No Tiene Manual del Usuario Normal del Sistema

DISEÑO DE UNA POLITICA DE SEGURIDAD PARA LA RED CORPORATIVA DE SUBOCOL S.A.

Alvaro Enrique De La Hoz Peñate
Orlando Duarte Arciniegas
Simón Gómez Medina

Director del Proyecto
Ing. Emilio Auque

Asesor del Proyecto
Ing. Emilio Auque

UNIVERSIDAD SIMON BOLIVAR
FACULTAD DE INGENIERIA DE SISTEMAS 11 "A" NOCTURNO
BARRANQUILLA
2003

CONTENIDO

INTRODUCCION

Las Políticas de Seguridad Informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una Organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocio.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCION DEL PROBLEMA

La Seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aún, desde la globalización de Internet.

Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez, más personas y más empresas sienten la necesidad de conectarse a este mundo.

1.2. FORMULACION DEL PROBLEMA

En vista que SUBOCOL S.A. Se encuentra en un proceso de expansión tecnológica se ve en la necesidad de implantar Políticas de Seguridad en su red que sirvan para contrarrestar ataques internos a la red local y proteger la información.

En estos momentos cuenta con un Servidor IBM Netfinity con 256 MB en ram, pentium III de 500 Mhz con doble procesador, arreglo de tres discos de 9 Gigabytes cada uno, una tarjeta de red, sistema operativo Windows NT, igualmente posee un proxy Wingate de 50 usuarios y no poseen firewall.

Presentan una Red LAN de 40 usuarios, conformada por un swich de 100baseT de 24 puertos, un concentrador 10baseT de 24 usuarios, cableado estructurado de nivel 5 de voz y datos, una UPS de 8 Kva y una de 6 Kva, usando protocolo TCP/IP con direcciones fijas. También poseen un canal dedicado a 128 Kbps.

Actualmente incluyeron un nuevo servicio como ISP (Proveedor de Servicios de Internet) para la comunidad automotriz.

Las estaciones de Subocol tienen diferentes sistemas operativos repartidos así: 30% Windows 95, 40% Windows 98, 20% Windows XP y un 20% Windows Millenium.

No existen Políticas que controlen que un usuario comparta archivos o carpetas con otro usuario. Poseen una RDSI de 64 como contingencia por si presentan problemas con el canal.

En cuanto a las Políticas de backup poseen un documento donde explican la forma de realizar el backup (ver figura 2) y otro donde explica la certificación del mismo (ver figura 1).

En la actualidad hacen backup los días lunes, miércoles y viernes de cada semana al servidor y no a las estaciones a menos que el usuario lo solicite, no existe una bitácora de backup que deje constancia de la copia, solo hacen un memorando de remisión hacia el departamento administrativo donde se entrega el backup de la semana.

Poseen un antivirus llamado Norman Virus Control version 5.00.42.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Diseñar una Política de Seguridad que refleje los elementos de confidencialidad, integridad y disponibilidad de la información de Subocol S.A.

2.2. OBJETIVOS ESPECIFICOS

- Establecer los recursos que se desean proteger.
- Construir un listado de posibles amenazas a la red: internas.
- Diseñar planes ante la eventualidad de un daño en el servidor.
- Ofrecer mecanismos que ayuden al control de acceso de los usuarios a la red y al monitoreo de la red.

3. JUSTIFICACION

La revolución tecnológica que vivimos hoy, está cambiando sustancialmente la manera de trabajar de las personas. Hoy en día el usuario tiene fácil acceso a todos los recursos de información en la red corporativa de Subocol S.A., lo que ha causado un cambio significativo en el flujo de la información. Desde el momento que la información de la empresa puede ser fácilmente accesada, pone en peligro la seguridad de la red. Por este motivo investigaremos y desarrollaremos una política de seguridad para proteger la información de la red.

Debemos tener en cuenta que nuestra red es vulnerable a cualquier usuario de la organización o cualquier usuario que no pertenezca a ella. No importa lo pequeña que sea. Simplemente un usuario malintencionado puede intentar atacarla. Este será el primer punto de trabajo para tener segura nuestra red.

El desarrollo de esta política de seguridad será de gran ayuda para SUBOCOL S.A. y para los Administradores del Sistema, porque facilitará el monitoreo de la red y el control de acceso de los usuarios a la misma.

Esta política será una guía que determinará ciertos procedimientos a seguir en determinadas circunstancias y que de todos modos requiere que se haga seguimiento para que sea eficaz.

4. MARCO DE REFERENCIA

4.1. MARCO TEORICO

El uso creciente de la tecnología de la información en la actividad económica ha dado lugar a un incremento en el número de puestos de trabajo informatizados, con una relación de una estación por empleado, el cual aumenta constantemente en todos los sectores industriales.

Es evidente que existe un flujo de información entre estas estaciones, con destino al mismo departamento o a un punto distante del sitio de donde se generó la información; todo esto incita a tomar acciones que optimicen la difusión de la información que se mueve en un ámbito local. Las Redes de Area Local (LAN) han sido creadas para responder a ésta problemática.

"Una red de computadoras consiste en un conjunto de computadoras interconectadas entre si por un medio fisico, generalmente cables, con el propósito de que puedan intercambiar

información y compartir los recursos que esta posee"[1]. El éxito de las LAN reside en que cada día es mayor la cantidad de información que se procesa de una manera local, y a su vez mayor el número de usuarios que necesitan estar conectados entre sí, con la posibilidad de compartir recursos comunes.

Según el lugar y el espacio que ocupen, las redes se pueden clasificar en Redes de Area Local (LAN), las cuales se definen como redes de alta velocidad que se emplean para conectar computadoras en una localidad única. Entre las configuraciones de LAN populares se cuentan Ethernet, Token Ring y 10BaseT (también conocida como par trenzado).

[1] Andrew Tanembaum. Redes de computadoras. Ed. Prentice Hall

Entre las redes WAN más grandes se encuentran: la ARPANET, que fue creada por la Secretaría de Defensa de los Estados Unidos y se convirtió en lo que es actualmente la WAN mundial: INTERNET, a la cual se conectan actualmente miles de redes universitarias, de gobierno, corporativas y de investigación.

Entre los componentes de una red tenemos:

- **Servidor (Server):** El servidor es la máquina principal de la red, la que se encarga de administrar los recursos de la red y el flujo de la información.
- **Estación de Trabajo (Workstation):** Es una computadora que se encuentra conectada físicamente al servidor por medio de algún tipo de cable. Muchas de las veces esta computadora ejecuta su propio sistema operativo y ya adentro se añade al ambiente de la red.
- **Sistema Operativo de Red:** Es el sistema (Software) que se encarga de administrar y controlar en forma general la red.
- **Recursos a Compartir:** Son todos aquellos dispositivos de Hardware que van a ser utilizados en la red. Por ejemplo, las impresoras.
- **Hardware de Red:** Son aquellos dispositivos que se utilizan para interconectar a los componentes de la red, serían básicamente las tarjetas

de red y el cableado entre servidores y estaciones de trabajo, así como los cables para conectar los periféricos.

Actualmente la seguridad en las redes ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Esto ha llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales hayan desarrollado documentos, directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y

servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

El proponer o identificar una Política de Seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha Política en función del dinámico ambiente que rodea las organizaciones modernas.

Una Política de Seguridad informática establece el canal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización. No es una descripción técnica de mecanismos de Seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de lo que deseamos proteger y el por qué de ello.

Cada Política de Seguridad es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

Las Políticas de Seguridad deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones, por qué son tan importantes estos u otros recursos o servicios.

De igual forma, establecen las expectativas de la organización en relación con la Seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otro lado, la Política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud que pasará cuando algo suceda; no es una sentencia obligatoria de la ley.

Las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios,

cambio o diversificación de negocios entre otros. Revisemos algunos aspectos generales recomendados para la formulación de las mismas:

- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.
- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.
- No dar por hecho algo que es obvio. Hacer explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y

malos entendidos en el momento de establecer los mecanismos de Seguridad que respondan a las PSI trazadas.

La Seguridad Informática se refiere a la "*posibilidad de que los recursos de la red se usen de una manera adecuada*"[2]. La Seguridad informática es una colección de soluciones técnicas a problemas que no son técnicos. Se puede invertir mucho tiempo, dinero y esfuerzo en Seguridad informática, pero nunca se resolverá realmente el problema de la pérdida accidental de datos o de la interrupción intencional de las actividades. Antes de construir una barrera de protección, como preparación para conectar su red con el resto de Internet, es importante que usted entienda con exactitud qué recursos de la red y servicios desea proteger contra intrusos maliciosos o hacker, "Se dice de quien goza averiguando los detalles de sistemas de cómputo y cómo llevarlos a su límite, en contraposición a la mayoría de los usuarios que prefieren aprender sólo lo mínimo necesario"[3]. Una Política de red es un documento que describe los asuntos de Seguridad de red de una organización. Este documento se convierte en el primer paso para construir barreras de protección efectivas.

[2] Karanjit Siyan – Chris Hare. Firewalls y Seguridad en Internet. Prentice Hall
[3] GUY L., Steele. The Hacker's Dictionary

Un planteamiento posible para desarrollar esta política es el análisis de lo siguiente: ¿Qué recursos se quieren proteger?, ¿De qué personas necesita proteger los recursos?, ¿Qué tan reales son las amenazas?, ¿Qué tan importante es el recurso?, ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?. Al crear una política de seguridad, se debe saber cuáles recursos de la red vale la pena proteger, y entender que algunos son más importantes que otros. El análisis de riesgos implica determinar lo siguiente: Qué necesita proteger, De quién debe protegerlo, Cómo protegerlo.

En el análisis de riesgo es necesario determinar los siguientes factores: Estimación del riesgo de pérdida del recursos (Ri), Estimación de la importancia del recurso (Wi).

Con la siguiente fórmula es posible calcular el riesgo general de los recursos de la red:

$$WR = (R1 * W1 + R2 * W2 + ... + Rn * Wn) / (W1 + W2 + ... + Wn)$$

Muchas veces las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las

acciones de las mismas, con relativo éxito. Según algunos estudios resulta ardua el convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y la falta de una estrategia de mercadeo de los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para los juguetes de los ingenieros". Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad, que en muchos de los casos lleva a comprometer su información sensitiva y por ende su imagen corporativa.

Ante esta encrucijada, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

En particular, la gente debe saber las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una buena intrusión o una

travesura puede convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos.

Luego, para que las PSI logren abrirse espacio al interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía. De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en su diario hacer, donde se identifiquen las necesidades y acciones que materializan las políticas.

En este contexto, el entender la organización, sus elementos culturales y comportamientos nos deben llevar a reconocer las pautas de seguridad necesarias y suficientes que aseguren confiabilidad en las operaciones y funcionalidad de la compañía.

Algunas recomendaciones para "vender" las preocupaciones sobre la seguridad informática:

- Desarrolle ejemplos organizaciones relacionados con fallas de seguridad que capten la atención de sus interlocutores.

- Asocie el punto anterior a las estrategias de negocio y la imagen de la empresa en el desarrollo de sus actividades.
- Articule las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información.
- Muestre una valoración costo – beneficio, ante una falla de seguridad.
- Desarrolle las justificaciones de la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización.
- Un consejo más, sea oportuno y sagaz para presentar su producto, procurando tener la mayor información del negocio y los riesgos asociados con los activos críticos de la organización.

Las Políticas de Seguridad Informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad, integridad y disponibilidad de su sistema. En razón a lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos.

Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responden a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a conocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

Otros factores que se deben considerar para el análisis de riesgo de un recurso de red son, su disponibilidad, su integridad y su carácter confidencial. El RFC 1244 lista los siguientes recursos de red que deben ser considerados al estimar las amenazas a la seguridad general: **Hardware,** Procesadores, tarjetas, teclados, terminales, líneas de comunicación, enrutadores, etc.; **Software,**

Programas fuente, programas objeto, utilerías, programas de comunicación, sistemas operativos, etc.; **Datos,** Durante la ejecución, almacenamiento en línea, base de datos, bitácoras de auditoría, etc.; **Gente,** Usuarios, Operadores de Sistemas; **Documentación,** Sobre programas, hardware, sistemas, procedimientos administrativos locales; **Accesorios,** Papel, formas, cintas, información grabada.

En realidad es un concepto cuya definición exacta es difícil de proporcionar, debido a la gran cantidad de factores que intervienen. Sin embargo es posible enunciar que Seguridad es el conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

La Seguridad Informática debe vigilar principalmente por las siguientes propiedades:

Privacidad - La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la Privacidad es la Divulgación de Información Confidencial.

Integridad - La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

Disponibilidad - La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (En Inglés Denial of Service o DoS) o "tirar" el servidor.

Para simplificar, es posible dividir las tareas de administración de seguridad en tres grandes rubros. Estos son:

Autenticación .- Se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.

Autorización .- Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan efectivamente acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

Auditoria .- Se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este rubro el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Para ejemplificar lo anterior, tomemos el ejemplo de una compañía ficticia a la que llamaremos "Servicios de Cómputo". Esta compañía dispone de un servidor donde corre el software a través del cual se lleva a cabo el procesamiento de las nóminas y el control de recursos humanos. Autenticación se refiere a que sólo las personas de esos departamentos tengan cuentas de acceso a dichos equipos, puesto que sería peligroso que algún otro departamento lo tuviera. El responsable de los equipos de cómputo llevaría a cabo la labor de Autorización, al no permitir que todas las personas responsables de recursos humanos tuvieran acceso a las Bases de Datos de Nóminas, si no lo necesitan. La Auditoria se lleva a cabo al establecer políticas de uso y acceso a los recursos, así como reglamentos que rijan la no-divulgación de información confidencial. También aquí se debe llevar un registro de los recursos utilizados para prevenir, por ejemplo, que un uso del 100% en un disco provoque que el sistema deje de funcionar. Debe vigilarse también los intentos de acceso legal e ilegal al mismo.

La clasificación dentro de cada una de las áreas arriba expuestas es también un tanto compleja. Pero a grandes rasgos podemos decir que la seguridad en un sistema está determinada por:

- **EL FACTOR ORGANIZACIONAL:**

a) Usuarios:

- Tipo de usuarios que se tienen
- Reglamentos y Políticas que rigen su comportamiento.
- Vigilar que esos reglamentos y Políticas se cumplan, y no queden sólo en papel.

b) La alta dirección:

- Inversión en capacitación de los Administradores.
- Apoyo económico orientado a la adquisición de tecnología de Seguridad.
- Negociar acuerdos de soporte técnico con los proveedores de equipo.

- **EL FACTOR SOFTWARE:**

a) El sistema operativo

- Observar las recomendaciones del fabricante y aplicar los parches.
- Vigilar siempre las bitácoras.
- Mantenerse informado sobre las alertas de Seguridad.

b) Software de red:

- Vigilar de cerca las estadísticas de acceso y tráficos de la red Procurar implementar cortafuegos (firewalls).
- En la medida de lo posible, apoyar las conexiones cifradas.

- **EL FACTOR HARDWARE:**

a) Hardware de red:

- Elegir adecuadamente el tipo de tecnología de transporte (Ethernet, FDDI, etc).
- Proteger muy bien el cableado, las antenas y cualquier dispositivo de red.
- Proporcionar periódicamente mantenimiento a las instalaciones.

b) Servidores:

- Mantenerlos en condiciones de humedad y temperatura adecuados.
- Establecer políticas de acceso físico al servidor.
- El mantenimiento también es importante aquí.

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su voluntad de hacer algo que permita detener un posible ataque antes de que éste suceda (proactividad).

Hecha la aclaración, enumeremos algunos otros métodos:

I.- Sistemas de detección de intrusos.- Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, en base a la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

II.- Sistemas orientados a conexión de red.- Monitorean las conexiones de red que se intentan establecer con una red o un equipo en particular, siendo capaces de efectuar una acción en base a métricas como: origen de la conexión, destino de la conexión, servicio solicitado, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador vía correo electrónico o vía pager. En esta categoría están los cortafuegos (firewalls) y los wrappers.

III.- Sistemas de análisis de vulnerabilidades.- Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La desventaja de estos sistemas

es que pueden ser utilizados tanto por personas autorizadas como por personas que busquen acceso no autorizado al sistema

IV.- Sistemas de protección a la privacidad de la información.- Herramientas que utilizan criptografía para asegurar que la información sólo es visible a quien tiene autorización de verla. Su aplicación es principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas podemos situar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los certificados digitales tipo X.509

V.- Sistemas de protección a la integridad de información.- Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest 5 (MD5) o Secure Hash Algorithm 1 (SHA-1), o bien sistemas que utilizan varios de ellos como Tripwire.

Algunos consejos aplicables en cualquier ambiente:

a) Informar al usuario/administrador – Si usted es un administrador, notifique a sus usuarios de los mecanismos de seguridad que usted tiene

implementados, y anímelos a utilizarlos haciendo de su conocimiento las posibles consecuencias de no cumplir con ellos. Así pues hágales saber que si prestan su password están cometiendo una falta, y que igualmente serán responsables por los actos, de buena o mala fe, que alguien más realice con su cuenta si logra adivinar dicho password. Si usted es un usuario por otra parte, observe siempre una conducta acorde a lo que su administrador ha determinado como válida para el sistema al que tiene acceso. Así mismo, dé a conocer a su administrador, cualquier sospecha de violación a cualquier recurso al que usted tiene acceso legítimo.

b) Respaldar siempre.- Sin embargo no basta con efectuar respaldos. Una buena política de respaldos contempla, entre otras cosas: tiempos óptimos de respaldo y recuperación, periodicidad del respaldo y verificación de integridad (de nada sirve un respaldo no íntegro), necesidad de duplicidad y expiración de los respaldos. Si es usted un usuario, haga además un respaldo propio adicional al que hace el administrador siempre que le sea posible, dependiendo también de la importancia de su información.

c) Realizar verificaciones no predecibles.- Si un ladrón conoce las horas a las que la guardia de un banco hace su rondín, seguramente decidirá no robarlo a esas horas. Lo mismo sucede con los sistemas: si se hacen verificaciones periódicas, y alguien más conoce qué y cuándo se realizan,

será necesario además hacer verificaciones de periodicidad no predecible, a fín de obtener una estadística más real del comportamiento del sistema.

d) Leer las bitácoras.- Las bitácoras del sistema reflejan lo que ocurre en el mismo. De nada sirve tenerlas si no son leídas. Ahí es donde pueden descubrirse ataques no exitosos perpetrados contra su sistema, por ejemplo.

e) Aplicar "parches" o tener las últimas versiones del software.- Las vulnerabilidades sobre algún producto o plataforma, pueden dar la vuelta al mundo rápidamente gracias a Internet. Es recomendable por ello contar siempre con la versión más actualizada del software, o bien aplicar los "parches" respectivos cuando son liberados. En este rubro, el software libre (Como Linux o Apache) cuenta con una ventaja sobre software comercial, pues el tiempo de respuesta es dramáticamente más rápido para el software libre.

f) Leer noticias sobre Seguridad: Si su proveedor mantiene una lista de Seguridad, únase a ella. Así mismo suscríbase a listas que le informen sobre Seguridad en general de modo que obtenga un panorama amplio pero conciso sobre el tema. Seg-l es en este sentido una excelente opción;).

g) Cancelación de cuentas.- Todo lo anterior no sirve si personas que han trabajado para la organización poseen sus cuentas de acceso después de haber dejado de colaborar con ella. Las estadísticas demuestran que un

85% de los ataques de seguridad son realizados desde dentro de la organización, o bien a través de cuentas de personal que estuvo dentro de ella.

El Instituto Británico de Normas Técnicas (BSI) espera dar respuesta a todas las preguntas de las empresas Británicas o no, sobre Seguridad en Redes a través de la creación de la Norma Británica BS7799, que es un amplio plan para la implementación de la seguridad efectiva en Internet. El código de normas de la seguridad en Internet le brinda a los profesionales de tecnología de la información un anteproyecto para que desarrollen políticas y procesos de seguridad empresarial.

Publicada por primera vez en 1995, la norma BS7799 prepara a las empresas para que reciban la acreditación de seguridad en Internet del BSI a través de una auditoría realizada por un auditor externo a BSI pero acreditado por este. La acreditación les asegurará a sus clientes y asociados que la información guardada en las redes empresariales está segura y que la seguridad general de la empresa es confiable. Muchas organizaciones que se enfrenta a retos cada vez mayores en materia de seguridad están adoptando las normas BS7799 sin

el proceso de acreditación y lo utilizan simplemente como guía de los mejores procedimientos.

La norma ha tenido gran aceptación en muchos países como Australia, Sudáfrica, Nueva Zelanda, Holanda y Noruega. En efecto, el gobierno del Reino Unido recomendó como parte de su Ley de Protección a la Información de 1998, que entró en vigencia en marzo, 1 del 2000, que las compañías Británicas utilicen BS7799 como método de cumplimiento de la Ley. La versión internacional de la primera parte de BS7799 está actualmente en revisión por parte de la Organización Internacional de Normas Técnicas bajo la denominación ISO17799.

Si ISO17799 es aprobada por los socios, las normas serán adoptadas por las compañías y los asociados de las grandes compañías que realizan negocios en línea o que son contratistas del gobierno.

La norma BS7799 tiene tres grandes secciones: El código estándar o de los mejores procedimientos de seguridad, especificaciones de las normas para el sistema para el manejo de la seguridad de la información y por último el proceso de acreditación. El tiempo estimado para el proceso de

implementación de BS7799 y de preparación para la acreditación es de seis a nueve meses dependiendo de la complejidad de la infraestructura del Departamento de Sistemas.

En la sección de los mejores procedimientos, existen diez grandes áreas organizacionales con 127 controles de seguridad y más de 500 subcontroles que brindan ayuda a las empresas en la protección de información. Un enfoque general de esta sección es el manejo de riesgos cuyo objetivo es ayudar a la empresa en un plan previo para sus políticas de seguridad. No todos los controles podrán aplicarse a cada empresa, sin embargo la norma BS7799 ayuda a los lectores a identificar controles relevantes para sus empresas. Para la acreditación, la empresa debe especificar los controles que no están incluidos en sus políticas de seguridad y justificar su exclusión. Los temas de control son el uso de Internet, e-commerce, teléfonos móviles de teleconmutación, teléfonos móviles, aspectos jurídicos y recursos humanos.

La segunda sección de la norma BS7799 ayuda al personal de sistemas a evaluar y dar prioridad a las redes de acuerdo a los objetivos de la compañía para luego organizarlos en plan de seguridad o sistema para el manejo de la seguridad de la información. El plan de seguridad consta de cuatro fases:

Evaluación de riesgos, Manejo de riesgos, Implementación de los dispositivos de seguridad e Instructivo de aplicabilidad.

- **Evaluación de Riesgos:** Es el análisis de lo que puede sucederle a las redes y el impacto que el incidente puede tener en los objetivos de la empresa. Los códigos maliciosos y acceso a la red no autorizado son ejemplos de riesgos.
- **Manejo de Riesgos:** Es el plan que su empresa puede utilizar para reducir los riesgos. Los métodos utilizados en el manejo de riesgos no solo comprenden dispositivos de seguridad de la red, como los firewalls, sino también la seguridad física, procedimientos administrativos, planes de contingencia e iniciativas de los recursos humanos.
- **Dispositivos de Seguridad:** Son las herramientas actuales y recursos identificados y adoptados por la empresa para minimizar los riesgos.
- **Instructivo de Aplicabilidad:** Es un plan de seguridad que se requiere para la acreditación BS7799. Este instructivo comprende los controles de seguridad que la empresa ha adoptado y las razones por las cuales se tomaron esas medidas.

Además la empresa debe listar los controles específicos de BS7799 que no se han promulgado y explicar por qué.

La acreditación BS7799 termina con una auditoría a la seguridad. Muchas empresas deciden emplear consultores de la seguridad para que los ayuden en la preparación de la auditoría cuya preparación demora de seis a nueves meses. El proceso tiene dos partes para la auditoría de la acreditación. El auditor externo primero analiza el instructivo de aplicabilidad con la compañía y evalúa las razones para excluir los controles específicos para la norma BS7799. Esta parte de la auditoría se demora dos días. Al cabo de seis semanas, el auditor va al sitio para evaluar la efectividad de las políticas y procedimientos de seguridad empresarial. También se evalúa el cumplimiento de la empresa con los controles generales de la norma BS7799. Los auditores examinarán las tecnologías y entrevistarán a los empleados de varios departamentos para obtener una mejor apreciación sobre las políticas de seguridad empresarial adoptadas. Esta segunda parte de la auditoría de que la empresa es acreditada debe someter de nuevo a auditorías con cierta regularidad para conservar la acreditación.

Existen muchas ventajas operativas y estratégicas importantes por la acreditación de la norma BS7799. Entre sus beneficios específicos se encuentran los siguientes:

- Mejoramiento de la seguridad empresarial: A través del proceso de acreditación de la norma BS7799, las empresas reducirán la vulnerabilidad de las redes y tendrá un mejor manejo de los riesgos. La reducción de las vulnerabilidades significará menores transgresiones a la seguridad, lo cual generará una disminución de los fraudes, de los riesgos financieros y jurídicos, así como ahorro de tiempo y la confianza de los clientes.
- Planeación más efectiva de la seguridad: La norma BS7799 reúne 127 parámetros de seguridad en diez áreas con controles detallados y guía de los recursos humanos y de la planeación jurídica y de contingencia.
- Manejo más efectivo de la seguridad: Inevitablemente toda empresa debe iniciar el proceso de desarrollo o nuevo desarrollo de las políticas y procesos de seguridad en Internet. A diferencia de los proyectos empresariales orgánicos de seguridad empresarial, la norma BS7799 es un método comprobado para los mejores procedimientos de seguridad en Internet. Compañías como BT, HSBC, Marks and Spenser, Shell

International y Unilever contribuyen al desarrollo de BS7799 y han probado su efectividad en condiciones reales de negocios.

- Continua protección: Después de la acreditación, la empresa se mantendrá actualizada en las últimas vulnerabilidades y mejores procedimientos de la seguridad mediante auditorías y revisiones externas continuas de la norma BS7799.
- Alianzas más seguras: Para proteger mejor a la red empresarial mientras se realiza el EDE, la compañía puede utilizar la acreditación BS7799 como un requisito de seguridad para sus asociados y vendedores.
- E-Commerce seguro: La norma BS7799 le da a los consumidores un sello de seguridad y confiabilidad que le permite a los vendedores e-commerce acreditados, de instituciones financieras a e-tail, identificarlos con facilidad.
- Mayor confianza del cliente: Los clientes y vendedores con una alta sensibilidad a las transgresiones de seguridad en Internet buscan una evidencia concreta de la seguridad. Esta tranquilidad se la proporcionarán la acreditación de la nroma BS7799.
- Mayor auditoría ROI: La norma BS7799 contempla un proceso de acreditación con auditores acreditados. Aunque BS7799 es la norma

del sector, las empresas tendrán acceso a varios auditores externos acreditados, quienes deberán seguir los mejores procedimientos de auditoría para comprobar y evaluar las políticas de seguridad. El resultado será auditorías en seguridad más seguras y confiables.

- Menor responsabilidad civil: La responsabilidad civil de las empresas en incidentes de seguridad podrá reducirse si están acreditadas por la norma BS7799. Los tribunales reconocen que el cumplimiento de la norma es una señal de que existe una seguridad adecuada en las empresas.

El funcionamiento de la seguridad de la red para proteger la información es un aspecto importante para las actuales empresas. Aunque el proceso de implementación de políticas completas de la seguridad puede resultar intimidante, un proceso de normas para la seguridad en Internet como la norma BS7799 puede ayudarle al Departamento de Sistemas a administrar la seguridad de la red con eficie3ncia y efectividad.

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub.

Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", y con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Virtual LAN o red virtual), nos proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física.

Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast".

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma.

Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico.

Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, logramos, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.

Además, al poder distribuir a los usuarios en diferentes segmentos de la red, podemos situar puentes y encaminadores entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, podemos mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo.

Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN entre y salga desde/hacia otras redes.

Pero aún se puede llegar más lejos. Las redes virtuales nos permiten que la ubicuidad geográfica no se limite a diferentes concentradores o plantas de un

mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes.

Existen tres aproximaciones diferentes que pueden ser empleadas como soluciones válidas para proporcionar redes virtuales: conmutación de puertos, conmutación de segmentos con funciones de bridging, y conmutación de segmentos con funciones de bridging/routing.

Todas las soluciones están basadas en arquitecturas de red que emplean concentradores/conmutadores. Aunque las tres son soluciones válidas, sólo la última, con funciones de bridge/router, ofrece todos las ventajas a las VLAN.

1. **Conmutadores de puertos.** Los conmutadores de puertos son concentradores con varios segmentos, cada uno de los cuales proporciona el máximo ancho de banda disponible, según el tipo de red, compartido entre todos los puertos existentes en dicho segmento. Se diferencian de los conmutadores tradicionales en que sus puertos pueden ser dinámicamente asociados a cualquiera de los segmentos, mediante comandos software. Cada segmento se asocia a un "backplane", el cual a su vez, equivale a un

grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden asignadas y reasignadas a diferentes grupos de trabajo o redes virtuales.

Podemos definir a los conmutadores de puertos como "software patch panels", y su ventaja fundamental es la facilidad para la reconfiguración de los grupos de trabajo; sin embargo, tienen graves limitaciones.

Dado que están diseñados como dispositivos compartiendo un backplane físico, las reconfiguraciones de grupo de trabajo están limitadas al entorno de un único concentrador, y por tanto, todos los miembros del grupo deben de estar físicamente próximos.

Las redes virtuales con conmutadores de puertos, padecen de conectividad con el resto de la red. Al segmentar sus propios backplanes, no proporcionan conectividad integrada entre sus propios backplanes, y por tanto están "separados" de la comunicación con el resto de la red. Para ello requieren un

bridge/router externo. Ello implica mayores costes, además de la necesidad de reconfigurar el bridge/router cuando se producen cambios en la red.

Por último, los conmutadores de puertos no alivian el problema de saturación del ancho de banda de la red. Todos los nodos deben de conectarse al mismo segmento o backplane, y por tanto compartirán el ancho de banda disponible en el mismo, independientemente de su número.

2. **Conmutadores de segmentos con bridging:** A diferencia de los conmutadores de puertos, suministran el ancho de banda de múltiples segmentos de red, manteniendo la conectividad entre dichos segmentos. Para ello, se emplean los algoritmos tradicionales de los puentes (bridges), o subconjuntos de los mismos, para proporcionar conectividad entre varios segmentos a la "velocidad del cable" o velocidad máxima que permite la topología y protocolos de dicha red.

Mediante estos dispositivos, las VLAN no son grupos de trabajo conectados a un solo segmento o backplane, sino grupos lógicos de nodos que pueden ser

conectados a cualquier número de segmentos de red físicos. Estas VLAN son dominios de broadcast lógicos: conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la VLAN como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que los conmutadores de puertos, mediante comandos software se puede reconfigurar y modificar la estructura de la VLAN, con la ventaja añadida del ancho de banda repartido entre varios segmentos físicos. De esta forma, según va creciendo un grupo de trabajo, y para evitar su saturación, los usuarios del mismo pueden situarse en diferentes segmentos físicos, aún manteniendo el concepto de grupo de trabajo independiente del resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados.

Aún así, comparten el mismo problema con los conmutadores de puertos en cuanto a su comunicación fuera del grupo. Al estar aislados, para su comunicación con el resto de la red precisan de routers (encaminadores), con las consecuencias de las que ya hemos hablado en el caso anterior respecto del coste y la reconfiguración de la red.

3. **Conmutadores de segmentos con bridging/routing:** Son la solución evidente tras la atenta lectura de las dos soluciones anteriores. Dispositivos que comparten todas las ventajas de los conmutadores de segmentos con funciones de bridging, pero además, con funciones añadidas de routing (encaminamiento), lo que les proporciona fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expanden a través de diferentes segmentos de red.

Además, sus funciones de routing facilitan la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante las redes virtuales, podemos crear un nuevo grupo de trabajo, con tan solo una reconfiguración del software del conmutador. Ello evita el recableado de la red o el cambio en direcciones de subredes, permitiéndonos así asignar el ancho de banda requerido por el nuevo grupo de trabajo sin afectar a las aplicaciones de red existentes.

En las VLAN con funciones de routing, la comunicación con el resto de la red se puede realizar de dos modos diferentes: permitiendo que algunos segmentos sean miembros de varios grupos de trabajo, o mediante las funciones de routing multiprotocolo integradas, que facilitan el tráfico incluso entre varias VLAN's.

Los dispositivos con funciones VLAN nos ofrecen unas prestaciones de "valor añadido", suplementarias a las funciones específicas de las redes virtuales, aunque algunas de ellas son casi tan fundamentales como los principios mismos de las VLAN.

Al igual que en el caso de los grupos de trabajo "físicos", las VLAN permiten a un grupo de trabajo lógico compartir un dominio de broadcast. Ello significa que los sistemas dentro de una determinada VLAN reciben mensajes de broadcast desde el resto, independientemente de que residan o no en la misma red física. Por ello, las aplicaciones que requieren tráfico broadcast siguen funcionando en este tipo de redes virtuales. Al mismo tiempo, estos broadcast no son recibidos por otras estaciones situadas en otras VLAN.

Las VLAN no se limitan solo a un conmutador, sino que pueden extenderse a través de varios, estén o no físicamente en la misma localización geográfica.

Además las redes virtuales pueden solaparse, permitiendo que varias de ellas compartan determinados recursos, como backbones (troncales) de altas prestaciones o conexiones a servidores.

Uno de los mayores problemas a los que se enfrentan los administradores de las redes actuales, es la administración de las redes y subredes. Las VLAN tienen la habilidad de usar el mismo número de red en varios segmentos, lo que supone un práctico mecanismo para incrementar rápidamente el ancho de banda de nuevos segmentos de la red sin preocuparse de colisiones de direcciones.

Las soluciones tradicionales de internetworking, empleando concentradores y routers, requieren que cada segmento sea una única subred; por el contrario, en un dispositivo con facilidades VLAN, una subred puede expandirse a través de múltiples segmentos físicos, y un solo segmento físico puede soportar varias subredes.

Asimismo, hay que tener en cuenta que los modelos más avanzados de conmutadores con funciones VLAN, soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, que nos permiten determinar con gran precisión las características del tráfico y de la seguridad que deseamos en cada dominio, segmento, red o conjunto de redes. Todo ello se realiza en función de algoritmos de bridging, y routing multiprotocolo.

Vamos a intentar esquematizar los puntos en que las redes virtuales pueden beneficiar a las redes actuales:

1. *Movilidad:* Como hemos visto, el punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo.

2. *Dominios lógicos:* Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos, o en otras palabras, los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos.

3. *Control y conservación del ancho de banda:* Las redes virtuales pueden restringir los broadcast a los dominios lógicos donde han sido generados. Además, añadir usuarios a un determinado dominio o grupo

de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.

4. *Conectividad:* Los modelos con funciones de routing nos permiten interconectar diferentes conmutadores y expandir las redes virtuales a través de ellos, incluso aunque estén situados en lugares geográficos diversos.

5. *Seguridad:* Los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de cada red, proporcionando un alto grado de seguridad.

6. *Protección de la inversión:* Las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costes adicionales.

El primer suministrador de conmutadores con soporte VLAN fue ALANTEC (familia de concentradores/conmutadores multimedia inteligentes PowerHub), pero actualmente son muchos los fabricantes que ofrecen equipos con soluciones VLAN: Bytex (concentrador inteligente 7700), Cabletron (ESX-

MIM), Chipcom (OnLine), Lannet (MultiNet Hub), Synoptics (Lattis System 5000), UB (Hub Access/One) y 3Com (LinkBuilder).

Con los procesos de reingeniería de empresas y de downsizing, y con las nuevas necesidades de independencia, autonomía y fluidez entre grupos de trabajo, se requieren nuevas facilidades y más dinámicas para realizar cambios en las redes.

Las redes virtuales combinan mayores anchos de banda, facilidades de configuración y potencial de crecimiento, lo que ayudará a que se conviertan en un standard en los entornos corporativos.

En la actualidad, las implementaciones de tecnologías de redes virtuales no son interoperativos entre diferentes productos de diversos fabricantes.

Muchos de estos fabricantes intentan buscar soluciones adecuadas para lograr dicha interoperatividad, y por ello, una gran ventaja de las soluciones basadas en software es que podrán ser adaptadas a las normalizaciones que tendrán lugar en un futuro cercano. Algunas soluciones basadas en hardware habrán de quedarse atrás en este sentido.

Otro punto a destacar es que la tecnología ATM prevé, como parte importante de sus protocolos, grandes facilidades para las redes virtuales, lo que sin duda equivaldrá a grandes ventajas frente a la competencia para aquellos equipos que actualmente ya soportan sistemas VLAN.

El futuro es claro respecto de este punto: Las características VLAN formarán parte, en breve, de todos los equipos que se precien de querer ser competitivos.

Un cortafuegos o firewall es un sistema de defensa basado en el hecho de que todo el trafico de entrada o salida a la red debe pasar obligatoriamente por un sistema de seguridad capaz de autorizar, denegar, y tomar nota de aquello que ocurre en la red, o es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración.

desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

Aunque hay programas que se venden bajo la denominación de firewall, un firewall NO es un programa. Un firewall consiste en un conjunto de medidas HARDWARE y SOFTWARE destinadas a asegurar una instalación de red.

Un Firewall actúa en los niveles 3 (red) a 7 (aplicación) de OSI. Sus funciones son básicamente las siguientes:

- Llevar contabilidad de las transacciones realizadas en la red. Filtrar accesos no autorizados a máquinas (mediante filtrado de paquetes, o bien observando el contenido de las unidades de protocolo de Transporte, Sesión, Presentación, y aplicación).
- Alertar en caso de ataques o comportamiento extraño de los sistemas de comunicación.

Cualquier Firewall puede clasificarse dentro de uno de los tipos siguientes (o como una combinación de los mismos):

Filtros (Packet Filters).

Su cometido consiste en filtrar paquetes dejando pasar únicamente cierto tipo de tráfico. Estos filtros pueden implementarse a partir de routers (p.ej: en un Cisco, podemos definir access-lists asociadas a cada uno de los interfaces de red disponible). No son capaces de discernir si el paquete cuya entrada se permite incluye algún tipo de datos "maliciosos". Además, cualquier tipo de paquetes no permitidos puede viajar en el interior de tráfico permitido (ej: IP sobre IP). Desgraciadamente son difíciles de definir y depurar.

Proxy (Circuit Gateways)

En este caso la pasarela actúa del mismo modo que un simple cable (vía software) conectando nuestra red interna con el exterior. En general se requiere que el usuario esté autorizado para acceder al exterior o interior y que tenga una cuenta de salida en el proxy. Ciertos sistemas como SOCKS necesitan programas cliente modificados para soportarlo.

Pasarelas a nivel de Aplicación (Application Gateway)

Estas pasarelas se ocupan de comprobar que los protocolos a nivel de aplicación (ftp,http,etc...) se están utilizando de forma correcta sin tratar de

explotar algunos problemas que pudiese tener el software de red. Deben estar actualizados; de otro modo no habría forma de saber si alguien está tratando de atacar nuestro sistema.

Podemos bloquear todos los servicios basados en datagramas que no hagan uso de autentificación (todos los basados en UDP no cifrados), y todos los servicios basados en TCP que no se consideren estrictamente necesarios.

Un Switch es un dispositivo de Red situado en la capa 2 del modelo de referencia OSI, en esta capa además se encuentran las NIC (Netwok Interface Card; Placa de Red) pueden ser inalámbricas y los Bridges (Puentes).

La capa 2 del modelo de referencia OSI es la capa de Enlace de datos, esta capa proporciona un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

Un switch, al igual que un puente, es un dispositivo de la capa 2. De hecho, se denomina puente multipuerto, así como el hub se denomina repetidor multipuerto. La diferencia que tiene con el hub es que toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, así hacen que la LAN sea mucho más eficiente, hacen esto "conmutando" datos sólo desde el puerto al cual está conectado el host correspondiente. A diferencia de esto, el hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos. Esto hace que la LAN sea mas lenta.

A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión (pueden ser de 8, 12, 24 o 48, o conectando 2 de 24 en serie), dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red).

La diferencia entre un hub y un switch está dada por lo que sucede dentro de cada dispositivo.

El propósito del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, piense en el switch como un elemento que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto. El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total. Básicamente un Switch es un administrador inteligente del ancho de banda.

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño. De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz. Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina microsegmentación. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host. Los switches de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de Capa 2 de dirección MAC

destino, los switches pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la totalidad del paquete ingrese al switch. Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

Hay dos motivos fundamentales para dividir una LAN en segmentos. El primer motivo es aislar el tráfico entre segmentos, y obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños. Si la LAN no se divide en segmentos, las LAN cuyo tamaño sea mayor que un grupo de trabajo pequeño se congestionarían rápidamente con tráfico y colisiones y virtualmente no ofrecerían ningún ancho de banda.

Al dividir redes de gran tamaño en unidades autónomas, los puentes y los switches ofrecen varias ventajas. Un puente, o switch, reduce el tráfico que experimentan los dispositivos en todos los segmentos conectados ya que sólo se envía un determinado porcentaje de tráfico. Los puentes y los switches amplían la longitud efectiva de una LAN, permitiendo la conexión de estaciones distantes que anteriormente no estaban permitidas.

Aunque los puentes y los switches comparten los atributos más importantes, todavía existen varias diferencias entre ellos. Los switches son significativamente más veloces porque realizan la conmutación por hardware, mientras que los puentes lo hacen por software y pueden interconectar las LAN de distintos anchos de banda. Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch. Estos pueden soportar densidades de puerto más altas que los puentes. Algunos switches soportan la conmutación por el método cut- through, que reduce la latencia y las demoras de la red mientras que los puentes soportan sólo la conmutación de tráfico de guardar y enviar (store-and-forward). Por último, los switches reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.

5. FORMULACION DE LA HIPOTESIS

SI disponemos de metodología, asesoría calificada, investigación profunda sobre Políticas de Seguridad en el mundo; ENTONCES crearemos una política de Seguridad para Subocol S.A., eficiente para evitar intrusos, garantizar la seguridad de los datos realizando respaldo y recuperación de los mismos y auditar el uso de los recursos.

GLOSARIO

- **LAN:** Una red de computadoras consiste en un conjunto de computadoras interconectadas entre si por un medio físico, generalmente cables, con el propósito de que puedan intercambiar información y compartir los recursos que esta posee.
- **SERVIDOR (Server):** El servidor es la máquina principal de la red, la que se encarga de administrar los recursos de la red y el flujo de la información.
- **ESTACIÓN DE TRABAJO (Workstation):** Es una computadora que se encuentra conectada físicamente al servidor por medio de algún tipo de cable. Muchas de las veces esta computadora ejecuta su propio sistema operativo y ya adentro se añade al ambiente de la red.
- **PSI:** Políticas de Seguridad en Informática.
- **ISP:** Proveedor de Servicios de Internet.
- **BSI:** Instituto Británico de Normas Técnicas.

- **VLAN**: (Virtual LAN o red virtual), nos proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física.
- **SWITCH:** Un Switch es un dispositivo de red situado en la capa 2 del modelo de referencia OSI. Dispositivo de la red utilizado para separar dominios de colisión o segmentos de la red. Las unidades aprenderán la dirección original y de destino de otros nodos de la red y cuando se reciben los paquetes de datos, verifica esas direcciones y decide si los paquetes deben ser redirigidos a otro puerto.
- **FIREWALL:** La función del firewall es ser una sólida barrera entre su red y el mundo exterior. Este permite habilitar el acceso a usuarios y servicios aprobados. El firewall mantiene separada su red interna (de la cual usted tiene control) de diferentes tipos de redes externas (de las cual usted NO tiene control). El firewall controla la entrada y salida de trafico protegiendo su red de intromisiones indeseadas.
- **HUB:** También es llamado concentrador o repetidor. Extiende una red compartida a otros hubs o estaciones mediante la retransmisión de los marcos y la propagación de las colisiones.
- **ROUTER:** El router es un elemento más inteligente y posibilita la interconexión de diferentes tipos de redes de ordenadores. Un dispositivo

de la red que funciona como un switch inteligente. Es capaz de aprender no solo la dirección de origen y de destino sino también las sendas que deben utilizar los paquetes para llegar a su destino. Múltiples routers pueden ser seteados de modo de ser utilizados como respaldo en caso de una falla.

REFERENCIAS BIBLIOGRAFICAS

ANDREW, Tanembaum. Redes de computadoras. Ed. Prentice Hall.

KARANJIT, Siyan. CHRIS, Hare. Firewalls y seguridad en Internet. Prentice Hall.

GUY L., Steele. The Hacker's Dictionary.

http://master.cic.uanl.mx/~mhoz/seguridad/

http://www.netcraft.co.uk/security/diary.html

http://www.hispasec.com

DOCUMENTO
POLITICAS DE SEGURIDAD

SUBOCOL S.A.

SUBOCOL S.A. VEHICULOS & REPUESTOS	**AREA DE SEGURIDAD DE TECNOLOGIA** **PROCEDIMIENTOS Y POLITICAS DE RESPALDO Y RECUPERACION**	

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

INTRODUCCIÓN

Debido a la importancia de la información dentro de cada corporación es vital que ésta se encuentre protegida para garantizar su permanencia y efectividad a través del tiempo, esta protección de permitir que la organización pueda recuperarse ante cualquier evento que pudiese afectar el normal comportamiento y funcionamiento operativo, dicho evento puede ser desde un caso común problema de hardware hasta actos terroristas que pudiesen en un momento afectar significativamente los sistemas vigentes.

Este documento analiza la situación actual de los procedimientos y métodos utilizados en **SUBOCOL S.A.** para la recuperación de la información como también para los respaldos del sistema operativo y permitir así una recuperación efectiva de los diferentes sistemas.

SUROCOL S.A. VEHICULOS & REPUESTOS	GESTION DE SISTEMAS CERTIFICACIÓN DE BACKUPS DEL SISTEMA DATACAR 2001	Código: 010001 Página: 1 de 2

OBJETO

✪ Asegurar la integridad de la información para prevenir cualquier tipo de eventualidad que se presente.

AREA	RESPONSABLE	FLUJOGRAMA

DIRECCION DE SISTEMAS

1 Se anota el numero de registro y nombre de cada tabla que conforma la base de datos

2 En horas no laborables cuando ningún usuario este accesando el Datacar, Se limpian las tablas, corriendo la opción "limpiar tablas" del menú utilitarios de Datacar.

3 Desde explorador de Windows, se verifica la capacidad del disco duro, si existe espacio de 500 Megabites, crear carpeta nueva "Copiadatosdc2000". Si no existe ese espacio, LLAMAR ADMINISTRADOR, borrar archivos innecesarios.

4 El backup de datos debe realizarse sobre la carpeta "DATOS", de la carpeta principal "DC2000".

5 Verificar que al crear copia de seguridad, del menú utilitarios del programa se efectúa copia de las tablas principales del sistema a dicha carpeta, con la cual se montaran nuevas copias.

6 Ubicar carpeta "datos", alojada bajo la carpeta "dc2000". Copiar el contenido de esta a la recién creada "copiadatosdc2000"

7 Una vez ubicada "copiadatosdc2000", debe efectuarse sobre la misma un proceso de compresión de archivos. Para ello se utiliza el programa Winzip o Powerarchive

8 Se asigna un nombre al archivo de compresión que los agrupa, indicando dia mes y año, asi: datacarddmmaaaa.zip

9 Se copia este archivo a un medio externo (desde disco duro a cd, o diskette)

10 Se quema el archivo datacarddmmaaaa.zip en 2 cd. Etiquetados con el mismo nombre del archivo, con fecha y hora del backup, además se indica la cantidad de registros de las tablas de base de datos en el rotulo de caja del cd.

11 Se restaura el archivo datacarddmmaaaa.zip en otro computador que tenga instalado el programa DATACAR, borrando previamente, la carpeta "datos" de este nuevo computador.

12 Se descomprime en el nuevo computador el archivo datacarddmmaaaa.zip, proveniente de uno de los cd.

13 FORMATO DE CONSTANCIA

REVISADO:	APROBADO:	FECHA ULTIMA ACTUALIZACION:

NORMAS

1.	El Auxiliar de Sistemas es responsable por el mantenimiento de Backups semanales.
2.	El Analista de Tesorería es el encargado de la custodia de los backups en la caja fuerte hasta que se ordene su destrucción.
3.	

FORMATO CONSTANCIA COPIA DE SEGURIDAD

Fecha de Backup:	Hora Inicio:
Nombre del Administrador:	Hora Final:
Cantidad de Registros:	
Nombre Archivo .ZIP (datacarddmmaaaa.zip):	

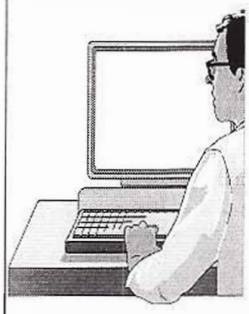
Observaciones:

Firma quien realiza Respaldo:

SUBOCOL S.A. VEHICULOS & REPUESTOS	GESTION DE SISTEMAS CUSTODIA DE COPIAS DE RESPALDO	Código: 010002 Página: 1 de 2

OBJETO

✪ Asegurar la integridad de la información para prevenir cualquier tipo de eventualidad que se presente.

AREA	RESPONSABLE	FLUJOGRAMA
DIRECCION DE SISTEMAS	 ANALISTA DE DESARROLLO	1 Semanalmente genera como mínimo trescopias del Backup de archivos establecidos por Cada una de las áreas de Subocol S.A. Este backup lo efectúa junto con el usuario del sistema correspondiente. ↓ Certificación del Backup 2 ↓ 3 Informa al Director de Sistemas que el backup ha sido efectuado y elabora el *FORMATO DE CONSTANCIA* para proceder a la entrega del backup para ser guardado en la caja fuerte.
DIRECCION ADMINISTRATIVA Y FINANCIERA	 ANALISTA DE TESORERIA	↓ 4 Recibe del Auxiliar de Sistemas los backups efectuados, firma el FORMATO DE CONSTANCIA y los guarda en la caja fuerte. ↓ 5 FORMATO DE CONSTANCIA

REVISADO:	APROBADO:	FECHA ULTIMA ACTUALIZACION:

SUBOCOL S.A. VEHICULOS & REPUESTOS	GESTION DE SISTEMAS CUSTODIA DE COPIAS DE RESPALDO	Código: 010002 Página: 2 de 2

OBJETO

- Asegurar la integridad de la información para prevenir cualquier tipo de eventualidad que se presente.

NORMAS

1.	El Auxiliar de Sistemas es responsable por el mantenimiento de Backups semanales.
2.	El Analista de Tesorería es el encargado de la custodia de los backups en la caja fuerte hasta que se ordene su destrucción.
3.	

FORMATO CONSTANCIA COPIA DE SEGURIDAD

Fecha de Backup:	Hora Inicio:
Nombre del Administrador:	Hora Final:
Cantidad de Registros:	
Nombre Archivo .ZIP (datacarddmmaaaa.zip):	

Observaciones:

Firma quien realiza Respaldo:

REVISADO:	APROBADO:	FECHA ULTIMA ACTUALIZACION:

SUBOCOL S.A. VEHICULOS & REPUESTOS	GESTION DE SISTEMAS POLITICAS PARA RESPALDO DE ESTACIONES	Código: 010003 Página: 1 de 1

OBJETO

✪ Asegurar la integridad de la información para prevenir cualquier tipo de eventualidad que se presente.

- El usuario Administrador debe ser quien realice el respaldo de la información de la estación de trabajo del usuario que lo solicite.
- Esto debe estar soportado a través de un FORMATO DE SOLICITUD DE BACKUP PARA ESTACIONES, donde debe aparecer la fecha de solicitud, nombre de quien solicita el respaldo de la información, cargo de quien solicita el respaldo de la información, área a la que pertenece, Nombre de quien realiza el respaldo, cargo de quien realiza el respaldo, firma de quien realiza el respaldo y firma del usuario donde confirma la realización del backup. En este formato debe haber un campo donde se escriba cualquier anomalía durante la copia o si no se pudo realizar el respaldo explicar el por que. Este formato debe ser diligenciado por la persona que solicita el backup y entregarlo al Auxiliar de Sistemas.
- Debe hacerse cada vez que el usuario lo solicite.

FORMATO SOLICITUD RESPALDO ESTACION DE TRABAJO

Fecha de Solicitud:	Hora Inicio:
Nombre del Solicitante:	Hora Final:
Cargo del Solicitante:	
Area del Solicitante:	

Nombre del Administrador:

Observaciones:

Firma quien realiza Respaldo:

Firma quien recibe a satisfacción:

REVISADO:	APROBADO:	FECHA ULTIMA ACTUALIZACION:

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

Se debe implementar un cronograma de copias de respaldo por días, en donde identifique cronológicamente el nodo, tipo de backup a realizar y su respectiva hora.

Se debe implementar una planilla de verificación de la realización de las copias de respaldo en donde se chequea que las copias programadas se realizaron a la hora indicada, si por alguna razón no se realizaron, asentar las respectivas observaciones, así como asentar el resultado de la verificación de las copias de respaldo y/o anotar casos especiales o errores en la verificación.

Se debe establecer una revisión periódica de las cintas de respaldo seleccionando medios al azar, con el propósito de chequear tanto el estado de la información almacenada como el estado del medio.

Se tiene que realizar una prueba de recuperación de las bases de datos de SUBOCOL S.A. en un sitio alterno mínimo una vez al año, con el propósito de identificar los requerimientos, afinar los procedimientos de recuperación, identificar y minimizar el tiempo de recuperación de las bases de datos.

Se debe implementar un esquema en donde los usuarios que componen el sistema de copias de respaldo, se configuren con los perfiles necesarios para ejecutar su tarea sin tener permisos que les permitan modificar, actualizar o borrar objetos propios del sistema operativo como de la base de datos.

Se tiene que restringir los permisos de los directorios y archivos que componen el sistema de copias de respaldo en donde solamente puedan ser ejecutados y leídos por los usuarios del sistema de copias de respaldo. Esto solo deben tener acceso el usuario Administrador; se deben quitar todos los permisos para el resto de los usuarios.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

- No lo use para resolver temas complejos. El correo electrónico es para transmitir información, no es muy bueno para resolver problemas complejos, ya que la comunicación y la retroalimentación son lentas y algo limitadas.

- No participe en cadenas de cartas o cosas por el estilo. Este tipo de mensajes consumen recursos de red y de correo que son costosos, adicionalmente lo distraen del trabajo. Este tipo de correos son usados para recoger direcciones de correo y luego usarlas para el envío de mensajes de propaganda o mensajes de todo tipo; También son muy usados para propagar virus.

- No se enoje por correo electrónico. Todos hemos enviado y recibido "mensajes fuertes" y también hemos deseado poder revertirlos. La razón es muy simple; es mucho más fácil enojarse de verdad con un monitor que con una persona con sentimientos que tiene una respuesta y que puede resolver nuestros problemas. En realidad es más fácil, pero es un desperdicio de energía.

- Los conflictos son normales dentro del trabajo en equipo. Los conflictos por correo electrónico son una perversión de la tecnología.

- No envíe mensajes obscenos. Consideren que a cualquiera puede molestarle.

- No use el correo electrónico para pedir donativos, para vender, para realizar promociones, para obras de caridad, para mensajes políticos, para mensajes subliminales, presentaciones de temas sin interés, mensajes religiosos, chistes, cadenas etc. o de cualquier otro tipo que no tenga relación con el trabajo en la compañía. Si usted es victima de este tipo de mensajes por favor informe a la cuenta del administrador del mail.

- No trate de concertar citas o reuniones por el correo electrónico que se vayan a llevar a cabo dentro de las próximas 24 horas. Todos vivimos muy ocupados y recibimos mucho correo, y si bien es nuestra obligación ver el correo, tampoco lo tenemos que estar viendo todo el tiempo. Así que si quieren reunirse con alguien o cambiar una cita dentro de un período menor de 1 día use el teléfono o contacte personalmente a los involucrados.

- Identifique claramente la persona a la cual le enviara el correo verifique que es la persona que necesita, recuerde que existen nombres parecidos u homónimos.

- Piense bien a quién va a enviar un mensaje. Use la lista más pequeña que sea posible. No conteste "Responder a Todos" a no ser que sea estrictamente necesario!!!.

OBJETO

- Ayudar al usuario a usar el correo electrónico adecuadamente.

- Cuando sea necesario enviar mensajes a un grupo amplio de destinatarios, adicione el siguiente texto al final del mensaje: "FAVOR NO RESPONDER A ESTE CORREO", si el mensaje no debe ser respondido. En el caso en que el mensaje deba ser respondido adicione: "EN CASO DE RESPONDER ESTE MENSAJE, POR FAVOR HÁGALO SOLO AL REMITENTE Y NO A TODAS LAS PERSONAS".

- Si el mensaje requiere de acción por parte de alguien en específico, diríjalo a esa persona. Ponga los demás nombres en la lista de "Cc:" (Con copia CC).

- Utilice el campo CCO (Con copia Oculta), cuando se envíe o se responda un mensaje que incluya direcciones por fuera de la compañía. También, cuando envíe mensajes que incluyan muchas personas o grupos corporativos. Esto con el fin de no publicar las direcciones de correo al exterior y que después seamos saturados de correos con basura

- Utilice con prudencia las listas de direcciones. No envíe copias de correo electrónico a personas que no necesitan ese mensaje.

- Actualice con frecuencia su libreta personal de direcciones, grupos personales y contactos.

- No envíe correos masivos sin importancia, con asuntos personales o que no tienen relación con el trabajo, este tipo de mensajes molestan y hacen perder tiempo a quienes van dirigidos.

- Los mensajes masivos deben ser enviados, en horario no hábil. 6:00 PM a 7:00 AM y de 12:00 M a 1:00 PM. Recuerde que EL PROGRAMA DE CORREO le permite programar estos envíos.

- No envíe correos (ni internos ni externos) en los cuales se hable mal de la competencia.

- No envíe información confidencial de la compañía o de los clientes por este medio.

- Cree grupos personales de usuarios en su libreta de direcciones o contactos, para que la comunicación se realice sólo entre las personas afines a su actividad.

- Consulte regularmente su buzón y recuerde que es su responsabilidad hacer copias de seguridad al archivo de mensajes (Carpetas personales que se encuentran en el disco de su computador), para evitar perdidas de información en caso de daños en los computadores. (Una vez por semana ó cuando crea que puede perder información importante).

- Realice mantenimiento periódico de su buzón de mensajes y del archivo de carpetas personales(Las que se encuentran en el disco duro de su computador).Borre con frecuencia los mensajes de correo que ya no le son útiles. Por ejemplo borre los mensajes de la "Bandeja de Entrada", "Elementos Eliminados" y "Elementos Enviados" de su buzón.

OBJETO

- Ayudar al usuario a usar el correo electrónico adecuadamente.

- No mantenga muchos mensajes en la Bandeja de entrada de su Buzón. Ud. debe tener el menor número posible de mensajes en la Bandeja de entrada, cree carpetas personales y mueva los mensajes de la Bandeja de entrada a estas carpetas. Puede organizar estas carpetas, por temas, por labores, por proyectos, mensajes pendientes etc.

- Procure que su mensaje no sea mayor de dos pantallas. Organice su mensaje y use "viñetas ", Colores, tipos de letra cuando sea posible.

- Ponga Un asunto claro y elocuente. Así como un libro necesita un buen título, un mensaje de correo electrónico necesita una línea de asunto. Si el mensaje es extenso, indíquelo en el encabezado, Si hay una fecha en juego, póngala en la línea del asunto. Eso ayudará a fijar el nivel de precisión y urgencia adecuado. Si hay un lugar, especifíquelo.

- Dígale al destinatario qué quiere. Una vez diga de qué se trata el mensaje, cuéntele lo que espera que el destinatario haga: ¿Confirmar la fecha? ¿Leer el plan de negocios? ¿Hacer correcciones al informe?. También diga la fecha para la que espera la respuesta. Por supuesto, siempre será tan pronto como sea posible, pero es mejor ser específico al respecto: "Entre más pronto, mejor, pero lo necesito a más tardar el jueves"

- Ejercite el buen gusto, sea respetuoso. Una cuenta de correo electrónico no es una licencia para abusar u ofender a la gente.

- Sea Breve. Debe pensar en el tiempo del destinatario y en los costos de la comunicación. Los mensajes funcionan mejor si son cortos y van al grano.

- Describa brevemente quién es usted, si el destinatario no lo sabe todavía. Utilice una firma, casi todos los programas de correo le permiten crear una. Se trata de un pequeño bloque de texto que se incorpora automáticamente a los mensajes que envía. Su objetivo es darle a la gente una idea de quién es usted: nombre, empresa, cargo, teléfono (si quiere que la gente lo tenga); Considérela como su tarjeta de presentación virtual.

- Tenga conciencia de que el correo electrónico puede ser archivado y bajo ciertas circunstancias no ser confidencial.

- No exagere. Evite los mensajes marcados como "urgentes " o "prioritarios", a menos que en realidad lo sean.

- Emplee las letras mayúsculas con prudencia. Cuando alguien utiliza mayúsculas en todo un mensaje, muchas personas perciben que está gritando, además es más difícil de leer.

- Evite responder a los mensajes con palabras como: "OK", "LISTO", "ENTERADO". Tómese el respeto de redactar una respuesta apropiada siempre y cuando el mensaje lo amerite

- Si va a disfrutar de su periodo de vacaciones o se va a ausentar de su puesto por varios días, delegue en otra persona la lectura de su correo, haga uso de las herramientas que para esto tiene su cliente de correo.

OBJETO

- Ayudar al usuario a usar el correo electrónico adecuadamente.

- No envíe documentos o imágenes adjuntos mientras no sea estrictamente necesario, ya que estos utilizan muchos de los recursos del sistema y son de mayor dificultad para leer.

- Limite el número de archivos anexos. Los archivos anexos (attachments) son útiles para enviar documentos largos en formatos específicos, pero no son un sustituto para el texto de un mensaje. Toma cierto tiempo abrir un anexo; con frecuencia, el destinatario prefiere revisar el siguiente mensaje y dejar el archivo anexo para más tarde. Si usted envía uno de estos documentos, asegúrese de explica qué es: ¿un comunicado de prensa? ¿sobre qué? ¿un plan de negocios, una hoja de vida. Finalmente, los archivos anexos pueden llevar virus.

- Cuando envíe documentos adjuntos, estos deben ser en los programas estándares de la compañía: Works, Word, Excel y Power Point. Sólo envíe en otros programas en casos específicos y cuando este seguro que la

- persona a la que se lo envía tiene estos programas. Procure siempre enviar los documentos del menor tamaño posible, haga uso de los programas que comprimen el tamaño de los archivos.

- Por seguridad y para evitar el contagio de virus, las siguientes extensiones están restringidas para el ingreso y salida de mensajes de Internet: VCBS, MP3, CHM, SCR, EXE, SHS, OCX, HTA, BMP, PIF, DLL, VCF, GIF, BAT, INI, HTR, AVI, COM, INF, HTT, PPS.

- Ninguna dependencia esta autorizada para instalar en sus equipos programas de correo electrónico diferentes a los corporativos. Actualmente el programa de correo electrónico autorizado es Outlook Express y Microsoft Outlook.

- No se permite modificar en el correo electrónico nada que afecte la configuración de la cuenta (Nombre del servidor, Nombre de la cuenta, entrega de mensajes, el tipo de conexión y la seguridad del inicio de sesión)

Llevar todo esto a la práctica nos ayudará a trabajar más eficientemente, nos hará sentir mejor y obtendremos mayores ventajas de la herramienta que poseemos:"El correo electrónico".

Agradecemos tomar atenta nota de estas indicaciones.

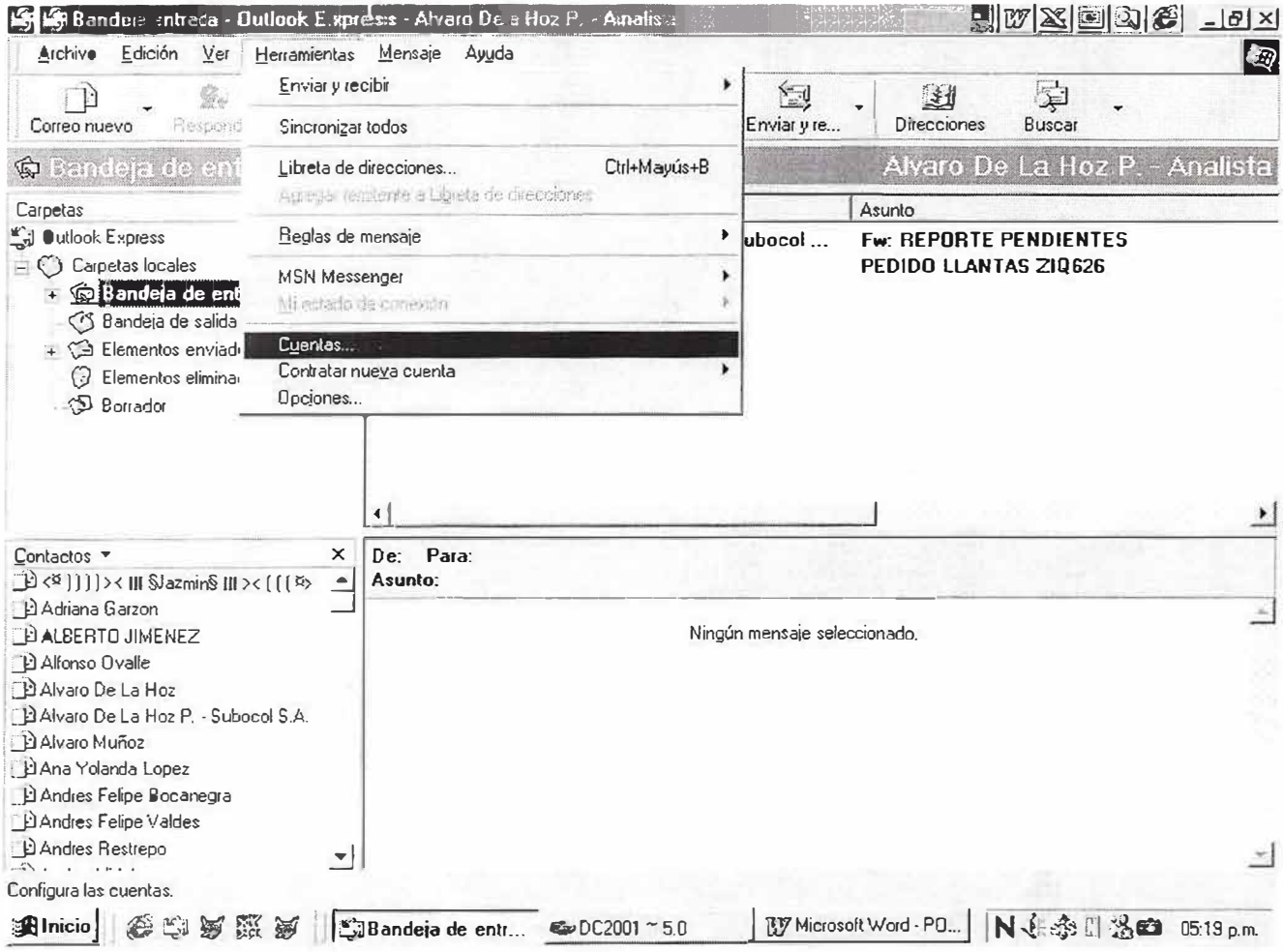
SUBOCOL S.A. VEHICULOS & REPUESTOS	AREA DE SEGURIDAD DE TECNOLOGIA NORMAS, POLITICAS Y RECOMENDACIONES PARA LA CONFIGURACION DE EQUIPOS PARA EL USO DE CORREO ELECTRONICO E INTERNET	Código: 020002 Página: 1 de 10

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

Para configurar la cuenta de correo en un computador se deben hacer los siguientes pasos:

- Abrir el programa de correo Outlook Express y escoger la opción Herramientas / Cuentas.

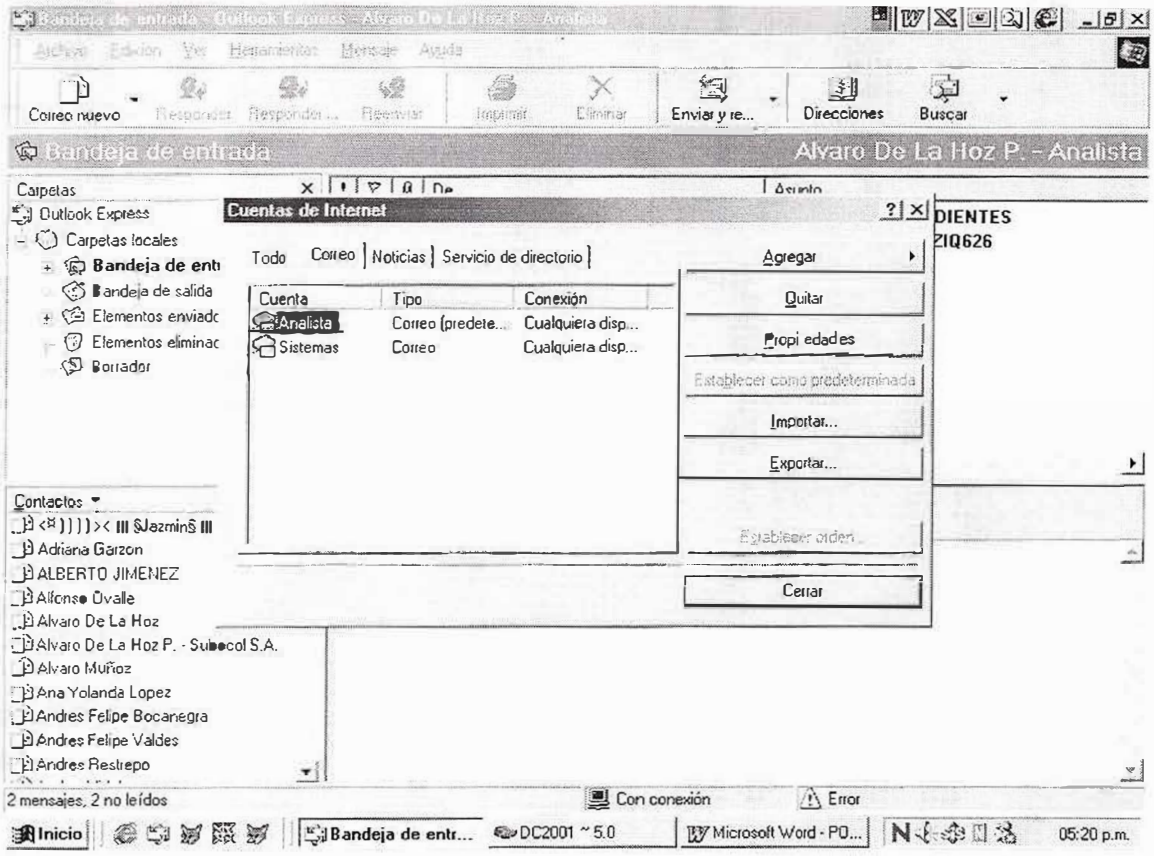


REVISADO:	APROBADO:	FECHA ULTIMA ACTUALIZACION:

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

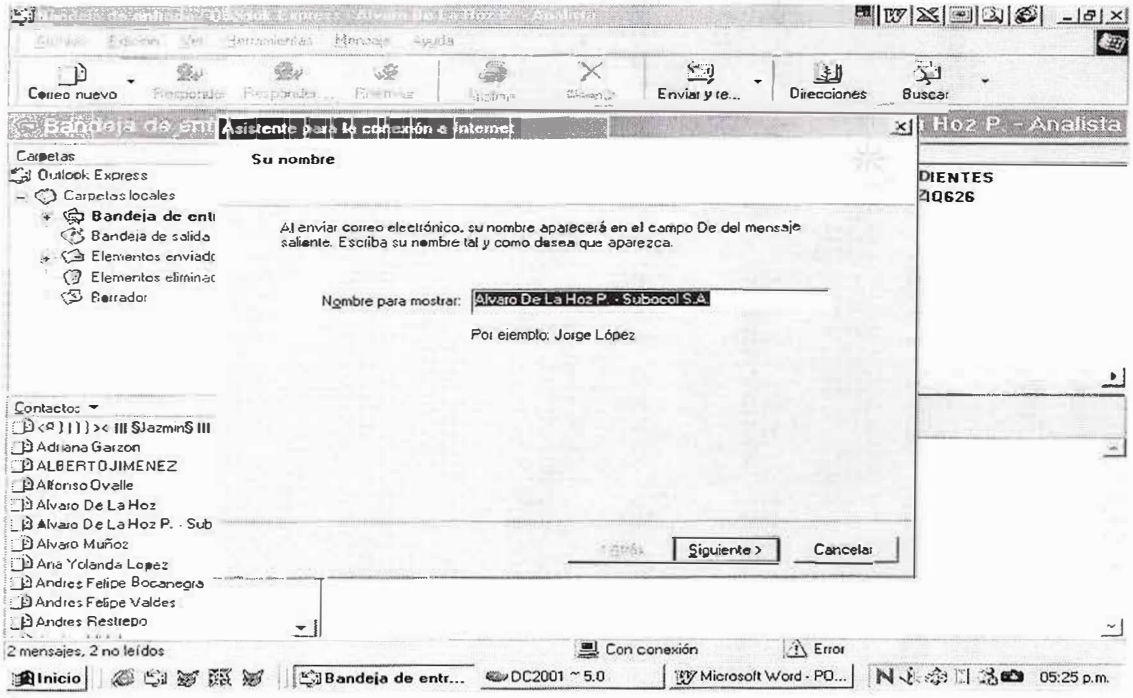
- Al dar click a la opción Cuentas, aparece el siguiente cuadro:



DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

➢ Dar click al botón Agregar, Escoger la opción Correo y aparece el siguiente cuadro:

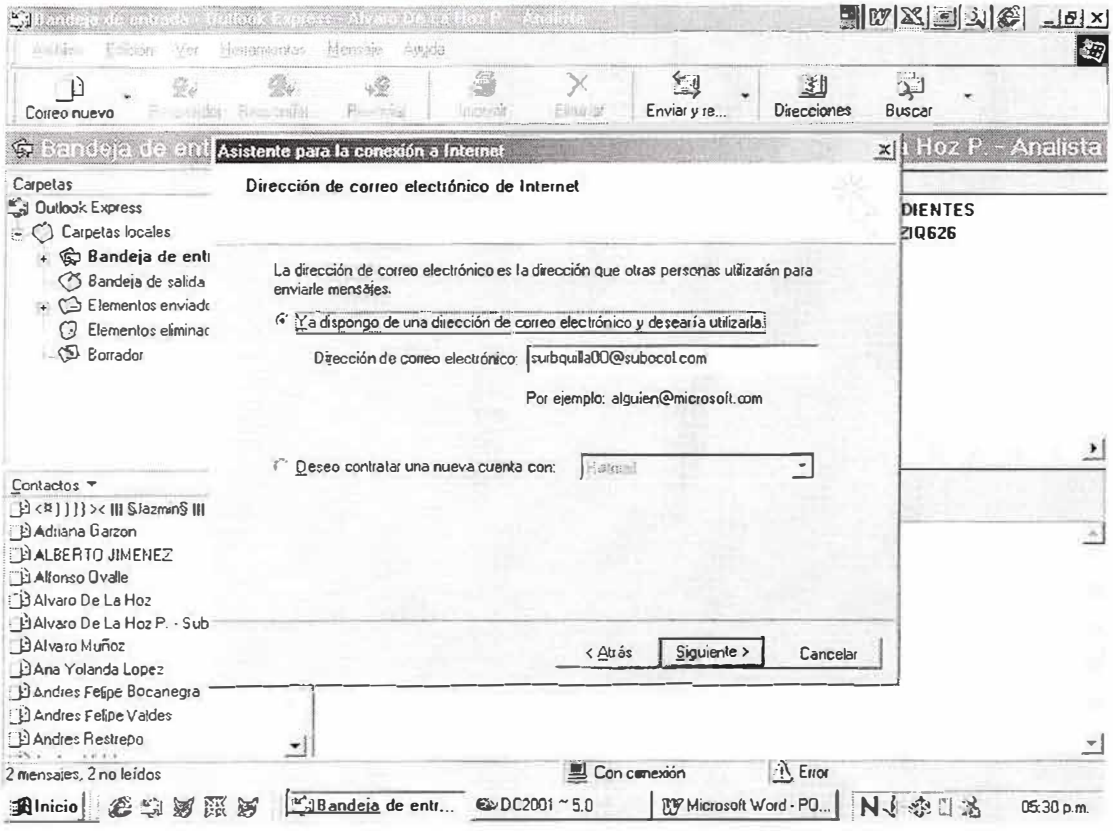


REVISADO:	APROBADO:	FECHA ULTIMA ACTUALIZACION:

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

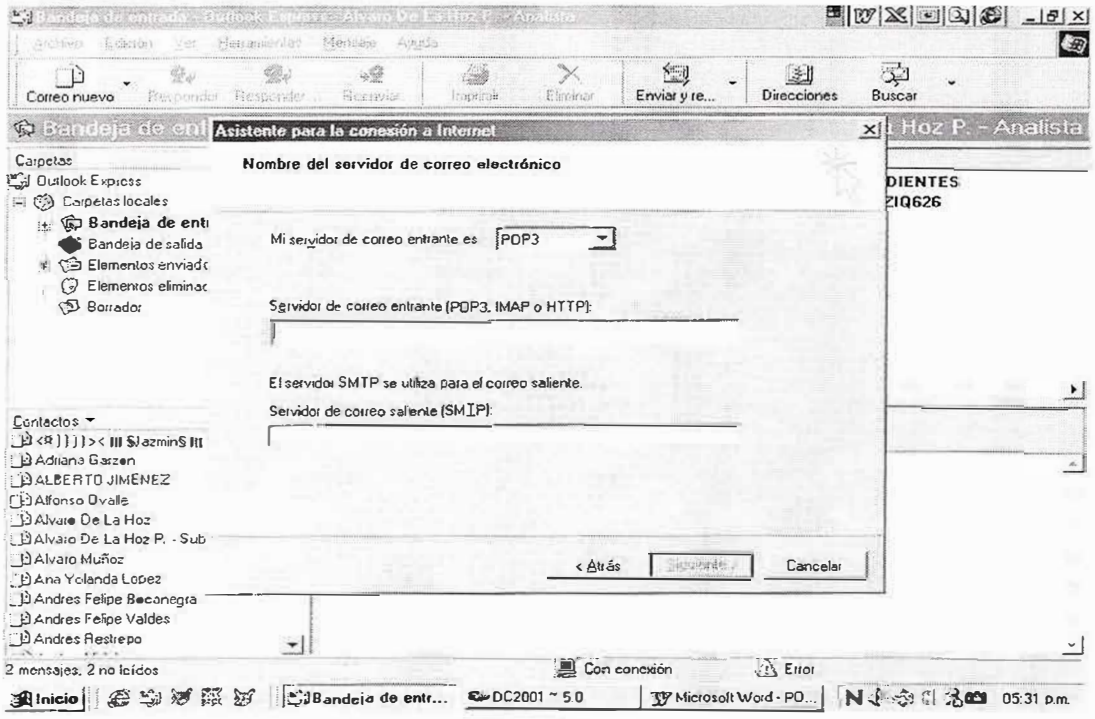
- En el recuadro debe escribir el Nombre para Mostrar cuando envíe un Mensaje. (p.e. Pedro Pérez – Subocol S.A.) y dar click en el botón Siguiente, y aparece la siguiente ventana:



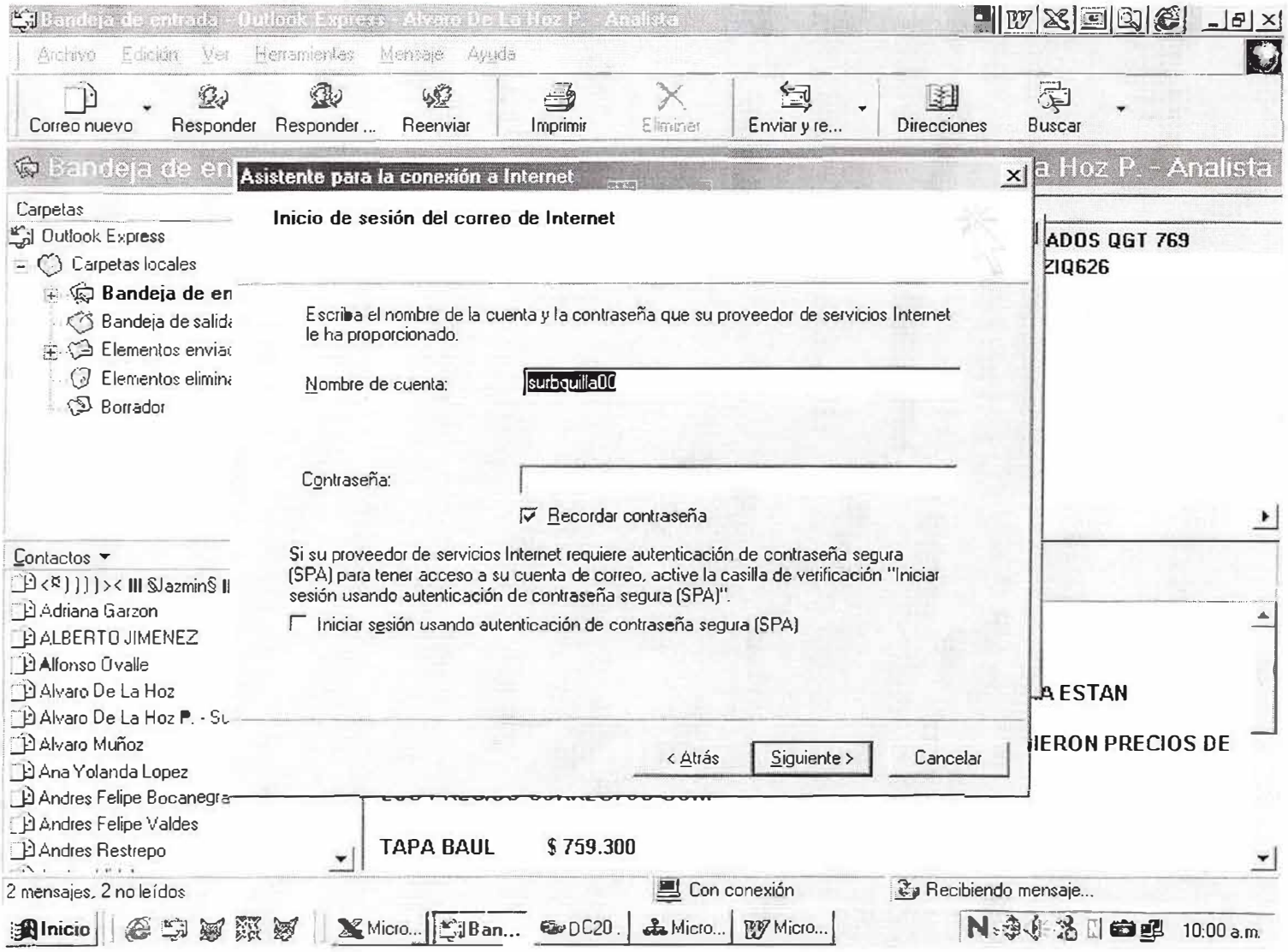
DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

- Debe escribir la cuenta de correo electrónico y dar click en el botón siguiente y aparece el siguiente recuadro:



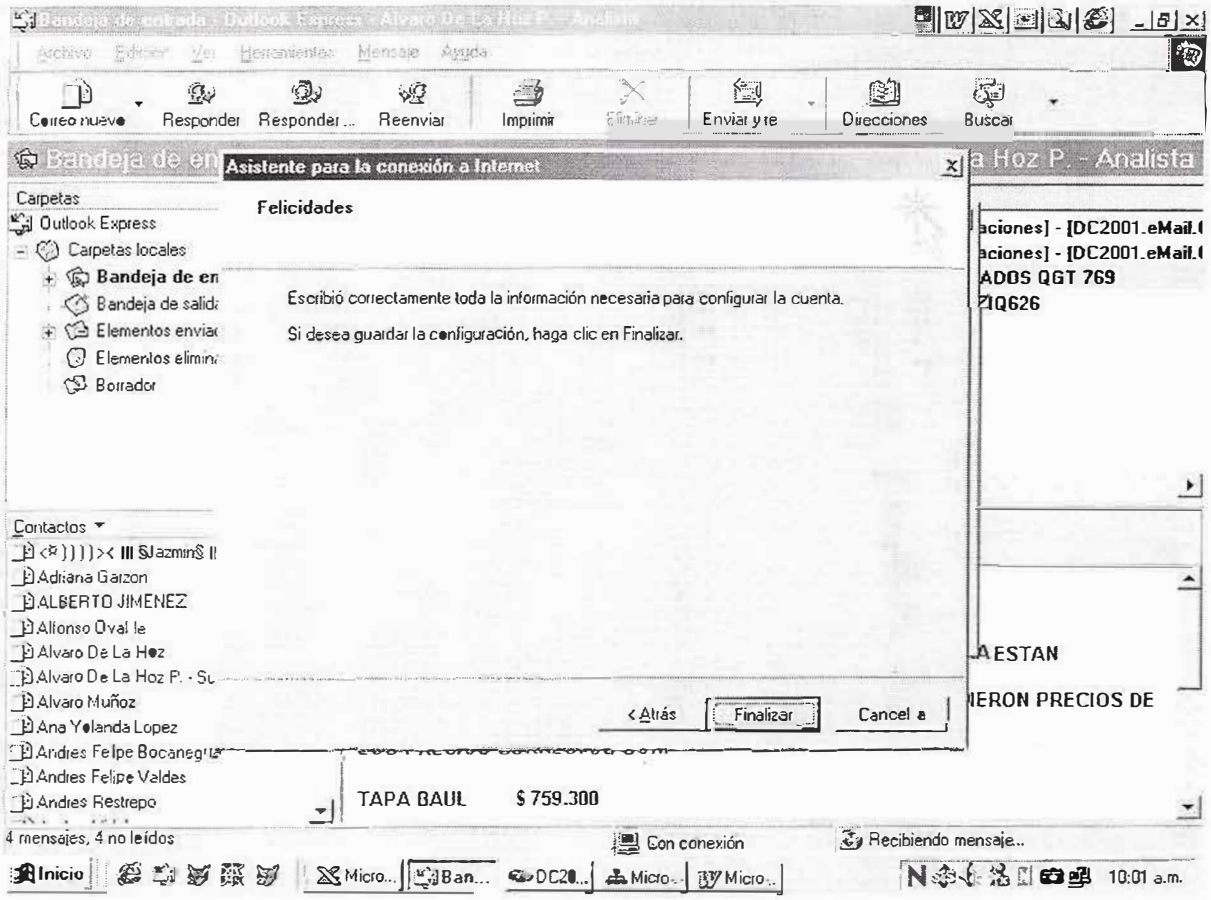
- Luego escribir el servidor POP3 y servidor SMTP en el recuadro correspondiente, y dar click en siguiente y aparece la siguiente ventana:



DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

- Configura el Inicio de Sesión para que le permita bajar el correo, coloca el nombre de la cuenta y su contraseña y presiona el botón siguiente, luego aparece la ventana:



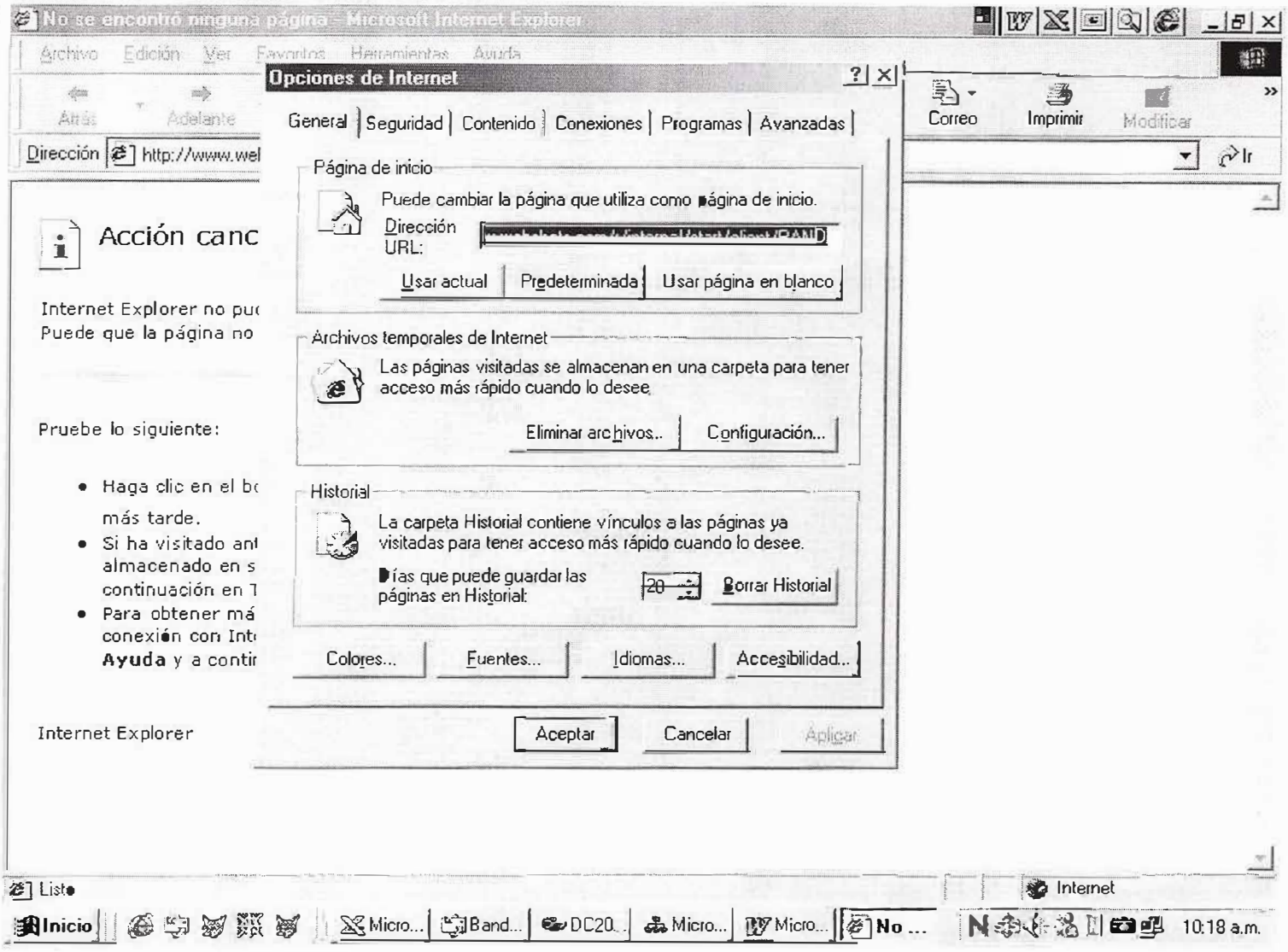
- Donde presiona el botón Finalizar, y lo regresa al pantallazo inicial donde presiona el botón Cerrar y queda configurada la cuenta de correo.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

Para configurar el acceso a Internet se deben hacer los siguientes pasos:

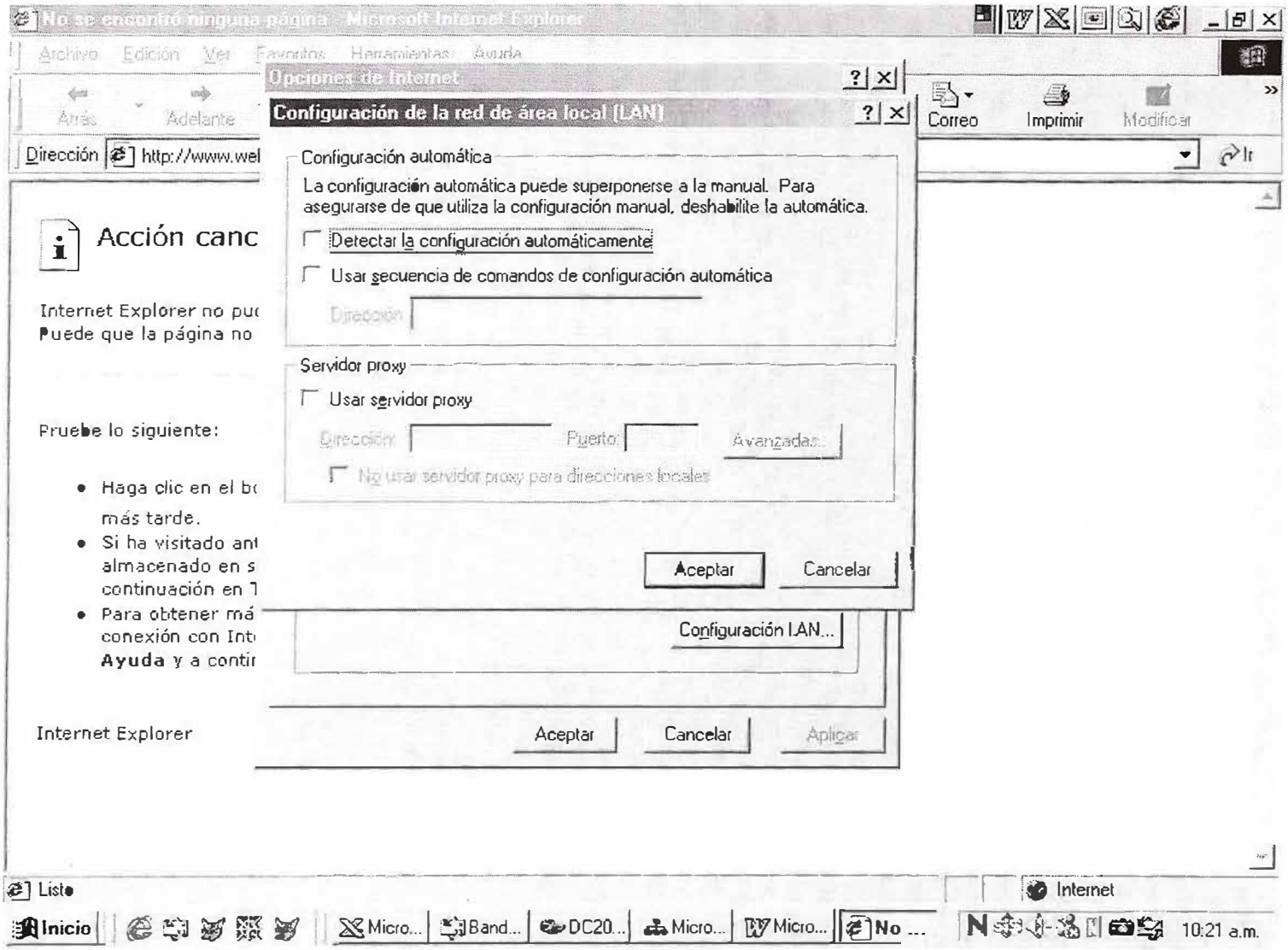
- Abrimos Internet Explorer, seleccionamos del Menú Herramientas la opción Opciones de Internet:



DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

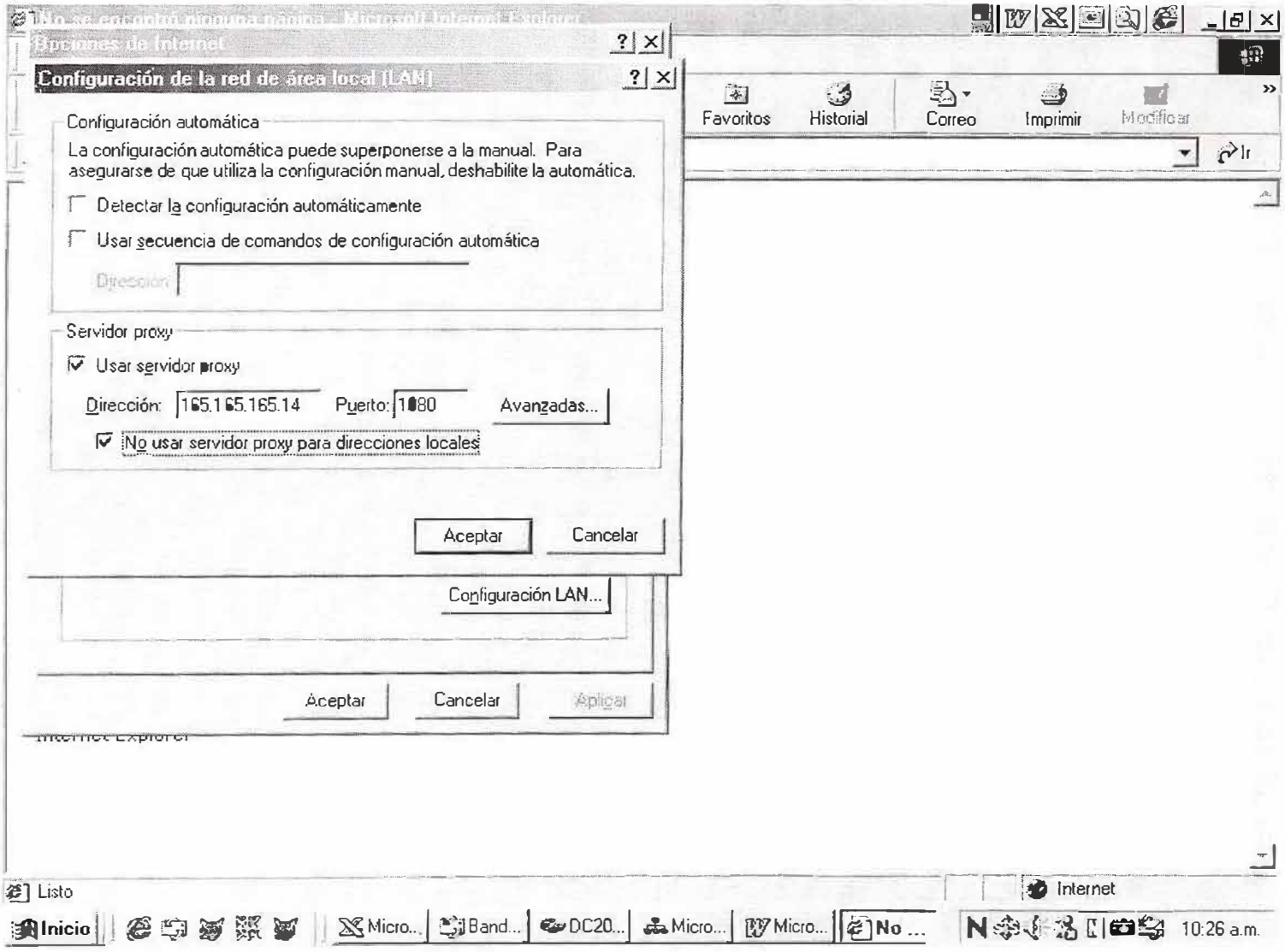
- Luego seleccionamos la pestaña Conexiones y presionamos el botón Configuración LAN, apareciendo la siguiente ventana:



DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

- El el Recuadro Servidor Proxy, chuleamos la casilla de verificación para que nos permita digitar la dirección IP del Proxy y el número del puerto. (p.e. Dirección: 165.165.165.14 Puerto: 1080). Y damos click en la casilla de No Usar Servidor Proxy para Direcciones Locales y presionamos el botón Aceptar, quedando configurado el acceso a Internet.



DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

En un mundo dominado por la tecnología informática la aparición de ataques a los sistemas de información es cada vez mayor. Esto se ha vuelto una lucha codo a codo entre los que defienden sus datos y sistemas y entre los que buscan la puerta que se deja abierta para entrar y causar los daños mas insospechados. Pero estos ataques no solo se pueden esperar desde el exterior, gran parte de ellos se originan al interior de las empresas. Esto hace que el tomar conciencia acerca de lo vulnerables que podamos ser sea algo de gran importancia y la búsqueda e implementación de soluciones sea un aspecto de considerable urgencia.

Las soluciones a estos problemas deben comenzar a partir de los recursos con los que se cuente, tanto humanos como técnicos, y su implementación debe darse a partir de políticas claras de seguridad y procedimientos que se diseñen para enfrentar las diversas vulnerabilidades que poseamos y las que en algún momento puedan surgir.

En este documento abarcaremos el tema de seguridad en la administración de usuarios, el cual en el momento es una de nuestras grandes vulnerabilidades dada su administración tan dispersa y por la multiplicidad de plataformas y modelos de seguridad. Con este compendio de políticas y procedimientos haremos el máximo esfuerzo por estar un paso adelante de los posibles ataques a los cuales podamos estar expuestos, estableciendo normas y especificando la forma en que debemos proceder con la administración de usuarios para evitar ser vulnerables.

Este debe ser un compromiso de toda la Gerencia de Informática, la cual debe poner en disponibilidad todo su recurso humano y técnico para ayudar en el cumplimiento de las políticas y procedimientos que a continuación proponemos.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

CONTROL DE ACCESO

- Se debe prevenir el acceso no autorizado a todos los ambientes disponibles (Red, correo, C/S, Web, bases de datos) mediante la definición de perfiles, usuarios y privilegios especiales.

- Todo usuario utilizado en cualquiera de los recursos informáticos de software con los que cuenta actualmente la compañía debe estar asociado a un perfil

- Los perfiles deben definir el alcance o tipo de información a la cual los usuarios asociados tengan acceso.

- Debe exigirse que todo recurso informático de software que adquiera la compañía y el cual esté orientado al manejo de información del negocio tenga en el aspecto de seguridad como mínimo un manejo de usuarios y perfiles de usuarios.

ADMINISTRACIÓN DE ACCESO DE USUARIOS

- Los procedimientos declarados en este documento se deben emplear para controlar la creación de usuarios, la asignación de derechos de acceso a los sistemas de información y servicios y para su eliminación y depuración.

- La elaboración de nuevas políticas y procedimientos para la administración de usuarios debe contar con la aprobación del área de Seguridad de Tecnología

- Todo cambio en el contenido de este documento será manejado y estará bajo responsabilidad del área de Seguridad de Tecnología

REGISTRO DEL USUARIO

- No deben existir usuarios compartidos ni genéricos
- Todo usuario debe tener autorización del dueño del sistema o servicio para su uso.
- Cuando se tome la decisión de contratar un nuevo empleado en la compañía se debe solicitar con anterioridad al Auditor de servicios la instalación del equipo y la creación de los usuarios que requeriría el nuevo empleado (usuario de red, usuario de correo, usuarios de aplicación), diligenciando el formato establecido para tal fin. Esto permite agilizar el proceso de adecuación tecnológica y creación de usuarios oportunamente.
- Se debe tener un registro formal de los usuarios habilitados a ingresar a un servicio específico y de los privilegios especiales asignados.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

ADMINISTRACIÓN DE PRIVILEGIOS ESPECIALES

- Los privilegios sobre una plataforma que soliciten ser asignados a un usuario deben hacerse solamente sobre la base de necesidad de uso, especificando el tiempo que requerirá los privilegios solicitados y adjuntando su respectiva justificación.
- Debe mantenerse un procedimiento para la autorización y registro de privilegios adicionales.
- Estos privilegios no deben ser asignados hasta tanto no se halla cumplido con este procedimiento.
- Solo usuarios autorizados (con perfil de administradores) pueden modificar o inhabilitar las funciones de seguridad del sistema.

ADMINISTRACIÓN DE CONTRASEÑAS DE USUARIO

- Exigir que las contraseñas temporales deban ser suministradas a los usuarios de una manera segura. El uso de terceras personas o mensajes de correo electrónicos desprotegidos deben evitarse. Los usuarios deben confirmar el recibo de dichas contraseñas vía mail o telefónicamente al Auditor de servicios.
- En la medida que la plataforma lo permita, obligar a que la contraseña sea cambiada cuando se registre el primer ingreso.
- Una contraseña debe tener un tamaño mínimo de 6 caracteres. Esto en la medida que la plataforma lo permita
- Cada plataforma no debe permitir repetir las últimas 5 anteriores contraseñas. Esto en la medida que la plataforma lo permita

REVISIÓN DE DERECHOS DE ACCESO DE USUARIOS

- Cada 2 meses se hará una verificación de la lista de usuarios de un servicio o aplicativo determinado seleccionado dentro de los considerados como críticos para el negocio. Para esto se contará con la ayuda del usuario o analista dueño respectivo, En la verificación se determinará, mediante la toma de una muestra representativa del total del usuarios, si efectivamente se encuentran activos y/o tienen asignado el perfil que les fue autorizado y/o tienen los privilegios especiales asignados autorizados. Cualquier inconsistencia se documentará para luego tomar los correctivos respectivos.

RESPONSABILIDADES DEL EMPLEADO

- IMPORTANTE: Estas responsabilidades tienen relación al manejo que todos los empleados deben hacer de los usuarios que posean para el acceso a servicios/aplicaciones ofrecidos por la compañía. Las responsabilidades generales con todos los servicios informáticos deben ser consultadas en el documento de políticas generales

- Se debe prevenir el acceso de usuarios no autorizados a los ambientes disponibles.
- Debe exigirse a los empleados que se comprometan a guardar confidencialmente las contraseñas personales y de trabajo y que las contraseñas de grupo permanezcan solamente dentro de los miembros de dicho grupo.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

- Los usuarios deben tomar conciencia acerca de las responsabilidades que tienen en la conservación de controles de acceso eficaces, particularmente con respecto al uso de contraseñas y la seguridad de su equipo.
- Cuando el Auxiliar de Sistemas le confirme a un empleado la creación de un usuario específico o la asignación de privilegios adicionales, se le deberán explicar claramente sus obligaciones como usuario del ambiente asignado.
- Cumplir con los procedimientos establecidos para la solicitud de creación o eliminación de usuario en cualquiera de las plataformas, al igual que para la autorización de privilegios adicionales.

USO DE LA CONTRASEÑA

- Las contraseñas o mecanismos de acceso que les sean otorgados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ningún tercero tanto al interior como al exterior de la compañía.
- Se prohíbe el uso no autorizado de usuarios o contraseñas.
- Los empleados son responsables de todas las actividades llevadas a cabo con su código de usuario y contraseñas personales.
- Los empleados deben evitar guardar un registro de sus contraseñas en papel o en algún medio o documento electrónico, a menos que esto puede guardarse en lugar seguro.
- Cambiar las contraseñas siempre que exista cualquier indicio de un posible compromiso del sistema o de las mismas contraseñas.
- Seleccionar contraseñas con una longitud mínima de seis caracteres que sean:

1. Fáciles de recordar.
2. Que no sean basadas en nada que alguien más pueda deducir fácilmente u obtener usando a una persona relacionada, por ejemplo nombres de familiares, números teléfónicos, fechas de nacimiento, nombres de animales u objetos comunes.
3. Que esté libre de caracteres idénticos consecutivos, evitar que contenga solo números o letras, se recomienda combinar números y letras.
4. No debe incluir los caracteres ñ, Ñ, vocales con tilde o diéresis, estos generan problemas de autenticación.
5. La clave de acceso no debe igual al nombre del usuario asignado.
6. Debe tener un tamaño mínimo de 6 caracteres. Esto en la medida que la plataforma lo permita.
7. No debe repetir las últimas 5 claves anteriores. Esto en la medida que la plataforma lo permita

- Los usuarios (no importando su nivel de alcance dentro de la plataforma y/o aplicativo al que están ingresando) y contraseñas son personales e intransferibles.
- En la medida que la plataforma lo permita, todos los usuarios de red, de aplicaciones C/S y Web deben pedir cambio de contraseña cada 3 meses de manera obligatoria en forma automática, pero el empleado lo podrá cambiar cuantas veces quiera.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

- Para los casos en que sea necesario realizar soporte a los empleados, el personal encargado de esto no podrá solicitar al empleado que le suministre sus claves de acceso para poder realizar el trabajo. Igualmente el empleado no debe suministrar sus claves de acceso por iniciativa propia.
- Está prohibido que el personal de soporte presten ayuda a empleados que suministren datos de usuario y clave que no sean las asignadas a ellos. Esto va contra la norma de que esta información es personal e intransferible.
- Los empleados deben estar atentos a evitar que personal ajeno a la compañía ingresen sin autorización a la red o a cualquiera de los recursos informáticos que esta posee.

EQUIPOS SIN VIGILANCIA

- Los usuarios deben asegurar que los equipos sin vigilancia tengan protección apropiada. Los equipos instalados en las áreas de trabajo, por ejemplo estaciones de trabajo o servidores, deben tener protección específica al acceso no autorizado cuando están sin vigilancia por un periodo extendido. Para esto deberá mantenerse activo el descansador de pantalla protegido por contraseña o el bloqueo de pantalla según lo permita el sistema operativo.
- Par a todo el personal es obligatorio debe tener activado el descansador de pantalla y protegido por contraseña. En este punto se debe tener en cuenta lo siguiente:

1. Para estaciones, el descansador debe activarse mínimo a los tres minutos.
2. Para servidores debe activarse inmediatamente la consola deje de utilizarse.

- Todo usuario debe terminar las sesiones activas cuando hallan acabado sus labores o cuando el trabajo deba ser suspendido por un largo período de tiempo y esto represente estar ausente de su puesto de trabajo.
- Todos los equipos deben tener activada su contraseña de arranque.
- En caso de que el usuario desconozca como activar el protector de pantalla protegido por contraseña o la contraseña de arranque del equipo, deberá contactar al Puesto de Ayuda para recibir instrucciones al respecto.

POLÍTICAS GENERALES DE USUARIOS

- La solicitud para hacer cualquier operación sobre los usuarios (creación, borrado, adición de privilegios adicionales, traslado, modificación de datos) debe hacerse por medio del formato. Podrán presentarse casos en los cuales las solicitudes se harán vía mail directamente al Auxiliar de Sistemas, pero esto solo es permitido hacerlo siempre y cuando esté especificado en el procedimiento respectivo.
- En toda solicitud debe especificarse la información que sea considerada como obligatoria, no debe aceptarse una solicitud hecha con datos parciales. Esta verificación debe ser hecha por la persona que reciba las solicitudes.
- Las solicitudes solo deben ser gestionadas por las personas autorizadas según indican los procedimientos respectivos. Toda solicitud hecha por una persona diferente no será atendida.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

- Algunos códigos de usuario no estarán activos para trabajar en las aplicaciones de la compañía fuera del horario de trabajo establecido. Esta inactivación debe ser definida y autorizada por el dueño de la aplicación especificando que tipos de usuarios tendrán esta restricción. En caso de requerirse activar un código de usuario de alguna aplicación para trabajar un fin de semana o en horas no laborales, éste debe ser solicitado con anterioridad por el gerente del área respectiva.
- Los códigos de usuario de las aplicaciones y de la red serán inactivados durante el tiempo en que el empleado este efectivamente en vacaciones o en licencia (periodos superiores a 30 días).
- En caso de que exista un reemplazo durante este tiempo, se debe solicitar un usuario temporal para el reemplazo por dicho tiempo, finalizado éste se eliminará el usuario temporal y se activará nuevamente el del empleado.

- El Puesto de Ayuda y el personal de soporte técnico y desarrollo en general no debe conocer las claves de acceso de los usuarios a cualquier plataforma.
- Deben asegurarse la existencia y revisión periódica de procesos para:

1. Creación de usuarios.
2. Asignación de privilegios especiales
3. Depuración de usuarios para eliminar usuarios que ya no trabajen para la compañía o hallan cambiado de área.
4. Eliminación de usuarios
5. Traslado de usuarios

- Todo usuario que valla a conectarse local o remotamente a recursos de la compañía deben pasar por al menos un proceso de autenticación.
- Para ingresar a la red y al correo siempre debe pasarse por un proceso de autenticación, es decir, se debe exigir un usuario y una clave de acceso.
- Al ingresar a la red se debe desplegar un mensaje informativo en el cual se le indique al usuario que el equipo y los recursos informáticos que va a comenzar a utilizar son exclusivamente para los objetivos del negocio. Debe tener claro que no puede utilizar estas herramientas para labores personales.

ESTANDAR PARA NOMBRAR UN USUARIO

- Todos los usuarios de red, Correo Electrónico y de aplicaciones C/S y Web deben cumplir con lo siguiente:

1. El usuario se define como las 4 primeras letras del nombre, las 2 primeras letras del primer apellido y para terminar las 2 primeras letras del segundo apellido. Por Ejemplo, si el usuario se llama Liliana Carvajal Montoya su usuario de red será LiliCaMo. Observe que las iniciales del Nombre y cada uno de los apellidos se escriben en mayúscula.
2. Si el primer nombre del usuario tiene 3 letras o menos se completan Cuatro caracteres con su segundo nombre, por ejemplo, para Luz Stella Botero Ospina el Logín Name sería LuzSBoOs.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

3. Si el empleado no tiene segundo apellido el usuario se complementa repitiendo las dos primeras letras del primer apellido, por ejemplo, para John Fredy Betancur, el usuario debe ser JohnBeBe.
4. En caso de que el usuario coincida con uno ya existente el último carácter del usuario se reemplaza por la primera consonante del segundo apellido, a partir del segundo carácter, por ejemplo, si el Login Name LiliCaMo ya existe y ahora debemos crear un usuario de red en el mismo contexto para Liliana Cadavid Molina, el usuario debe establecerse como LiliCaMl
5. La única excepción es cuando empleados no estén de acuerdo con el usuario asignado porque este puede resultar ofensivo.

➢ Se debe tener en cuenta los siguientes aspectos cuando sea necesaria la creación de usuarios genéricos:

1. No se permite la creación de usuarios genéricos, la definición del usuario de red se realiza a partir de los nombres y apellidos del usuario mismo, se debe evitar la creación de usuarios de red como TEMPORAL, CAJA1, ASESOR.
2. No se permite que un usuario tenga más de una conexión simultánea a la red, exeptuando al personal que por las labores definidas para su cargo obligue a que posea un usuario con mas de una conexión simultánea.
3. Para estos casos excepcionales se deberá tener en cuenta lo siguiente:

❖ Se deberá solicitar autorización al área de Seguridad de Tecnología para la creación de usuarios genéricos
❖ Cuando sea solicitado un usuario de este tipo se deberá incluir la justificación de su uso, además del empleado que será responsable del usuario, propósito de uso del usuario y fecha de creación.
❖ Esta información deberá quedar documentada en el campo "Descripción".

SUBOCOL S.A. VEHICULOS & REPUESTOS	AREA DE SEGURIDAD DE TECNOLOGIA NORMAS PARA LA ASIGNACION DE CONTRASEÑAS	Código: 020004 Página: 1 de 1

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

FORMATO PARA LA SOLICITUD DE USUARIOS
(Aplicaciones, Red, Correo, Web, Privilegios, Perfiles)

IMPORTANTE:

- Todos los campos en negrilla son indispensables para el trámite de la solicitud.
- Por favor relacione en aplicaciones o en ramos solamente lo nuevo que requiere.

Nombre completo usuario	
Cédula/NIT usuario o proveedor	
Código de nómina usuario (para personal contratado)	
Cargo/Proyecto	
Nombre Gerente o Ejecutivo Responsable	
Teléfono oficina	
Tipo de Contrato	
Fecha Fin Contrato (si aplica)	
Nombre de Oficina o dependencia	
Código de Oficina o dependencia	
Aplicaciones nuevas que requiere: Por ejemplo C/S, Web, Correo Electrónico, Red, Office, otras aplicaciones.	
Privilegios especiales: En la red, bases de datos, puertos especiales de salida a Internet, autorización de usuarios en horarios no permitidos, etc. **Coloque N/A en este campo si no necesita privilegios adicionales**	
Fecha expiración privilegios especiales	
Creación/Modificación perfiles (Detallar trabajo a realizar)	
Código de Identificación del Equipo o CPU	
Justificación:	
¿Ya posee usuario de red ?	SI Cual: NO

REVISADO:	APROBADO:	FECHA ULTIMA ACTUALIZACION:

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

FORMATO RESPUESTA CREACIÓN DE USUARIO O ASIGNACIÓN DE PRIVILEGIOS ESPECIALES

Sr/Sra

XXXXXXXXXXXXXX

El usuario es:
XXXXXXXX
Fecha expiración usuario:
XXXXXXXX
El cual tendrá acceso a:
XXXXXXXX
Las opciones activadas fueron:
XXXXXXXX
Los privilegios asignados fueron:
XXXXXXXX
Fecha expiración privilegios:
XXXXXXXX

- Recuerde que sus obligaciones y responsabilidades para el acceso a los servicios/aplicaciones de la plataforma informática de Subocol son, entre otros:

- El usuario, las claves de acceso (password) de red, correo, aplicativos o privilegios especiales que le fueron asignados son personales e intransferibles, usted es el único responsable de todas las actividades llevadas a cabo con su usuario y claves de acceso.

- Usted no debe informar a nadie de sus claves de acceso, esto incluye a compañeros de trabajo, personal de soporte (analistas, técnicos de IBM, agentes del Puesto de Ayuda, personal de mantenimiento de equipos)

- Debe evitar guardar sus claves de acceso escritas en papel. De ser necesario esto, por favor manténgalas en lugar seguro.

- Usted debe cambiar las claves de acceso cada que exista cualquier indicio de un posible compromiso del sistema o de las mismas contraseñas. Si desconoce el procedimiento para el cambio de sus claves de acceso por favor póngase en contacto con el Puesto de Ayuda. Adicionalmente puede encontrar un manual de apoyo en http://www.suranet.com/consulta/nws/index.htm.

DISEÑADO:

- Ing. ALVARO DE LA HOZ PEÑATE
- Ing. ORLANDO DUARTE ARCINIEGAS
- Ing. SIMON GOMEZ MEDINA

- Se recomienda que cada tres meses cambie sus claves de acceso. Para el caso de usuarios con privilegios de administración, el cambio debe ser cada 15 días

- Algunas recomendaciones para asignar claves de acceso:

1. Procure que sean fáciles de recordar, pero a la vez no deben resultar obvias.
2. Que no sean basadas en nada que alguien más pueda deducir fácilmente u obtener usando a una persona relacionada, por ejemplo nombres de familiares, números teléfónicos, fechas de nacimiento, nombres de animales u objetos comunes.
3. Que esté libre de caracteres idénticos consecutivos, evitar que contenga solo números o letras, se recomienda combinar números y letras.
4. No debe incluir los caracteres ñ, Ñ, vocales con tilde o diéresis, estos generan problemas de autenticación.
5. La clave de acceso no debe igual al nombre del usuario asignado.
6. Debe tener un tamaño mínimo de 6 caracteres. Esto en la medida que la plataforma lo permita.
7. No debe repetir las últimas 5 claves anteriores. Esto en la medida que la plataforma lo permita.

- Recuerde que toda solicitud de usuario nuevo, privilegios especiales, asignación o modificación de perfiles y opciones deben ser solicitadas en el formato. No se atenderán requerimientos solicitados por otros medios.

Cordialmente

Auxiliar de Sistemas – Subocol S.A.

Estándar para Servidor (Hardware y Software)

Servidor IBM Netfinity con 256 MB en RAM, Procesador Pentium IV de 1.8 Gigabytes con doble procesador, arreglo de tres discos de 40 Gigabytes cada uno, una tarjeta de red, Proxy Wingate de 50 usuarios. Swich 100 base T de 24 puertos, Concentrador 10 base T de 24 puertos, Cableado Estructurado de nivel 5 de voz y datos, UPS de 8 Kva y de 6 Kva, Protocolo TCP/IP con direcciones fijas, canal dedicado a 128 kbps. Debe tener como mínimo Windows 2000 para Servidor.

Estándar para Estaciones (Hardware y Software)

Compaq Deskpro con 128 MB en RAM, mínimo un Procesador Pentium III de 950 Mhz, Disco Duro de 40 Gigabytes, una tarjeta de red. Deben tener instalado Windows Workstation, Office 2000, Datacar 5.0. Outlook Express 5.0 o superior o Microsoft Outlook.

Un plan de contingencia es una lista ordenada de acciones a tomar ante la presencia de un siniestro (**Es la interrupción en el ciclo productivo de una organización, el cual le genera perdidas económicas)** o de una interrupción prolongada de las operaciones en el sistema de información.

OBJETIVO

- Proveer una solución para mantener operando las funciones que son fundamentales para la alta dirección de la organización, cuando son paralizadas por siniestros que afectan a la instalación computacional.

VENTAJAS

- El levantamiento de información efectuado permite determinar acciones preventivas, reduciendo el grado de vulnerabilidad y la exposición al riesgo.
- Permite dimensionar el riesgo potencial a que esta expuesta la organización.
- Permite tomar decisiones rápidamente ante anormalidades o fallas que se presenten en el centro de computo o en las comunicaciones.
- Contribuye a generar una mayor cultura de seguridad en la organización.
- Permite asegurar la estabilidad de la organización ante la presencia de un siniestro.

FACTORES QUE SE DEBEN CONSIDERAR EN EL DESARROLLO DEL PLAN DE CONTIGENCIA

- ¿Cuánto tiempo puede operar la organización sin su capacidad de procesamiento de datos?
- ¿Cuánto tiempo puede operar la organización sin el sistema en línea?
- ¿Cuáles son las amenazas potenciales a la capacidad de procesamiento de datos de la organización?
- ¿De que manera se pueden ver afectadas las comunicaciones entre oficinas y entre computadores?
- ¿En que debe invertir la organización para afrontar una contingencia que afecte su capacidad de procesamiento de datos?
- ¿Cuáles aplicaciones deben ser procesadas durante el tiempo que demora la contingencia?
- ¿Es imprescindible ante la presencia de un siniestro que todas las oficinas estén en línea?

ETAPAS PARA DESARROLLAR UN PLAN DE CONTIGENCIA

A. Análisis General del Riesgo
B. Definición de requerimientos para casos de contingencia
C. Identificación de alternativas estratégicas
D. Desarrollo del plan
E. Implantación del plan

A. ANALISIS GENERAL DEL RIESGO

- Determinar las aplicaciones computacionales relacionadas con funciones que son criticas para la organización.
- Identificar los ambientes operativos que se ven afectados en caso de siniestro.
- Identificar los puntos de la configuración donde las consecuencias que provoca su paralización son criticas para la organización.
- Identificar que partes de la configuración representan escenarios (**Ocurrencia de los posibles siniestros que afectan los diferentes recursos informáticos**) de importancia para casos de contingencia.

- Identificar debilidades de control general, que pueden comprometer la integridad o confidencialidad de la información.
- Identificar las aplicaciones criticas afectadas en cada uno de los escenarios de importancia.
- Definir los escenarios que se van a considerar en el desarrollo del plan en caso de siniestro.
- Identificar las debilidades de seguridad en la transmisión de datos, y en el acceso a los diferentes archivos.

METODOLOGIA A UTILIZAR EN EL ANALISIS DE RIESGO

- Entrevistas para determinar criticidades, los ambientes informáticos y la lista de siniestros a considerar, al igual conocer la administración del centro de computo, de las comunicaciones y de las bases de datos.
- Formularios para conocer ambiente informático.
- Inspección de Centros de Computo.

TIPOS DE SINIESTROS

A. SINIESTROS NATURALES
B. SINIESTROS OCASIONADOS POR EL HOMBRE

Estos siniestros se clasifican en:

- Siniestros catastróficos (Terremotos, Temblores, Huracanes, Anegación, Incendio, Sabotaje, Terrorismo, Sustracción de Hardware).
- Siniestros que afectan parcialmente los equipos, software, información y las comunicaciones (Falla en el suministro de energía, Sustracción de Software, Fallas Hardware, Fallas Equipos Comunicaciones, Fallas en Comunicaciones, Fallas en planta eléctrica, Fallas en UPS, Falla en reguladores, Falla aire acondicionado, Falla Tablero de Control, Fallas en el software operativo, aplicativo y de comunicación).
- Siniestros por retiro de personal o por alta dependencia de ellos (Conflicto laboral, retiro de personal clave, retiro masivo de personal).
- Siniestros por imposibilidad de acceso (Imposibilidad de Acceso).
- Siniestros por huelga en los servicios públicos (Energía Eléctrica, Comunicaciones).

CRITICIDAD DE APLICACIONES

CRITICIDAD "A": Todas aquellas aplicaciones que necesariamente deben ejecutarse. Esto significa que la interrupción no deberá ser mayor de un numero determinado de horas.

CRITICIDAD "B": Son aplicaciones que admitirían una interrupción de mediana magnitud y que so susceptibles de: Permanecer interrumpidas durante un periodo definido, Ser reemplazadas temporalmente por procedimientos manuales.

CRITICIDAD "C": Son aplicaciones que admiten una interrupción prolongada, no siendo indispensable la recuperación de la información comprendida en el tiempo generado por la interrupción.

FORMULARIO DE ENTREVISTAS PARA DETERMINAR CRITICIDAD DE APLICACIONES

NOMBRE DE FUNCIONARIO: _____

CARGO: _____

ANTIGÜEDAD EN LA EMPRESA: _____

ANTIGÜEDAD EN EL CARGO: _____

APLICACIONES DE QUE ES USUARIO:

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

DE LAS SIGUIENTES **APLICACIONES** CUALES CONSIDERA QUE PUEDEN SER LAS MAS CRITICAS PARA LA **ENTIDAD** (CLASIFIQUELAS EN A, B, C CON BASE EN EL NIVEL DE CRITICIDAD).

CRITICIDAD "A"	CRITICIDAD "B"	CRITICIDAD "C"
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

QUE CONSECUEWNCIAS TENDRIA PARA LA ORGANIZACIÓN NO PODER PROCESAR LA INFORMACION DE LAS APLICACIONES CONSIDERADAS CON CRITICIDAD "A"?

APLICACIÓN	CONSECUENCIA
_____	_____
	_____

FORMULARIO DE ENTREVISTAS PARA DETERMINAR CRITICIDAD DE APLICACIONES

APLICACIÓN	CONSECUENCIA

ES NECESARIO ANTE LA PRESENCIA DE UN SINIESTRO QUE TODAS LAS OFICINAS ESTEN OPERANDO EN LINEA?

OBSERVACIONES:

CUANTO TIEMPO PUEDE LA ORGANIZACIÓN OPERAR SIN LA INFORMACION QUE PROVEE LAS APLICACIONES QUE USTED HA CONSIDERADO COMO LAS MAS CRITICAS?

APLICACIÓN	TIEMPO	APLICACIÓN	TIEMPO

FORMULARIO DE ENTREVISTAS PARA DETERMINAR CRITICIDAD DE APLICACIONES

CONSECUENCIAS SEGÚN DURACION:

LISTA DE CHEQUEO PARA LA INSPECCION DE RIESGOS EN CENTROS DE COMPUTO

A. Distribución del Centro de Computo.

Se debe revisar:

- Amplitud del centro de computo
- Distancias entre equipos
- Zonas adecuadas de circulación
- Independencia y delimitación de zonas (CPU, controladores, impresoras, equipos de comunicación, unidades de cinta, consolas).
- Aislamiento total en las siguientes áreas: papelería, formas continuas, cintoteca, oficinas administrativas, laboratorios de reparación de equipos, desarrollo de sistemas, mesa de control, captura de datos.

B. Revisión de Materiales de Construcción y de los Equipos de Ofina.

- Material de las paredes: vidrios (de seguridad), enchapes (Material no Inflamable), Muros (revisar presencia de humedad y el estado general).
- Muebles (Material No Inflamable).
- Cortinas (Material No Inflamable).
- Piso Falso (Material No Inflamable y revisar el estado general).
- Techo Falso (Material No Inflamable y revisar el estado general).

C. Revisión de las Instalaciones y Cableado Eleéctrico.

- Tomas Eléctricas en buen estado.
- Distribución de cables en forma ordenada (potencia eléctrica, transmisión de datos, líneas telefónicas).
- Organización de los cables (aun por debajo del piso falso).

D. Tratamiento de los Equipos.

- Estado general de los equipos: daños externos, tapas de los equipos en su lugar, limpieza exterior en general.
- No deben permanecer elementos tales como: cintas, manuales, papelería y en general ningún elemento sobre los equipos de computo.
- No se debe permitir el consumo de alimentos dentro del centro de computo.
- Los equipos deben estar libres de cajas y papeles.
- El centro de computo debe estar siempre limpio y elementos que no cumplan ninguna función.

E. Cintoteca.

Se debe mantener una cintoteca en el centro de computo y otra fuera de las instalaciones de la empresa.

- Condiciones de humedad.
- Aislamiento del centro de computo.
- No existencia de material inflamable: madera, cajas de cartón, enchapes, etc.
- Amplitud – Circulación.

F. Papelería.

Se debe revisar:

- Condiciones de calor.
- Aislamiento total del centro de computo.
- No-existencia de material inflamable.

G. Instalaciones aledañas al Centro de Computo.

Se debe revisar:

- Baños cercanos al centro de computo.
- Nivel de altura del piso donde se encuentra ubicado el centro de computo.
- Que se encuentra debajo y que se encuentra encima del centro de computo.

H. Seguridad Física.

Se debe revisar:

- Acceso al centro de computo.
- Existencia de extintores automáticos contra incendios.
- Si hay extintores manuales, se debe revisar su fecha de vencimiento y el tipo de material que contienen.

I. Equipos de Soporte.

Se debe revisar:

- Cuarto de la UPS – ubicación e instalación.
- Cuarto de la planta eléctrica – ubicación e instalación.
- Cuarto de la subestación eléctrica - ubicación e instalación.
- Aire Acondicionado - ubicación e instalación.

MATRIZ DE DIAGNOSTICO Y RECOMENDACIONES

OBSERVACION	IMPACTO	RECOMENDACIÓN	RESPONSABLE

MATRIZ DE ESCENARIOS / IMPACTO

RECURSOS / SINIESTRO			

POTENCIALIDAD	
0	NULO
1	BAJO
2	MEDIO
3	ALTO
N/A	NO APLICA

- Crear un Comité Directivo de Contingencias
- Elegir un líder para el equipo de contingencia, el líder debe cumplir las siguientes funciones:

Fase 1: Reacción Inicial

- Determinar que tipo de siniestro se ha presentado
- Notificar al Director del Comité Directivo
- Dar a viso a seguridad.
- Notificar a los miembros del equipo de contingencias que considere necesarios, de acuerdo con el tipo de siniestro presentado.
- Notificar a los miembros del comité directivo sobre el estado de la emergencia.
- Dar aviso a los proveedores de los equipos afectados y reunirse con ellos.
- Mantener actualizados a los funcionarios sobre los procedimientos de emergencia.
- Determinar con los otros miembros y con el proveedor del equipo la magnitud del daño generado por el siniestro y determinar si se requiere poner en marcha el plan.

Fase 2: Plan para trasladarse al sitio de Soporte

- Efectuar una reunión inicial del equipo de contingencias para distribuir las tareas y responsabilidades asignadas en el plan.
- Coordinar con los centros alternos de proceso, de grabación y de operación, el traslado para la ejecución de las operaciones.
- Autorizar la obtención de cintas de backup en custodia externa.
- Revisar que se tenga acceso inmediato al manual de contingencias.
- Mantener informado al comité directivo.
- Nombras otros miembros del equipo cuando así lo exijan las circunstancias.
- Ordenar junto con los otros miembros del equipo el traslado a los centros alternos de proceso, de grabación y de operación.

Fase 3: Tareas en el sitio alterno de Soporte

- Verificar que se estén efectuando los procedimientos de recuperación.
- Coordinar el flujo de documentos e información entre oficinas, centros de grabación y de procesamiento alterno.
- Coordinar que se provean los recursos para la ejecución normal de labores en los diferentes centros de operación.
- Verificar que la operación de las aplicaciones criticas se realice en forma satisfactoria mediante pruebas iniciales y análisis de controles.
- Autorizar la operación de las aplicaciones críticas.

Fase 4: Regreso a la situación normal de operación

- Coordinar el regreso a una situación normal de operación.
- Coordinar la adecuada instalación del hardware, software aplicativo, operativo, utilitarios, etc.
- Coordinar la instalación de las comunicaciones.

SINIESTROS CON PROBABILIDAD DE OCURRENCIA EN LOS AMBIENTES INFORMATICOS DE SUBOCOL S.A.

Centro de Cómputo Principal (Santafé de Bogotá):

Daños en lineas telefónicas por lluvias,
Errores de Digitación,
Daños en Discos y Unidades de Cinta,
Falla en comunicaciones con Regionales (problema con el servidor),
Virus,
Daño en impresoras,
Incendio,
Sustracción de Hardware,
Fallas en el Fluido Eléctrico,
Falla Aire Acondicionado,
Falla UPS o Regulador

OBSERVACION	IMPACTO	RECOMENDACION
Las áreas del Centro de Cómputo no cuentan con un sistema de detección de humo.	En caso de presentarse un siniestro por Incendio no se detectaría oportunamente.	Instalar un sistema de detección de humo.
El material de las cortinas del Centro de Cómputo es de material inflamable	Hay alto riesgo de siniestro por incendio.	Cambiar el material de las cortinas por uno no inflamable.
No tienen procedimientos para revisión de los backup tomados.	Hay alto riesgo de pérdida de información de respaldo al no verificarse la correcta elaboración del backup.	Definir un procedimiento que permita verificar la correcta ejecución del backup.
Hay usuarios que consumen bebidas y la colocan cerca de los computadores a pesar que esta prohibido hacerlo.	Hay riesgo de daño de los equipos por dicho consumo.	Controlar el debido acato a las normas de no consumir alimentos en cerca de los micros.
Los vidrios de las ventanas del centro de computo no son de seguridad.	Ante un siniestro, los vidrios no ofrecen ninguna resistencia ante impactos fuertes.	Colocar vidrios de seguridad.
La caja de teléfonos se encuentra sin tapa y algunos cables están pelados.	Aumenta el riesgo de una interrupción en las comunicaciones	Colocar la tapa a la caja, y aislar los cables telefónicos.
No se tiene claramente definido y reglamentado, que software se puede instalar en los computadores.	Al no contar con normas claramente establecidas, se puede llegar a instalar software infectado que genere daños y perdida de información incalculables.	