terceras partes, contratistas y empleados temporales

4 PROCEDIMIENTOS

1.1 ASIGANCION DE CLAVE A UN NUEVO USUARIO.

Para la asignación de password a un nuevo funcionario se seguirá el siguiente procedimiento:

- Al momento de crear la cuenta de usuario se le asigna un password temporal que es 1-2-3-4-5-6 el mismo que deberá ser cambiado cuando el nuevo funcionario ingrese por primera vez en el computador.

1.2 CAMBIO DE CLAVE POR EL USUARIO.

Al ingresar por primera vez el usuario al computador este deberá digitar la clave 1-2-3-4-5-6, inmediatamente le aparecerá una ventana de dialogo que le indicara que debe cambiar su clave.

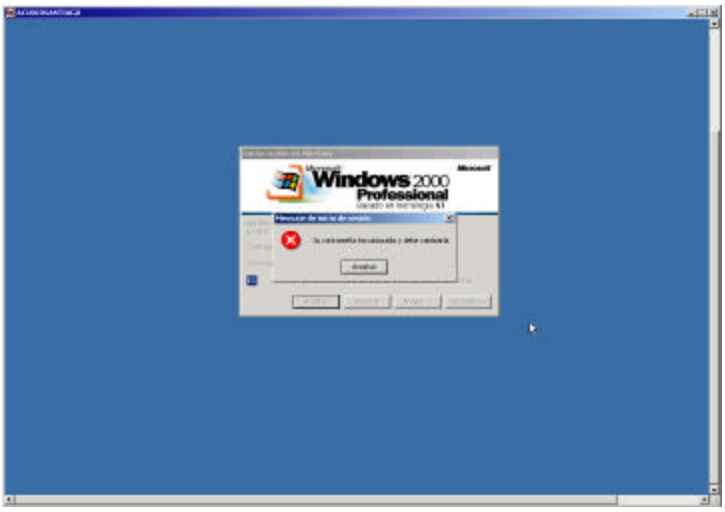

Figura 16: Mensaje de cambio de clave

Al presionar el botón de aceptar le aparecerá una nueva ventana de dialogo que le dirá que ingrese su clave anterior es decir 1-2-3-4-5-6 y a continuación ingresar un nuevo password y confirmarlo.

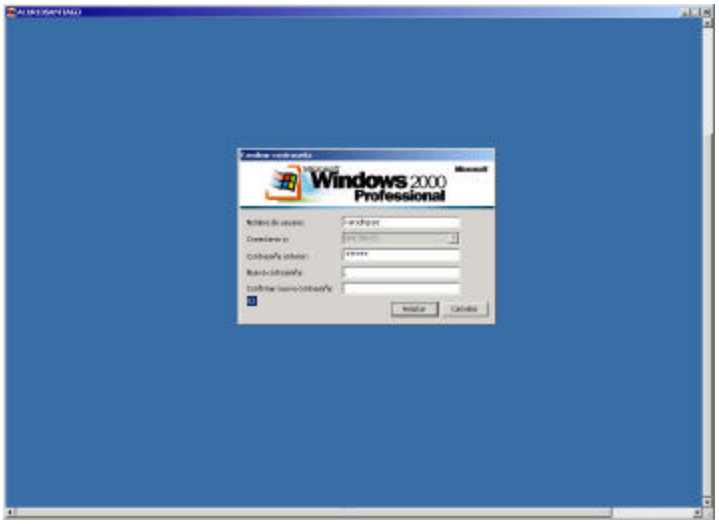

Figura 17: Ingreso de clave nueva

3.5.2 CAMBIO DE PASSWORD DE USUARIOS DE RED.

Por seguridad de la integridad y fidelidad de la información existente en cada una de las computadoras que se utilizan en toda la red de ANDINATEL S.A., se ha decidido que la contraseña de inicio de sesión de red sea cambiada cada 90 días.

1. En primera instancia aparecerá una ventana con un mensaje que su contraseña a caducado y debe ser cambiada como se muestra en la siguiente figura.

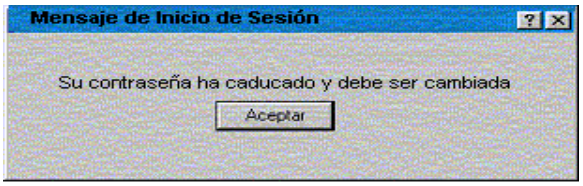

Figura 18: Mensaje de caducidad de contraseña

2. La ventana que aparecerá es la que se muestra en la figura siguiente.

   En esta ventana se deberá ingresar la contraseña anterior con la que estaban ingresando en la casilla contraseña anterior. A continuación debe ingresar la nueva contraseña que usted desee en la casilla contraseña nueva, tomando en cuenta que no debe ser menor de 5 caracteres y tampoco espacios en blanco, luego de efectuado este

paso se debe volver a ingresar la contraseña nueva en la casilla de confirmar contraseña nueva.

Figura 19: Cambiar contraseña

Nota: por favor tomar en cuenta que los caracteres que se ingresen estén en letras mayúsculas o minúsculas.

3. Una vez concluido el paso anterior aparece una ventana indicando que la contraseña ha sido cambiada exitosamente ante lo cual presionamos el botón aceptar como se muestra en la siguiente figura.

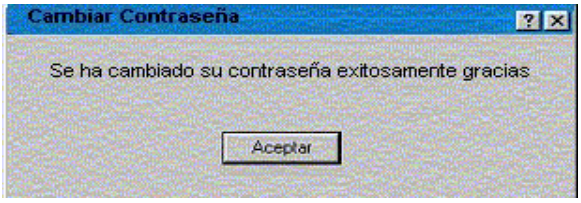

Figura 20: Cambio exitoso de contraseña

En caso de tener algún inconveniente con este procedimiento por favor llamar a los siguientes teléfonos: 02-2-461400 Ext. 523, 557, 809. Estarán gustosos de ayudarle.

3.5.3 ADMINISTRACION DE USUARIO S DE RAS.

1 PROPÓSITOS

- Normar la administración de usuarios en Servidores de Acceso Remoto.

2 ALCANCE

Esta política es aplicable para todas las dependencias de Andinatel S.A.

3 NORMAS

- Solamente el Presidente y Vicepresidentes Ejecutivos de cada área podrán solicitar al Jefe del departamento de Redes de la Gerencia de Informática la creación de una cuenta en el RAS para acceder a la red de datos de Andinatel por medio de un modem.

- Es obligación de Recursos Humanos comunicar al Jefe del departamento de Redes de la Gerencia de Informática cuando un empleado sale de la empresa. Es sumamente riesgoso tener habilitada una cuenta de un funcionario que dejó de prestar servicios.
- El Jefe del departamento de Redes de la Gerencia de Informática está facultado para realizar auditorias de las cuentas de usuario creadas en el RAS. Estas auditorias servirán para detectar si existen personas que quieren ingresar indebidamente a la red. Las auditorias se realizarán indistintamente. Los Vicepresidentes y Gerentes de área también pueden solicitar al Jefe del departamento de Redes de la Gerencia de Informática la auditoria de las cuentas por un tiempo determinado
- De detectar que un usuario está haciendo mal uso de su cuenta, el Jefe del departamento de Redes de la Gerencia de Informática después de cancelar la cuenta, solicitará la sanción correspondiente a Recursos Humanos.
- La red de datos de Andinatel es para exclusiva utilización de trabajos relacionados con la Empresa.

4 PROCEDIMIENTOS

4.1 SOLICITUD CREACIÓN DE CUENTAS DE USUARIO

Para la solicitud de creación de cuentas de usuario en los equipos RAS se seguirá el siguiente procedimiento:

1. El Presidente y/o Vicepresidentes Ejecutivos deberá solicitar al Jefe del departamento de Redes de la Gerencia de Informática la creación de una cuenta de usuario en los equipos RAS indicando si es el caso el horario con el que el usuario podrá ingresar a la red de Andinatel por medio de este servicio.
2. El jefe del departamento de Redes de la Gerencia de Informática creará y configurará la cuenta de acuerdo a lo solicitado.
3. El Jefe del departamento de Redes de la Gerencia de Informática asignará un técnico para que configure el equipo del usuario dueño de la cuenta con el servicio de acceso remoto. El técnico reportará al jefe del departamento de Redes de la Gerencia de Informática el cumplimiento del trabajo.

4.2 CREACIÓN DE CUENTAS DE USUARIO EN EQUIPOS RAS.

Para la creación de cuentas en servidores Windows NT se deberá seguir el siguiente procedimiento.

1. Ir a Inicio – Ejecutar y digitar Telnet XXX.XXX.XXX.XXX, debiendo ser reemplazado las X con el número IP asignado al equipo RAS.
2. Digitar el Login y Password del administrador del equipo RAS
3. Ingresar el siguientes comando:

   add user Nombre_usuario password Password_usuario .....

   En nombre_usuario se ingresará el siguiente estándar:

   - La inicial del primer nombre y a continuación el primer apellido. Por ejemplo, si el usuario se llama Francisco Xavier Páez Albán, el nombre de usuario será: fpaez.

   - Si existen algún otro usuario ya creado con el mismo nombre de usuario, luego la inicial del primer nombre se

incrementará la inicial del segundo nombre. Si todavía se repite el nombre de usuario, al final del apellido se incrementará la inicial del segundo apellido. En caso de volver a repetirse al final del nombre se añadirá un número secuencial para los casos que existan.

En password se ingresará una clave secreta para el usuario.

4. Con esto el usuario será agregado al equipo RAS.

4.3 CONFIGURACIÓN DE EQUIPO PARA INGRESO AL RAS.

Para ingresar a la red de servidores Windows NT se deberá seguir el siguiente procedimiento:

1. Encender el equipo.
2. Cuando finaliza de cargar Windows, El programa se quedará en una pantalla en donde se solicita ingresar el nombre de usuario, la contraseña y el dominio a donde corresponde. Para esto el usuario deberá ingresar el nombre de usuario asignado, su contraseña secreta y por último escribir el dominio correspondiente dependiendo del lugar en donde esté trabajando. Si el usuario se salta esta pantalla presionando cancelar o la tecla

escape, podrá ingresar a Windows pero no tendrá acceso a ningún recurso de la red, debiendo luego ingresar mediante ras a la red.

3. Presionar el Botón Acepta si estuviera conectado físicamente en la red.
4. Entonces se presentará la pantalla de inicio de Windows y se comenzará a trabajar sin problemas.
5. En cualquiera de los dos casos anteriores tanto conectado físicamente a la red o mediante Ras podrán utilizar los Recursos de red disponibles.

4.4 INGRESO AL SERVICIO RAS.

Para ingresar al servicio RAS se deberá seguir el siguiente procedimiento:

1. Ingresar inicio – Programas – Accesorios –Comunicaciones – Acceso Telefónico a redes, o Mi Pc, Acceso Telefónico a Redes.
2. Hacer doble clic en el ícono de ANDINATEL S.A..
3. Ingresar el nombre de usuario y password asignado al usuario. Posteriormente revisar el número de teléfono del equipo RAS al que se va a llamar.

4. Presionar el botón Marcar. Con esto el computador intentará realizar la llamada telefónica y conectarse al equipo RAS.
5. Al conectarse, el equipo presentará una pantalla de ingreso a la red Windows NT, en donde deberá ingresar los datos del usuario para poder utilizar la red de datos de ANDINATEL S.A..
6. Luego de esto podrá trabajar normalmente con todos los servicios de la red de datos que posee en la Empresa.

4.5 SOLICITUD DE ELIMINACIÓN DE CUENTAS DE USUARIO

Para la solicitud de eliminación de cuentas de usuario porque no Laboren en la Empresa se deberá seguir el siguiente procedimiento:

1. Recursos Humanos enviará una solicitud al Jefe del departamento de Redes de la Gerencia de informática indicando la cuenta que debe ser eliminada.
2. El Jefe del departamento de Redes de la Gerencia de Informática bloqueará esta cuenta por una semana para luego ser borrada definitivamente. Al borrar la cuenta, se borrará el acceso a todos los servicios de la red, incluyendo el buzón de correo que haya tenido el usuario.

3. El Jefe del departamento de Redes notificará a Recursos Humanos cuando la cuenta haya sido borrada.
4. O simplemente solo se borrará éste servicio por pedido del Vicepresidente del Área que pertenece el Usuario por ya no ser necesario el mismo, en este caso solo se cancelará la cuenta de RAS y no los servicios de la Red.

3.5.4 ADMINISTRACION DE USUARIOS DE RED.

1 PROPÓSITOS

- Normar la administración de usuarios de red

2 ALCANCE

Esta política es aplicable para todas las dependencias de ANDINATEL S.A..

3 NORMAS

- Las cuentas de usuario de acceso a la red de datos son controladas por los servidores Windows 2000 de ANDINATEL S.A.deben ser

solicitadas al Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet por el jefe superior del departamento en donde trabaja el nuevo usuario, indicando los servicios a los que debe tener acceso el usuario, tales como: servicio de correo electrónico, espacio en algún servidor, conexión a una determinada aplicación de la Empresa, etc. En el caso de acceso a Internet, se seguirá el procedimiento para acceso a los servicio de Internet.

- Cada usuario que trabaje en la red de datos controlada por los servidores Windows 2000 de ANDINATEL S.A.deberá poseer su cuenta de usuario para el ingreso a la misma. Esto hace que cada usuario sea responsable de lo que se realice en la red con esa cuenta, por tal motivo las claves de ingreso deben ser secretas.
- Las cuentas de usuario en los servidores de Windows 2000 deben tener una caducidad de 3 meses en cuanto a claves de usuarios. Esto quiere decir que los usuarios deberán cambiar su clave obligatoriamente cada 3 meses, de lo contrario no podrán ingresar a la red.
- Las cuentas de usuario se bloquean automáticamente luego del tercer intento fallido de ingreso a la Red. Para el desbloqueo de la cuenta el usuario deberá comunicarse con el departamento de Redes de la Vicepresidencia de Sistemas y Andinanet.

- Solamente el responsable de la cuenta o el Jefe superior del usuario pueden solicitar la intervención de una cuenta específica, de lo contrario éstas no pueden ser cambiadas.
- El Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet está facultado para realizar auditorias de las cuentas de usuario creadas en los servidores. Estas auditorias servirán para detectar si existen personas que quieren ingresar indebidamente a la red. Las auditorias se realizarán indistintamente. Los Vicepresidentes y Gerentes de área también pueden solicitar al Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet la auditoria de las cuentas por un tiempo determinado.
- De detectar que un usuario está haciendo mal uso de su cuenta, el Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet solicitará la sanción correspondiente a Recursos Humanos y procederá al bloqueo temporal de la misma, hasta que reciba las correspondientes disposiciones.
- Es obligación de Recursos Humanos comunicar cuando un empleado sale de la empresa al Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet para actualizar la lista de usuarios de la red.

- La red de datos de Andinatel es para exclusiva utilización de trabajos relacionados con la Empresa. En caso que se detecte una mala utilización de los recursos de la red se solicitará la sanción correspondiente a Recursos Humanos.
- Cualquier adición de un Servidor 2000 con su respectivo Software para su funcionamiento y de aplicación en la Intranet deberá ser administrado por el departamento de Servidores así como también la incorporación de redes lógicas dentro de la misma.

4 PROCEDIMIENTOS

4.1 SOLICITUD CREACIÓN DE CUENTAS DE USUARIO

Para la solicitud de creación de cuentas de usuario en los servidores Windows 2000 se deberá seguir el siguiente procedimiento

1. El Jefe superior del usuario que requiere la nueva cuenta deberá solicitar al Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet la creación de la misma con los diferentes servicios que necesita la persona, los principales son:

- Buzón de correo.
- Acceso a Lotus Notes.
- Acceso a espacio en un servidor de la Red.
- Acceso a una Aplicación específica creada para la Intranet o Extranet.

Si existe alguna condición específica para la creación de usuarios, en esta solicitud también se deberá especificarlas.

2. El jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet asignará un técnico para la creación de la cuenta y de los diferentes servicios que se solicite, así como también la configuración del equipo del nuevo usuario.
3. El jefe del departamento de Servidores bloqueará temporalmente una cuenta cuyo usuario haya salido de la empresa o se despidiera de la misma hasta recibir las instrucciones por parte de recursos humanos.
4. El técnico reportará al jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet el cumplimiento del trabajo.

4.2 CREACIÓN DE CUENTAS DE USUARIO EN SERVIDORES WINDOWS 2000

Para la creación de cuentas en servidores Windows NT se deberá seguir el siguiente procedimiento.

1. En la consola del servidor ingresar a: programas-Herramientas administrativas-Active directory users and computers.
2. Escoger el dominio y unidad organizacional en donde se va a crear la cuenta.

   - Uiomai01 para todos los usuarios que trabajan en ANDINATEL S.A.

3. Escoger en el menú principal Usuario-usuario nuevo, entonces se desplegará la siguiente ventana:

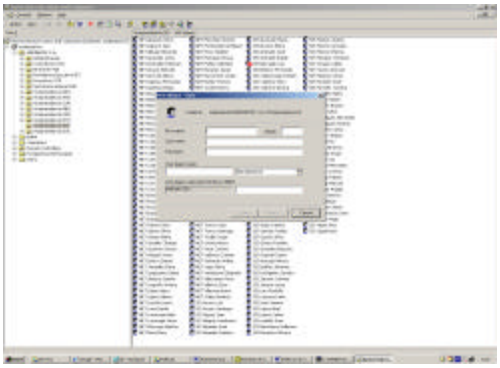

Figura 21: Active Directory Users and Computers

4. En la pantalla se ingresará el nombre de usuario. Para esto se llevará el siguiente estándar:

   - La inicial del primer nombre y a continuación el primer apellido. Por ejemplo, si el usuario se llama Francisco Xavier Páez Albán, el nombre de usuario será: fpaez.
   - Si existen algún otro usuario ya creado con el mismo nombre de usuario, luego la inicial del primer nombre se incrementará la inicial del segundo nombre. Si todavía se repite el nombre de usuario, al final del apellido se incrementará la inicial del segundo apellido. En caso de volver a repetirse al final del nombre se añadirá un número secuencial para los casos que existan.

5. Posteriormente se ingresará en el campo "Nombre Completo" el nombre completo de la persona.
6. En el campo Descripción se ingresará la ciudad en donde trabaja y el departamento.
7. En el campo Contraseña se ingresará el mismo nombre de usuario.
8. Se dejara el visto en la opción: "El usuario debe cambiar la contraseña en el siguiente inicio de sesión". Esto permitirá al usuario cambiar su contraseña al entrar por primera vez a la red,

y luego periódicamente según instrucciones emitidas vía Correo para el efecto.

9. En caso que el usuario pertenezca a un grupo de trabajo especial se le añadirá a este presionando en el botón de Grupos.
10. Luego de realizar estos pasos, se deberá presionar el botón de Agregar.
11. Con esto el usuario será agregado al dominio.

4.3 INGRESO A LA RED DE SERVIDORES WINDOWS 2000.

Para ingresar a la red de servidores Windows 2000 se deberá seguir el siguiente procedimiento:

1. Encender el equipo.
2. Cuando finaliza de cargar Windows, El programa se quedará en una pantalla en donde se solicita ingresar el nombre de usuario, la contraseña y el dominio a donde corresponde. Para esto el usuario deberá ingresar el nombre de usuario asignado, su contraseña secreta y por último escribir el dominio correspondiente dependiendo del lugar en donde esté trabajando. Si el usuario se salta esta pantalla, podrá ingresar a Windows pero no tendrá acceso a ningún recurso de la red.
3. Presionar el Botón Aceptar

4. Entonces se presentará la pantalla de inicio de Windows y se comenzará a trabajar sin problemas.

4.4 SOLICITUD DE INTERVENCIÓN DE UNA CUENTA.

La intervención de una cuenta se da por diferentes motivos, la más común es por el olvido de la contraseña. Para realizar este trabajo se seguirá el siguiente procedimiento.

1. El responsable de la cuenta o el jefe del mismo solicitará al Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet el cambio de cable de la cuenta.
2. El jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet asignará un técnico para realizar este trabajo.
3. El técnico cambiará la contraseña con el nombre de usuario del responsable de la cuenta y habilitará la opción: “El usuario debe cambiar la contraseña en el siguiente inicio de sesión”, para que luego el usuario o el Jefe superior ingrese su contraseña secreta.
4. Una vez terminado el trabajo, el técnico notificará el trabajo cumplido al usuario que solicitó y al Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet.

4.5 AUDITORIA A CUENTAS DE USUARIO

Para realizar la auditoria de las cuentas de usuario de los servidores Windows 2000 se deberá seguir el siguiente procedimiento

1. Los Vicepresidentes y Gerentes de área solicitarán al Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet la auditoria de las cuentas de usuario indicando el motivo de la misma.
2. Dependiendo del motivo se levantarán las auditorias en el servidor. El tipo de auditorias que se pueden realizar son las que se indican en el siguiente gráfico:

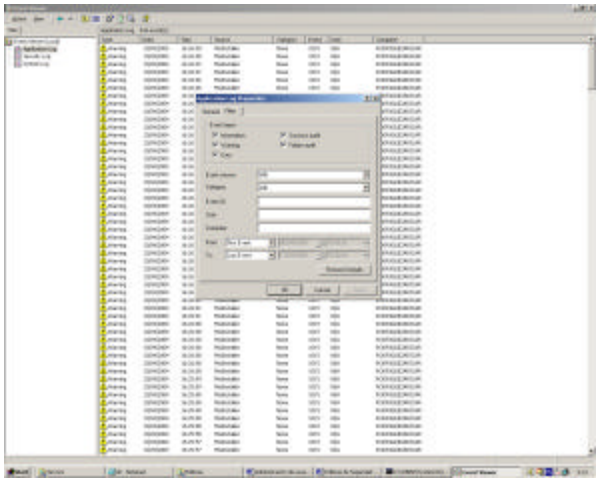

Figura 22: Event Viewer

3. Una vez pasado el periodo de auditoria solicitado, el Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet enviará el informe respectivo a la persona que lo solicitó.

4.6 SOLICITUD DE ELIMINACIÓN DE CUENTAS DE USUARIO

Para la solicitud de eliminación de cuentas de usuario se deberá seguir el siguiente procedimiento:

1. Recursos Humanos enviará una solicitud al Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet indicando la cuenta que debe ser eliminada.
2. El Jefe del departamento de Servidores de la Vicepresidencia de Sistemas y Andinanet bloqueará esta cuenta por una semana para luego ser borrada definitivamente. Al borrar la cuenta, se borrará el acceso a todos los servicios de la red, incluyendo el buzón de correo que haya tenido el usuario.
3. El Jefe del departamento de Servidores notificará a Recursos Humanos cuando la cuenta haya sido borrada.