PLAN DE CONTINGENCIA Y SEGURIDAD INFORMATICA INSTITUCIONAL

Versión 1.0
Fecha de Emisión: 17 de Julio del 2006
Fecha Ultima Modificación: 17 de Julio del 2006

INDICE

Ley de Murphy:

- Si un archivo puede borrarse, se borrará
- Si dos archivos pueden borrarse, se borrara el mas importante
- Si tenemos una copia de seguridad, no estará lo suficientemente actualizada.

1. PRELIMINAR

El plan de contingencia y seguridad informática implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de computo y la información contenida en los diversos medios de almacenamiento de la institución, por lo que en este manual se presentara un análisis de riesgos, como reducir su posibilidad de ocurrencia, políticas de seguridad a fin de asegurar los activos informativos de la información así como los procedimientos a seguir en caso que se presentara algún problema o contingencia.

Este plan es una herramienta que ayudará a que los procesos críticos de la entidad continúen funcionando a pesar de una posible falla en los sistemas computarizados así como preservar la información vital con la que cuenta la institución de intrusiones de cualquier tipo.

2. OBJETIVOS

OBJETIVO GENERAL
Salvaguardar la integridad de la información relevante de la institución adoptándose precauciones técnicas de seguridad, almacenamiento y recuperación lo que permita mantener la continuidad en las operaciones de la institución.

OBJETIVOS ESPECIFICOS

- Recuperar información de manera rápida y fiable.
- Brindar seguridad a los datos almacenados mediante mecanismos de respaldo eficientes.
- Facilitar el mantenimiento de los equipos de computo sin genera modificación, pérdida o eliminación de la información.
- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Preservar la información relevante de la institución de ataques internos o externos.

3. ANALISIS DE RIESGOS

Los siguientes sucesos constituyen los principales incidentes entre muchos que deben tomarse en consideración (de los más comunes a los más inesperados):

- Desperfecto de algún dispositivo de la computadora o componente de la red. (Falla de equipo)
- Infección del servidor y/o computadoras por acción de algún virus informático (acción de virus).
- Falla técnica (Corte del fluido eléctrico).
- Perdida de la información por inadecuado manejo del sistema operativo de red. (Equivocaciones)
- Apagado del servidor de la red en forma repentina ya sea en forma premeditada o en forma casual (Equivocaciones)
- Robo de la computadora o sustracción de sus componentes (Robo)
- Actos de fraude y/o robo de datos, desviando fondos usando las computadoras a través de los sistemas (Robo / Acceso no autorizado)
- Actos de vandalismo que dañen los equipos, archivos y/o centro de computo (Vandalismo)
- Generación de fuego por corto circuito, velas encendidas o uso de encendedores (Fuego).
- Acto terrorista que dañen las instalaciones de la entidad (Terrorismo)
- Fenómenos de la naturaleza como: lluvia intensa, inundación, terremoto, maremoto, etc. Que afecten a los recursos informáticos hasta el extremo de dejar inoperativa a la red (Fenómenos naturales)
- Otros que dejen inoperativo el funcionamiento de la red informática o sistemas de información utilizados por la entidad.

Factor de riesgo, probabilidad de ocurrencia del riesgo y estos pueden indicarse como: (bajo, muy bajo, alto, muy alto, medio)

TIPO DE RIESGO	FACTOR DE RIESGO
Fallas de equipos	Medio
Acción de virus	Medio
Corte de fluido eléctrico	Medio
Accesos no autorizados	Medio
Equivocaciones	Medio
Robo	Bajo
Vandalismo	Medio
Fuego	Bajo
Terrorismo	Bajo
Fenómenos Naturales	Bajo

4. DEFINICIONES

Acceso, es la recuperación o grabación de datos que han sido almacenados en un sistema de información.

Amenaza, Cualquier hecho que pueda interferir con el funcionamiento adecuado de una computadora personal o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: falla de suministro eléctrico, virus, sabotaje, etc.

Centro de Computo Principal, Ambiente físico en donde se ubican las computadoras principales (Hosts, Servidores, etc.) en los cuales se ejecutan los procesos con la información crítica del negocio.

Base de Datos, es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

Datos, son hechos y cifras que al ser procesados constituyen una información.

Incidente, es la acción de materializarse una amenaza.

Riesgo Informático. Posible acción que de ocurrir afectaría a los equipos o recursos informáticos en su normal funcionamiento, los cuales se catalogan en niveles de riesgo descritos anteriormente.

Software Base, aplicativos estándar utilizado por los usuarios de computadores para el desarrollo de sus actividades. Estos tipos de software son aplicativos de usuario final y como por ejemplo son: Sistemas Operativos, Procesadores de Textos, Hojas de Calculo, Generador de presentaciones, Administrador de base de datos y aplicativos que requiera la institución para realizar sus funciones.

5. RESPONSABILIDADES BASICAS Y PRELIMINARES DEL PLAN DE CONTINGENCIA

- Clasificación de la Información

  Crítica, información vital para la continuidad del funcionamiento de los procesos institucionales y debe ser recuperada inmediatamente.

  Necesaria, información importante que puede ser recuperada dentro de un determinado tiempo.

  Corriente, información que no afecta las operaciones normales de la institución.

- ALCANCE

  Los recursos informáticos protegidos son los siguientes:

INFORMACION	CLASIFICACION	UNIDAD ORGANICA DE LA INFORMACION	DETALLE
Base de Datos SQL Server	Citrica	VARIOS	Data de los Sistemas de Información.
Base de datos Sistemas XBase	Crítica	VARIOS	Data de los Sistemas de Información.
Aplicativos fuentes y ejecutables de los Sistema de Información	Crítica	INFORMATICA	Archivos fuente de los Sistemas de Información tanto Sistemas Xbase como Sistemas Visuales
Documentación de los sistemas de información	Necesaria	INFORMATICA	Manuales, informes, Directivas del sistema
Archivos de oficina en los directorios USUARIOS, GRUPOS, AREAS	Crítica	VARIOS	Archivos de tipo WORD, EXCEL, POWER POINT, etc. de los usuarios de la institución.
Servicio Correo Electrónico	Necesario / Critico	VARIOS	Los Correos Electrónicos de los usuarios de la institución
Servicio WEB	Necesario / Critico	VARIOS	Pagina WEB de la institución
Sistema SIAF (Aplicativo, Data)	Crítica	ECONOMIA	Transacciones del sistema SIAF del área de ECONOMIA
Sistema SIGA (Aplicativo, Data)	Crítica	LOGISTICA	Transacciones del sistema SIGA del área de LOGISTICA
Sistema ARFSIS (Aplicativo, Data)	Necesario	SEGUROS SIS	Transacciones del sistema SIS del área del SEGUROS SIS
Sistema SIP2000 (Aplicativo, Data)	Necesario	INFORMATICA PERINATAL	Transacciones del sistema Perinatal , normado por el Ministerio de Salud del área de INFORMATICA PERINATAL
Sistema SESE (Aplicativo, Data)	Necesario	SERIVICIO SOCIAL	Transacciones del sistema servicio social, normado por el Ministerio de Salud del área de SERVICIO SOCIAL
Sistema PDT – SUNAT (Aplicativo, Data)	Necesario	ECONOMIA	Transacciones PDT – Sunat de la unidad de ECONOMIA
Sistema SISMED (Aplicativo, Data)	Necesario	FARMACIA	Transacciones de la unidad de FARMACIA, sistema normado por el Ministerio de Salud
Sistemas Varios EPIDEMIOLOGIA: NOTI99 – EPI6 – VIGILA – VEA. VEIIH (Aplicativo, Data)	Necesario	EPIDEMIOLOGIA	Sistemas de Control epidemiológico de la unidad de EPIDEMIOLOGIA normados por el Ministerio de Salud
Sistema SISMAN (Aplicativo, Data)	Necesario	SERVICIOS GENERALES	Sistema de control de SERVICIOS GENERALES normado por el Ministerio de Salud
Sistema Personal /Asistencial (Aplicativo, Data)	Necesario	PERSONAL	Sistema de gestión del personal y asistencial de la unidad de PERSONAL

- RESPONSABLES Y RESPONSABILIDADES

1. Supervisor de Seguridad
   Administrar el Plan de Contingencia

2. Supervisor de Producción
   Ejecutar las tareas de los procesos de respaldo y restauración.

3. Supervisor de Soporte Técnico
   Ejecutar las tareas de soporte técnico.

- DATOS DE LOS RESPONSABLES

1. **PEDRO PABLO LINCHE GOICOCHEA**
   JEFE DE SISTEMAS
   RESPONSABLE DE LA SUPERVISION DE LA SEGURIDAD

DOMICILIO	:	CALLE LOS LIRIOS MZ "B" LOTE 7, PORTADA 1
DISTRITO	:	MANCHAY
TELEFONO	:	---------
CELULAR	:	99196876

2. **FABRICIO OMAR LOPEZ MEDINA**
   SUPERVISOR DE PRODUCCION

DOMICILI O	:	URB. ALBINO HERRERA MZ "N1" LOTE 2
DISTRITO	:	CALLAO
TELEFONO	:	5744535
CELULAR	:	90197664

3. **DANY PRADO GUTIERREZ**
   SUPERVISOR DE SOPORTE TECNICO

DOMICILIO	:	NRO. MZ.D INT. LT18 P.J. PAMPLONA ALTA
DISTRITO	:	SAN JUAN DE MIRAFLORES
TELEFONO	:	---------
CELULAR	:	99202830

6. MEDIDAS DE SEGURIDAD ADOPTADAS POR LA UNIDAD DE INFORMATICA

- Uso del software antivirus PANDA ENTERPRISECURE como estándar, instalado en un servidor virtual dedicado exclusivamente a la administración y configuración del software antivirus, (SBPANDA), instalación del software de detección en el total de servidores y estaciones de trabajo, configurado para la actualización automática de las firmas a través de Internet, con filtro para los archivos adjuntos de los correos electrónicos, aviso automático de detección de virus así como instalación remota a través del administrador centralizado.

- La contraseña de los usuarios para el acceso a sus pc's y los recursos compartidos se ha configurado con el fin de que sea cambiada forzosamente cada 90 días.

- Uso de grupos de usuarios para los accesos a los recursos compartidos de la red informática de la institución.

- Firewall y proxy corporativo configurado a través del software Microsoft Internet Security and Acceleration (ISA) Server para el uso de Internet, Correo Electrónico y FTP con el correspondiente control de puertos de acceso a los servidores (80,21 y 25).

- Proxy configurado para acceder a Internet por grupos de usuario y en horas determinadas.

- Aislamiento de la sala de servidores prohibiendo terminantemente del ingreso y permanencia de personal no autorizado por la jefatura de la oficina.

- Adquisición de dos cajas fuerte con el fin de brindar seguridad a las copias backup que se realizan en la institución, por lo que ciñéndose a las normas de seguridad vigentes se sitúan en las siguientes ubicaciones físicas :

  1. Una caja de seguridad en la sala de servidores.
  2. Una caja de seguridad en las instalaciones del ambiente de backup en el 2do piso de la cochera (local que se encuentra en las afueras del local central de la institución)

- Las estaciones de trabajo están configuradas para impedir que cierto software no sea instalado en la PC a fin de utilizar software estándar.

- Ingreso restringido a personal no autorizado a las Oficinas de Informática.

7. POLITICAS EN LA SEGURIDAD DE LA INFORMACION

JUSTIFICACION

Los activos de información y los equipos informáticos son recursos importantes y vitales de la institución. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales. La información perteneciente a la institución debe protegerse de acuerdo a su valor e importancia.

Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas áreas de la institución están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos.

A todo el personal de la institución se le debe proporcionar adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la institución. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la institución.

La finalidad de las políticas de seguridad es la de proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la institución (conectados o no en red), como la información guardada en ellos.

RESPONSABILIDADES

Los siguientes entes son responsables, en distintos grados, de la seguridad en la institución:

- La Jefatura de Estadística e Informática, es responsable de implantar y velar por el cumplimiento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la dirección de la institución.

  También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

- El Supervisor de Seguridad, es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

- El Administrador de Sistemas, es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto o de un ente como el CERT (Computer Emergency Response Team). El Administrador de Sistemas también es responsable de informar al Supervisor de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. El supervisor de seguridad asume las funciones del administrador de sistemas si este no existiera

- Los usuarios, son responsables de cumplir con todas las políticas de la institución relativas a la seguridad informática y en particular:

  - Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
  - No divulgar información confidencial de la institución a personas no autorizadas.
  - No permitir y no facilitar el uso de los sistemas informáticos de la institución a personas no autorizadas.
  - No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la institución.
  - Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
  - Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
  - Reportar inmediatamente a su jefe inmediato o al personal de informática cualquier evento que pueda comprometer la seguridad de la institución y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

POLITICAS DE SEGURIDAD PARA ESTACIONES DE TRABAJO

- Las estaciones de trabajo de la institución sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
- Los equipos de la institución no deben utilizarse para actividades tales como juegos, pasatiempos o actividades afines.
- Debe respetarse y no modificar la configuración del hardware y software establecido por la unidad de informática.
- No se permite fumar, comer o beber mientras se está usando un PC.
- Debe protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.
- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la institución de la institución se requiere una autorización escrita.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.
- Si una estación de trabajo tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.
- No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- Para prevenir la intrusión de hackers, no está permitido el uso de módems en estaciones de trabajo que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la red de la institución.
- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Los usuarios no deben copiar a un medio removible (diskette, cd, memorias portables, etc.), el software o los datos residentes en las computadoras de la institución, sin la aprobación previa de su jefatura.
- No pueden extraerse datos fuera de la sede de la institución sin la aprobación previa de la jefatura.
- Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la institución.
- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por la Unidad de Informática.
- Para prevenir demandas legales o la introducción de virus informáticos, se prohibe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware a menos que haya sido previamente aprobado por la Unidad de Informática.
- No deben usarse diskettes, cd's, memorias portables u otros medios de almacenamiento en cualquier computadora de la institución a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

POLITICAS DE SEGURIDAD PARA LAS COMUNICACIONES

Con el fin de mejorar la productividad la institución promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la institución y no propiedad de los usuarios de los servicios de comunicación.

- **USO DE LOS SISTEMAS DE COMUNICACIÓN**
  - Los sistemas de comunicación de la institución generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la institución.
  - Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
  - La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la institución y en tal sentido deben usarse las horas no laborables.

- **CONFIDENCIALIDAD Y PRIVACIDAD**
  - No debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrada. Para tal fin debe utilizarse Microsoft Outlook, Outlook Express u otros productos previamente aprobados por la Unidad de Informática.
  - Los empleados y jefes de la institución no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La institución se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación.
  - De manera consistente con prácticas generalmente aceptadas la institución procesa datos estadísticos sobre el uso de los sistemas de comunicación.

- **BORRADO DE MENSAJES**
  - Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

POLITICAS DE SEGURIDAD PARA ACCESO A LA RED INSTITUCIONAL

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la institución al estar conectada a redes de computadoras.

Es política de la institución prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria.

Todos los cambios en los servidores y equipos de red de la institución, incluyendo la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

- **CUENTAS DE LOS USUARIOS**
  - Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
  - La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.
  - No debe concederse una cuenta a personas que no sean empleados de la institución a menos que estén debidamente autorizados.
  - Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
  - No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Supervisor de Seguridad o el Jefe de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.
  - Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de servidores no deben entrar inicialmente como "ADMINISTRADOR", sino empleando su propio ID. En cualquier caso debe registrarse en la bitácora todos los cambios de ID.
  - Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 45 días.
  - Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Supervisor de Seguridad debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.
  - Cuando un empleado es despedido o renuncia a la institución debe desactivarse su cuenta antes de que deje el cargo.

- **CONTRASEÑAS Y CONTROL DE ACCESO**

  - El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

  - Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

  - Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

  - La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

  - Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

  - Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Supervisor de Seguridad. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

  - Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

  - Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso.

  - Acciones de esta naturaleza se consideran violatorias de las políticas de la institución, pudiendo ser causal de medida disciplinaria

  - Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

  - Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

  - Los servidores de red y los equipos de comunicación deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

8. PROCEDIMIENTOS DE RESTAURACION DE SERVICIOS ANTE UN PROBLEMA.

- PROCEDIMIENTO 1 :

PROCEDIMIENTO DE RESTAURACION DE SERVICIO A EQUIPOS DE COMUNICACIÓN

1. PROBLEMAS DE LÍNEA DEDICADA Y MODEM

ACCIONES:

- Resetear el MODEM (Apagar por 5 Minutos y Volverlo a Prender).
- Hacer Ping a la WAN de Telefónica : 200.48.227.109
- Si no responde llamar a Telefónica.
- Llamar a Telefónica del Perú - Atención de Averías.
  Central de Atención de Averías: **0-800-16600**
- Telefónica del Perú genera un código de avería, luego Telefónica del Perú devuelve la llamada o envía personal técnico a fin de solucionar la falla.

INFORMACION REQUERIDA

Información de la Línea Dedicada:

Circuito Digital	:	**CD49278**
Tipo de Conexión	:	**UNIRED LINEA DEDICADA**
Protocolo del Router	:	**CISCO 1721**
CIR	:	**512 Kbps**
Ancho de Banda	:	**512 Kbps**
Tipo de Enlace	:	**UNIRED**

2. DESFIGURACION DEL ROUTER

ACCIONES:

- Resetear el Router (Apagar por 5 Minutos y Volverlo a Prender).
-
- Hacer Ping a la LAN del Router : 200.60.102.34
- Hacer Ping a la WAN de Telefonica : 172.22.1.45
- Si no responde llamar a Telefónica.
- Llamar a Telefónica del Perú - Atención de Averías.
  Central de Atención de Averías: **0-800-16600**
- Telefónica del Perú genera un código de avería, luego Telefónica del Perú devuelve la llamada o envía personal técnico a fin de solucionar la falla.
- Utilizar ROUTER de emergencia configurado.

  (Esta acción trae como consecuencia la adquisición del router de emergencia si no se contara con el mismo, ver sugerencias)

- PROCEDIMIENTO 2 :

PROCEDIMIENTO DE RESTAURACION DE SERVICIOS DE LOS SERVIDORES

1. **CONSEGUIR LAS COPIAS DE RESGUARDO**

   La copia de resguardo a buscar debe ser la mas reciente, bajo este concepto debemos revisar la hoja de control de copias de respaldo y ubicar la copia mas apropiada.

   - Identificar el CD o Cinta que contiene la información a restaurar.
   - Trasladarse a la ubicación física que resguarda nuestro backup en caso que el CD o Cinta apropiado se encuentre allí.

2. **REEMPLAZAR LA INFORMACION DAÑADA**

   De acuerdo a la configuración del servidor que sufrió daños realizar la restauración de archivos y/o configuración de servicios de acuerdo al servidor que reporto la falla.

   (Véase configuración del Servidor SBDOMAIN en el anexo 02)
   (Véase configuración del Servidor SBDATA en el anexo 02)
   (Véase configuración del Servidor SBWEB en el anexo 03)
   (Véase configuración del Servidor SBCORREO en el anexo 04)
   (Véase configuración del Servidor SBISA en el anexo 05)
   (Véase configuración del Servidor SBDESARROLLO en el anexo 06)
   (Véase configuración del Servidor NOVELL NETWARE en el anexo 07)
   (Véase configuración del Servidor Virtual SBPANDA en el anexo 08)
   (Véase configuración del Servidor ESPEJO en el anexo 09)
   (Véase configuración de los Sistemas de Información en el anexo 10)

- PROCEDIMIENTO 3 :

PROCEDIMIENTO DE RESTAURACION DE ESTACION DE TRABAJO

Toda configuración de estaciones de trabajo va de acuerdo al estándar utilizado en la Institución. En consecuencia cuando ocurriera algún problema con alguna estación de trabajo se realizarán las siguientes acciones:

ACCIONES:

1. En caso el problema no es resuelto en el lapso de 20 minutos se procede a retirar la estación de trabajo a fin de ser revisada minuciosamente:
   - Si la criticidad de las operaciones del usuario lo requiere y se dispone de pc's de emergencia se procede a entregar una PC en forma temporal a fin de que pueda continuar con sus labores hasta que se le de solución al problema.
   - En el caso de detectarse problemas de hardware :
     - Si la pc no tuviera garantía vigente entonces se procede a la evaluación detallada por parte del personal de soporte técnico a fin de reemplazarse las piezas de hardware defectuosas.
     - Si la pc se encuentra con garantía vigente entonces se hará la llamada telefónica al proveedor reportando el hecho a fin de que pueda apersonarse en el menor lapso de tiempo para dar solucionar al problema.
2. Si el problema requiere una instalación total de software primero se procede a salvar toda la información útil del usuario (se debe revisar el directorio **Mis Documentos** y por estándar en este directorio se debe guardar alguna información útil del usuario que no es almacenada en las carpetas compartidas del servidor correspondiente) luego se procede a formatear el disco.
3. Para la instalación del software se utiliza una imagen del tipo de equipo, el cual contiene el software estándar de las estaciones de trabajo de la institución.
4. Se configura la estación de trabajo y se devuelve la misma al usuario.
5. Todo suceso debe ser registrado en el Sistema de Soporte Técnico.

9. ADMINISTRACION DE COPIAS DE RESPALDO

La información de la Institución se encuentra distribuida de la siguiente manera:

INFORMACION	SERVIDOR
Base de Datos SQL Server	SBDATA
Base de Datos Sistemas XBase	Servidor NOVELL
Fuentes y Documentación de los Sistemas de Información Visuales	SBDESARROLLO
Fuentes y Aplicativos de los Sistemas de Información XBase	Servidor NOVELL
Ejecutables de los Sistemas de Información Visual	SBWEB
Servidor de Archivos de oficina de los usuarios por grupos de trabajo	SBDOMAIN
Unidad de Archivos de oficina los usuarios por grupo de trabajo	Servidor NOVELL
WEB San Bartolomé	SBWEB
Base de Datos del Servidor de Correo	SBCORREO
Sistema SIAF	SBWEB
Sistema ARFSIS	Servidor NOVELL
Sistema SIS2000	Servidor NOVELL
Sistema SESE	Servidor NOVELL
Sistema PDT - SUNAT	PC ECONOMIA
Sistema SISMED	PC SEGUROS SIS
Sistema EPIDEMIOLOGIA : NOTI99 – EPI6 – VIGILA – VEA – VEIIH	PC EPIDEMIOLOGIA
Sistema SISMAN	PC SERVICIOS GENERALES
Sistema REMUNERACIONES Y ASISTENCIA	PC PERSONAL

ALMACENAMIENTO DE COPIAS

La información se almacena de acuerdo a la siguiente estructura:

- PROCESO DE RESPALDO 1 - (CINTA / CD) 1

  SERVIDOR NOVELL (SISTEMAS XBASE / Carpetas de Usuarios)

INFORMACION	SERVIDOR	UBICACIÓN LOGICA
Aplicativos XBase (CLIPPER)	NOVELL NETWARE	SYS2:\HOSPITAL
Base de Datos de los Aplicativos XBase (CLIPPER)	NOVELL NETWARE	SYS4:\SISTEMAS
Fuentes Sistemas XBase (CLIPPER)	NOVELL NETWARE	SYS6:\COMPUTO
Archivos de los usuarios por grupo de trabajo INCLUYE : *OFICINA DE INFORMATICA PERINATAL:* Sistema SIS2000 *OFICINA DE SERVICIO SOCIAL:* Sistema SESE	NOVELL NETWARE	SYS3:\OFICINAS

- PROCESO DE RESPALDO 2 - (CINTA / CD) 2

  SISTEMAS CENTRALIZADOS EN ESTACIONES DE TRABAJO

OFICINA/ INFORMACION	SERVIDOR/PC	UBICACIÓN LOGICA
OFICINA DE ECONOMIA: Sistema SIAF Sistema PDT	 PC WINDOWS 98 PC WINDOWS 98	 HARD DISK (C:\) HARD DISK (C:\)
OFICINA DE PERSONAL: Sistema Asistencial Sistema de Remuneraciones Sistema PDT-SUNAT	 PC WINDOWS 98 PC WINDOWS 98 PC WINDOWS XP	 HARD DISK (C:\) HARD DISK (C:\) HARD DISK (C:\)
OFICINA DE SEGUROS SIS: Sistema ARFSIS	 PC WINDOWS 98	 HARD DISK (C:\)
OFICINA DE FARMACIA : Sistema SISMED	PC WINDOWS 98	HARD DISK (C:\)
OFICINA DE EPIDEMIOLOGIA: Sistema NOTI99-EPI6-VEA-VEIIH	PC WINDOWS 98	HARD DISK (C:\)
OFIC.SERVICIOS GENERALES: *Sistema SISMAN*	PC WINDOWS 98	HARD DISK (C:\)

- PROCESO DE RESPALDO 3 - (CINTA / CD) 3

  SISTEMAS VISUALES

INFORMACION	SERVIDOR/PC	UBICACIÓN LOGICA
Base de Datos Sistemas Visuales : - Sistemas SIAH - Sistemas SIGA - Sistema Tramite Documentario - Portal WEB	 SBDATA SBDATA SBDATA SBDATA	 HARD DISK (D:\DATA SQL) HARD DISK (D:\DATA SQL) HARD DISK (D:\DATA SQL) HARD DISK (D:\DATA SQL)
Fuentes Sistemas Visuales: - Sistemas SIAH - Sistema Tramite Documentario - Portal WEB	 SBDESARROLLO SBDESARROLLO SBDESARROLLO	 HARD DISK (E:\PROYECTOS) HARD DISK (E:\PROYECTOS) HARD DISK (E:\PROYECTOS)
Aplicativos Sistemas Visuales: - Sistemas SIAF - Sistemas SIGA - Sistema Tramite Documentario - Portal WEB	 SBCORREO SBCORREO SBCORREO SBWEB	 HARD DISK (E:\APLICATIVOS) HARD DISK (E:\APLICATIVOS) HARD DISK (E:\APLICATIVOS) HARD DISK (C:\INITPUB)
Documentación y Archivos de trabajo Sistemas Visuales	SBDESARROLLO	HARD DISK (F:\DOCUMENTACION)
Base de Datos del Servidor de Correo	SBCORREO	HARD DISK (D:\)

REGISTRÓ DE COPIAS DE RESPALDO Y CONTROL DE ESTADO DE CINTA

1. Se trabaja con un formato estándar el cual cumple con la normativa vigente, a través he dicho formato es llevado a cabo el registro y clasificación de la información :

HOSPITAL NACIONAL DOCENTE MADRE NIÑO "SAN BARTOLOME"

HOJA DE REGISTRO DE PROCESO DE RESPALDO

Unidad de Informatica y Sistemas

FECHA _____ CODIGO _____

HORA DE INICIO _____ HORA DE TERMINO _____

RESPALDO REALIZADO A:

EQUIPO :	TIPO DE SISTEMA OPERATIVO	UBICACION UND. LOGICAS	NIVEL IMPORTANCIA

CONFIGURACION DEL EQUIPO QUE REALIZA RESPALDO:

TIPO DE PROCESADOR	:
TIPO DE SISTEMA OPERATIVO	:
CAPACIDAD DISCO DURO	:
UNIDAD DE GRABACION EN CINTA	:
UNIDAD DE GRABACION CD	:
CAPACIDAD DE MEMORIA	:
CAPACIDAD DE VIDEO	:
TIPO DE ACCESO	:

CONFIGURACION DEL MEDIO DE ALMACENAMIENTO:

TIPO DE MEDIO	:
CAPACIDAD	:
SOFTWARE Y/O PROGRAMA UTILIZADO	:
VERSION / DISTRIBUIDOR	:
TAMAÑO APROX. DE LA INFORMACION RESPALDADA	:
FRECUENCIA / FORMA	:

OBSERVACIONES:

* Se realiza de forma diaria y posterior a la depuración y desinfección de la información recibida en el Disco Duro instalado para tal fin.
* El respaldo de la información se realiza de forma MANUAL

Coordinador Area de Producción Informática

Se adjunta un modelo del formato utilizado para el proceso de respaldo identificado como proceso 1, se muestra la manera como se registra la información en el formato:

HOJA DE REGISTRO DE PROCESO DE RESPALDO

Unidad de Informatica y Sistemas

FECHA	15/02/2006	CODIGO	-
HORA DE INICIO	05:44pm	HORA DE TERMINO	07:36pm

RESPALDO REALIZADO A:

EQUIPO : SERVIDOR NOVELL	TIPO DE SISTEMA OPERATIVO	UBICACION UND. LOGICAS	NIVEL IMPORTANCIA
* APLICACIONES EN CLIPPER	NOVELL NETWARE 5.1	SYS2:\HOSPITAL	CRITICA
* ARCHIVOS DE OFICINA MS_OFFICE	NOVELL NETWARE 5.1	SYS3:\OFICINAS	NECESARIA CORRIENTE
* APLICACIONES EN CLIPPER	NOVELL NETWARE 5.1	SYS4:\SISTEMAS	CRITICA
* ARCHIVOS FUENTES .PRG CLIPPER	NOVELL NETWARE 5.1	SYS5:\COMPUTO	CRITICA

CONFIGURACION DEL EQUIPO QUE REALIZA RESPALDO

TIPO DE PROCESADOR	:	PENTIUM IV 1.7 GHZ
TIPO DE SISTEMA OPERATIVO	:	WINDOWS 95 SE
CAPACIDAD DISCO DURO	:	40 Y 80 GB.
UNIDAD DE GRABACION EN CINTA	:	TAPE DRIVE 12 / 24 GB
UNIDAD DE GRABACION CD	:	OMEGA CD RW HASTA 700M
CAPACIDAD DE MEMORIA	:	256 MB.
CAPACIDAD DE VIDEO	:	64 MB.
TIPO DE ACCESO	:	RED NOVELL / W2000 SVR

CONFIGURACION DEL MEDIO DE ALMACENAMIENTO:

TIPO DE MEDIO	:	TAPE 4mm DDS-125
CAPACIDAD	:	12 GB / 24 GB
SOFTWARE Y/O PROGRAMA UTILIZADO	:	BACKUP EXEC
VERSION / DISTRIBUIDOR	:	6.0 / SEAGATE
TAMAÑO APROX. DE LA INFORMACION RESPALDADA	:	12 GB.
FRECUENCIA / FORMA	:	DIARIA / RESPALDO TOTAL

OBSERVACIONES:

* Se realiza de forma diaria y posterior a la depuración y desinfección de la información ejecutada en el Disco Duro de 80 Gb, instalado para tal fin.
* Copia de la Información total de los volumenes señalados (Años : 2005-2006)
* El respaldo de la información se realiza de forma MANUAL.

Pedro Linche Goicochea
Coordinador Area de
Producción Informática

HORARIOS EN LOS QUE SE REALIZA LA COPIA

Al realizarse los Backups de forma manual, se debe tener en cuenta el tráfico de información por lo que la sugerencia es que se realice en horas de la tarde:

Cabe Resaltar el requerimiento de la adquisición de un software especializado para las labores automáticas de Backups (Ver Sugerencias y Recomendaciones)

HORARIO	TIPO DE BACKUP	PROCESO
DIARIO (A PARTIR DE LA 1pm)	INCREMENTAL	PROCESO DE RESPALDO 1
DIARIO (A PARTIR DE LA 1pm)	INCREMENTAL	PROCESO DE RESPALDO 2
DIARIO (A PARTIR DE LA 1pm)	INCREMENTAL	PROCESO DE RESPALDO 3
SEMANAL SABADOS (A PARTIR DE LAS 10am)	TOTAL	PROCESO DE RESPALDO 1
SEMANAL SABADOS (A PARTIR DE LAS 10am)	TOTAL	PROCESO DE RESPALDO 2
SEMANAL SABADOS (A PARTIR DE LAS 10am)	TOTAL	PROCESO DE RESPALDO 3

REGISTRÓ DE MANTENIMIENTO Y RECUPERACION DE COPIAS DE SEGURIDAD

Al realizarse los Backups de forma manual, se debe de realizar posteriormente un mantenimiento de recuperación de datos para salvaguardar la información institucional.

Por lo que la hoja de mantenimiento y recuperación de datos servirá para dejar constancia y tener una prueba fehaciente de la recuperación de la data almacenada.

Produccion de Informatica
y Telecomunicaciones

HOJA DE MANTENIMIENTO Y RECUPERACION DE DATOS

FECHA _____ COGIGO _____

HORA DE INICIO _____ HORA DE TERMINO _____

RECUPERACION DE DATOS REALIZADO A :

EQUIPO :	TIPO DE SISTEMA OPERATIVO	UBICACIÓN UND. LOGICA	NIVEL IMPORTANCIA

CONFIGURACION DEL EQUIPO QUE REALIZA LA RECUPERACION DE LA DATA :

TIPO DE PROCESADOR
TIPO DE SISTEMA OPERATIVO
CAPACIDAD DE DISCO DURO
UNIDAD DE GRABACION EN CINTA
UNIDAD DE GRABACION DE CD
CAPACIDAD DE MEMORIA
CAPACIDAD DE VIDEO
TIPO DE ACCESO
UNIDAD LOGICA PARA EL RESTORE DE LA DATA

SITUACION DE LA RECUPERACION DE LA DATA :

DATA RECUPERADA (OPERATIVO)	
DATA RECUPERADA INCOMPLETA	
DATA NO RECUPERADA	

OBSERVACIONES:
* Se realiza el mantenimiento y recuperacion de la data los dias lunes y jueves en el Disco Duro de la unidad logica del equipo servidor donde se realiza las copias de seguridad.
* El mantenimiento de recuperacion de la data se realiza de forma manual.

Coordinador Area de
Produccion Informatica

10. SUGERENCIAS Y RECOMENDACIONES

- Surge la necesidad imperiosa de contar con equipos básicos de prevención a fin de tener la suficiente capacidad de respuesta a los problemas que puedan surgir, bajo esta premisa se sugiere la adquisición de los siguientes equipos :

EQUIPOS	CANTIDAD	MOTIVO
Sistema automatizado de gestión de copias de seguridad (Data Storage DDS) (Hardware/Software)	1	Gestión automática de los backups a través de un sistema DDS inteligente (Digital Data Storage)
ROUTER backup de contingencia	1	Contingencia antes posibles fallas del ROUTER principal
PC's de contingencia	2	PC's que sirvan como respaldo a usuarios q realizan procesos críticos mientras su PC es reparada.
Discos SCSI de respaldo para los servidores	2	Discos de respaldo para ser utilizados en cualquier problema o contingencia que surga en los servidores
UPS para estaciones de trabajo criticas	10	A fin de ser instaladas en PC's que cumplen un trabajo considerado critico en la institución.

- Se recomienda la implementación de una PC Servidor Backup configurado para tales fines.
- Es necesario e importante realizar una evaluación de las partes y piezas de repuesto con las que cuenta el área de soporte técnico a fin de establecer si las adquisiciones programadas cubren la necesidad de la institución, de no ser este el caso se debería aplicar los correctivos necesarios a fin de poder prestar un servicio técnico rápido y fiable a las contingencias que puedan ocurrir.
- Es de necesidad también contar con estabilizadores de corriente para cada una de las maquinas de la institución. Las maquinas desprotegidas de las fluctuaciones eléctricas están mas propensas a fallas irreparables que resulten mas costosas y perjudiciales para la seguridad de las operaciones de la institución.

11. CONCLUSIONES

- El Presente plan de contingencias intenta prevenir catástrofes mayores que pudieran perjudicar el normal funcionamiento de las operaciones de la institución.
- Las políticas y normas de copias de seguridad apuntan a asegurar la integridad de la información a través de mecanismos de almacenamiento fiable y eficiente.
- La inversión en tecnologías orientadas a la prevención y la contingencia siempre será menor al costo de perdida de información producido por algún incidente no previsto.
- De forma anual se debe evaluar el plan de contingencia y seguridad con el fin de realizar actualizaciones y mejoras al mismo.
- Es necesaria la difusión de las medidas de seguridad a los usuarios de la red informática de la institución, asimismo se debe fomentar la cultura de la prevención de contingencias y de la importancia del buen uso de las estaciones de trabajo.
- Se debe procurar gestionar ante la dirección de la institución de los equipos mencionados en las recomendaciones del presente documento a fin de poder brindar un óptimo servicio y evitar siniestros no contemplados.

ALGUNOS COSTOS QUE IMPLICA NO CONSIDERAR LOS EQUIPOS Y ACCESORIOS SUGERIDOS:

- Mayor Cantidad de tiempo en horas/hombre pérdidas por el personal que utiliza los servicios e información de los servidores.
- Mayor tiempo de restauración de la información de equipos ante alguna falla.
- Personal de la Institución sin disponibilidad de acceso a los archivos de trabajo de la red.
- Personal de la Institución sin disponibilidad de acceso a los sistemas de información y datos XBase y SQL Server.
- Perdida de documentos de trabajo al momento de ocurrir un corte de fluido eléctrico.

ANEXO 01

CONFIGURACION DE SERVICIOS EN SERVER SBDC

Sistema Operativo instalado Windows Server 2003 R2 Enterprise Edition SP1

FUNCIÓN:
Primary Domain Controller(PDC)
Servidor de Archivos, Servidor de Impresoras y Reloj digital, Servidor WINS, Servidor DHCP y DNS.

CONFIGURACIÓN FÍSICA:

COMPONENTE	CARACTERISTICA
FACTOR DE FORMA	RACK-2U
PROCESADOR	2x Intel Xeon de 3.4Ghz
CARACTERISTICAS PRINCIPALES DEL PROCESADOR	Hyper-Threading Technology Bus 800 MHz EM64T
MEMORIA CACHE	2MB L2
MEMORIA RAM	3GB(instalados)Hasta 16 GB(maximo) – DDR II SDRAM - ECC 400 Mhz – PC2-3200
CONTROL DE ALMACENAMIENTO	PERC 4 RAIS 0, 1, 5, 10 con memoria de 256MB (ULTRA 320 SCSI)integrada
BAHIA DE DISCOS	6 x 1" Hot Swap SCSI
DISCO DURO	5 discos de 72GB RPM de 15 KRPM
ALMACENAMIENTO	Lector DVD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 700 Watts
CONTROLADOR GRAFICO	16 MB Integrada
CONEXIÓN DE REDES SLOTS	1 Fast Ethernet, 1 Gigabit Ethenet Cobre 03 Slot PCI-x de 64 bit/100 Mhz

IDENTIFICACIÓN:

Nombre de la computadora **SBDC**
Dominio **SBDOMAIN**

SERVICIOS:

- Computer Browser
- Active Directory
- Microsoft TCP/IP
- Service DHCP
- Service Wins
- File server
- Console Remote
- Agente Panda Antivirus
- Politica de Seguridad de Windows
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Intel PrO/1000 Mt Network Connection UTP

Dirección IP : 192.168.10.2
Mascara : 255.255.252.0

Adaptador 2 : Intel PrO/1000 Mt Network Connection UTP

Dirección IP : Deshabilitado
Mascara : Deshabilitado

CONFIGURACIÓN DEL WINS:

Dirección IP : 192.168.10.2

CONFIGURACIÓN DEL DHCP:

Automático.

CONFIGURACIÓN IP'S de IMPRESORAS:

Impresora de Economía Konica Minolta	Dirección IP Mascara	: :	192.168.10.20 255.255.252.0
Impresora de Economía Brother	Dirección IP Mascara	: :	192.168.10.24 255.255.252.0
Impresora de Logística Konica Minolta	Dirección IP Mascara	: :	192.168.10.21 255.255.252.0
Impresora de Logística Brother	Dirección IP Mascara	: :	192.168.10.25 255.255.252.0
Impresora de Planeamiento Estratégico	Dirección IP Mascara	: :	192.168.10.22 255.255.252.0
Impresora de Planeamiento Brother Estratégico	Dirección IP Mascara	: :	192.168.10.28 255.255.252.0
Impresora de Personal Konica Minolta	Dirección IP Mascara	: :	192.168.10.23 255.255.252.0
Impresora de Personal Brother	Dirección IP Mascara	: :	192.168.10.26 255.255.252.0
Impresora de Informática	Dirección IP Mascara	: :	192.168.11.50 255.255.252.0
Impresora de Epidemiologia Brother	Dirección IP Mascara	: :	192.168.10.27 255.255.252.0
Impresora de Estadística Brother	Dirección IP Mascara	: :	192.168.10.29 255.255.252.0
Impresora de Seguros Brother	Dirección IP Mascara	: :	192.168.10.30 255.255.252.0

CONFIGURACIÓN IP'S DE WIRELES BIBLIOTECA VIRTUAL:

Configuración IP — Dirección IP : 192.168.10.110
Mascara : 255.255.252.0

CONFIGURACIÓN IP'S DE RELOJ MARCADOR DIGITAL:

Reloj Digital 1 — Dirección IP : 192.168.11.11
Mascara : 255.255.252.0

Reloj Digital 2 — Dirección IP : 192.168.11.12
Mascara : 255.255.252.0

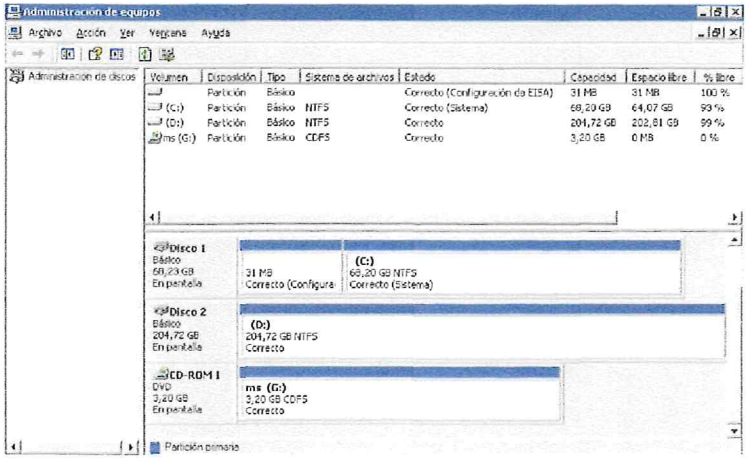
CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Física.

Estos discos se han divido en:

Disco 1 (Capacidad 68 GB) : (02 Discos) volumen C NTFS
RAID 1

Disco 2 (Capacidad 204 GB) : (04 Discos) volumen D NTFS
RAID 5



INFORMACIÓN ALMACENADA EN DISCOS:

Disco (1) Volumen C:

- Sistema Operativo Windows Server 2003
- Programas y Aplicaciones.
- Agente Panda Antivirus
- Directorios
- Grupos y Usuarios del Active Directory

- Papelera de Reciclaje

Disco (1) Volumen D:
- File Server
- Directorios de Grupos de Usuarios
- Directorios de Usuarios Personales

ANEXO 02

CONFIGURACION DE SERVICIOS EN SERVER SBWEB

Sistema Operativo instalado Windows Server 2003 R2 Enterprise Edition SP1

FUNCION:
Servidor Web, Servidor Windows Media, Servidor de Video Conferencias, Servidor Virtual.

CONFIGURACIÓN FÍSICA:

COMPONENTE	CARACTERISTICAS
FACTOR DE FORMA	RACK-2U
PROCESADOR	2x Intel Xeon de 3.4Ghz
CARACTERISTICAS PRINCIPALES DEL PROCESADOR	Hyper-Threading Technology Bus 800 MHz EM64T
MEMORIA CACHE	2MB L2
MEMORIA RAM	3GB(instalados)Hasta 16 GB(maximo) – DDR II SDRAM - ECC 400 Mhz – PC2-3200
CONTROL DE ALMACENAMIENTO	PERC 4 RAIS 0, 1, 5, 10 con memoria de 256MB (ULTRA 320 SCSI)integrada
BAHIA DE DISCOS	6 x 1" Hot Swap SCSI
DISCO DURO	5 discos de 72GB RPM de 15 KRPM
ALMACENAMIENTO	Lector DVD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 700 Watts
CONTROLADOR GRAFICO	16 MB Integrada
CONEXIÓN DE REDES SLOTS	1 Fast Ethernet, 1 Gigabit Ethenet Cobre 03 Slot PCI-x de 64 bit/100 Mhz

IDENTIFICACIÓN:

Nombre de la computadora **SBWEB**
Dominio **SBDOMAIN**

SERVICIOS:
- Computer Browser
- Microsoft TCP/IP
- File Server
- Servicios de Sistemas de Aplicaciones
- Servidor de Internet
- Servidor de Intranet
- Servicios de Video Conferencias Via Web
- Servicios de Windows Media
- Servicios Virtuales
  - Servidor Virtual Panda Antivirus
- Console Remote
- Agente Panada Antivirus
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Intel PrO/1000 Mt Network Connection UTP

Direccion IP	:	192.168.10.3
Mascara	:	255.255.252.0

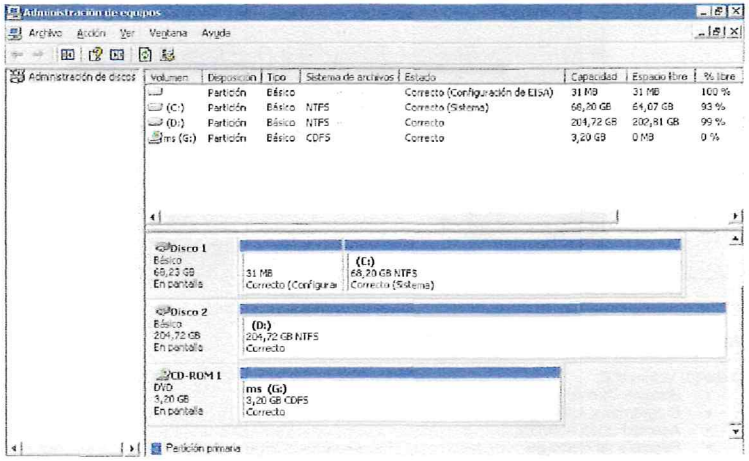
CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Física.

Estos discos se han divido en:

Disco 1 (Capacidad 68 GB) : (02 Discos) volumen C NTFS
RAID 1

Disco 2 (Capacidad 204 GB) : (04 Discos) volumen D NTFS
RAID 5



INFORMACIÓN ALMACENADA EN DISCOS:

Disco (1) Volumen C:

- Sistema Operativo Windows Server 2003
- Programas y Aplicaciones.
- Servicios de Windows Media
  - wmpub
- Servicios de Video Conferencia
  - wmpub
- Programa Agente Antivirus
- Directorios
- Papelera de Reciclaje

Disco (1) Volumen D:

- File Server
  - Directorio de Usuarios Personales
  - Directorio de Grupos de Usuarios
- Archivos de Aplicaciones
  - Sistema SIAH
  - Sistema SIGA
  - Sistema Tramite Documentario
- Servicios y Archivos de Publicación Portal Web Institucional
  - Inetpub
- Servicios y Archivos de Intranet Institucional
  - Inetpub
- Virtual Server
  - Sistema Operativo Windows Server 2003
  - Sistema Antivirus Panda Enterprise
  - Consola Panda Antivirus

ANEXO 03

CONFIGURACION DE SERVICIOS EN SERVER SBDATA

Sistema Operativo instalado Windows Server 2003 R2 Enterprise Edition SP1

FUNCIÓN:
Servidor de Base de Datos SQL.

CONFIGURACIÓN FÍSICA:

CARACTERISTICAS	OFERTADO
FACTOR DE FORMA	RACK-2U
PROCESADOR	2x Intel Xeon de 3.4Ghz
CARACTERISTICAS PRINCIPALES DEL PROCESADOR	Hyper-Threading Technology Bus 800 MHz EM64T
MEMORIA CACHE	2MB L2
MEMORIA RAM	3GB(instalados)Hasta 16 GB(maximo) – DDR II SDRAM - ECC 400 Mhz – PC2-3200
CONTROL DE ALMACENAMIENTO	PERC 4 RAIS 0, 1, 5, 10 con memoria de 256MB (ULTRA 320 SCSI)integrada
BAHIA DE DISCOS	6 x 1" Hot Swap SCSI
DISCO DURO	5 discos de 72GB RPM de 15 KRPM
ALMACENAMIENTO	Lector DVD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 700 Watts
CONTROLADOR GRAFICO	16 MB Integrada
CONEXIÓN DE REDES SLOTS	1 Fast Ethernet, 1 Gigabit Ethenet Cobre 03 Slot PCI-x de 64 bit/100 Mhz como Minimo Cumple

IDENTIFICACIÓN:

Nombre de la computadora **SBDATA**
Dominio **SBDOMAIN**

SERVICIOS:

- Computer Browser
- Microsoft TCP/IP
- Servidor de Base de Datos SQL
- Console Remote
- Agente Panda Antivirus
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Intel PrO/1000 Mt Network Connection UTP

Direccion IP : 192.168.10.4
Mascara : 255.255.252.0

Adaptador 2 : Intel PrO/1000 Mt Network Connection UTP

Direccion IP : Deshabilitado
Mascara : Deshabilitado

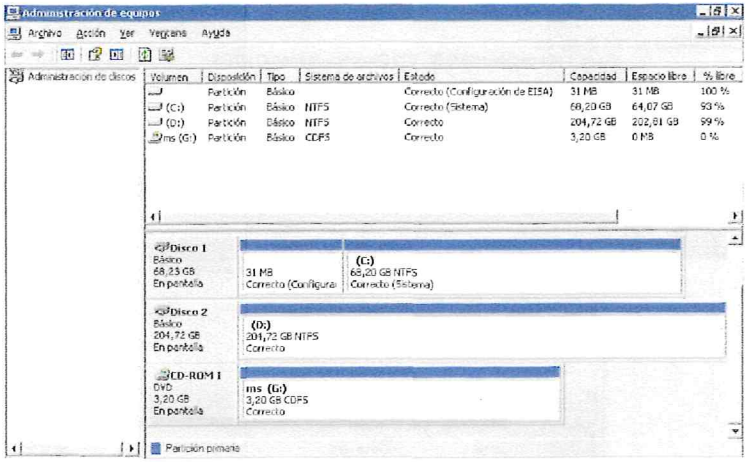
CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Fisica.

Estos discos se han divido en:

Disco 1 (Capacidad 68 GB) : (02 Discos) volumen C NTFS
RAID 1

Disco 2 (Capacidad 204 GB) : (04 Discos) volumen D NTFS
RAID 5



INFORMACIÓN ALMACENADA EN DISCOS:

Disco (1) Volumen C:

- Sistema Operativo Windows Server 2003
- Programas y Aplicaciones.
- Agente Panda Antivirus
- Papelera de Reciclaje

Disco (1) Volumen D:

- Servidor de Base de Datos SQL
- Archivos de Base de Datos
  - Base de Datos SIAH
  - Base de Datos SIGA
  - Base de Datos Tramite Documentario

ANEXO 04

CONFIGURACION DE SERVICIOS EN SERVER SBCORREO

Sistema Operativo instalado Windows Server 2003 R2 Enterprise Edition SP1

FUNCION:
Servidor de Microsoft Exchange Server, Servidor SIAF, Servidor ARFSIS.

CONFIGURACIÓN FÍSICA:

COMPONENTE	CARACTERISTICAS
FACTOR DE FORMA	RACK-2U
PROCESADOR	2x Intel Xeon de 3.4Ghz
CARACTERISTICAS PRINCIPALES DEL PROCESADOR	Hyper-Threading Technology Bus 800 MHz EM64T
MEMORIA CACHE	2MB L2
MEMORIA RAM	3GB(instalados)Hasta 16 GB(maximo) – DDR II SDRAM - ECC 400 Mhz – PC2-3200
CONTROL DE ALMACENAMIENTO	PERC 4 RAIS 0, 1, 5, 10 con memoria de 256MB (ULTRA 320 SCSI)integrada
BAHIA DE DISCOS	6 x 1" Hot Swap SCSI
DISCO DURO	5 discos de 72GB RPM de 15 KRPM
ALMACENAMIENTO	Lector DVD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 700 Watts
CONTROLADOR GRAFICO	16 MB Integrada
CONEXIÓN DE REDES SLOTS	1 Fast Ethernet, 1 Gigabit Ethenet Cobre 03 Slot PCI-x de 64 bit/100 Mhz como Mínimo Cumple

IDENTIFICACIÓN:

Nombre de la computadora **SBCORREO**
Dominio **SBDOMAIN**

SERVICIOS:

- Computer Browser
- Microsoft TCP/IP
- Servicios de Correo Electronico Institucional (SMTP)
- Servicios de Sistema SIAF
- Servicios de Sistema ARFSIS
- Servicios de Drivers y Soporte
- Console Remote
- Agente Panada Antivirus
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Intel PrO/1000 Mt Network Connection UTP

Direccion IP : 192.168.10.5
Mascara : 255.255.252.0

Adaptador 2 : Intel PrO/1000 Mt Network Connection UTP

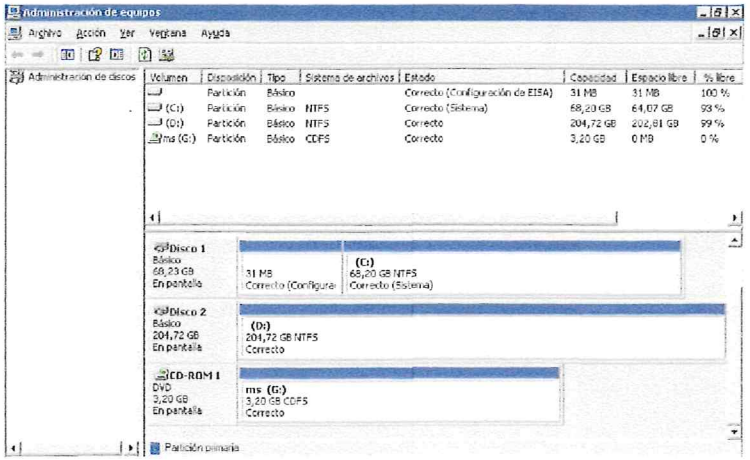
Direccion IP : Deshabilitado
Mascara : Deshabilitado

CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Física.

Estos discos se han divido en:
Disco 1 (Capacidad 68 GB) : (02 Discos) volumen C NTFS
RAID 1

Disco 2 (Capacidad 204 GB) : (04 Discos) volumen D NTFS
RAID 5



INFORMACIÓN ALMACENADA EN DISCOS:

Disco (1) Volumen C:

- Sistema Operativo Windows Server 2003
- Programas y Aplicaciones.
- Programa Agente Antivirus
- Papelera de Reciclaje

Disco (1) Volumen D:
- Sistema de Microsoft Exchange Server (SMTP)
- Buzones de Usuarios de Correos Electronico Institucional
- Base de Datos del Sistema SIAF
- Base de Datos del Sistema ARFSIS
- Drivers y Soporte Técnico

ANEXO 05

CONFIGURACION DE SERVICIOS EN SERVER SBISA

Sistema Operativo instalado Windows Server 2003 R2 Enterprise Edition SP1

FUNCION:
Servidor Firewall

CONFIGURACIÓN FÍSICA:

COMPONENTE	CARACTERISTICAS
FACTOR DE FORMA	RACK-2U
PROCESADOR	2x Intel Xeon de 3.4Ghz
CARACTERISTICAS PRINCIPALES DEL PROCESADOR	Hyper-Threading Technology Bus 800 MHz EM64T
MEMORIA CACHE	2MB L2
MEMORIA RAM	3GB(instalados)Hasta 16 GB(máximo) – DDR II SDRAM - ECC 400 Mhz – PC2-3200
CONTROL DE ALMACENAMIENTO	PERC 4 RAIS 0, 1, 5, 10 con memoria de 256MB (ULTRA 320 SCSI)integrada
BAHIA DE DISCOS	6 x 1" Hot Swap SCSI
DISCO DURO	1 discos de 72GB RPM de 15 KRPM
ALMACENAMIENTO	Lector DVD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 700 Watts
CONTROLADOR GRAFICO	16 MB Integrada
CONEXIÓN DE REDES SLOTS	1 Fast Ethernet, 1 Gigabit Ethenet Cobre 03 Slot PCI-x de 64 bit/100 Mhz como Mínimo Cumple

IDENTIFICACIÓN:

Nombre de la computadora **SBISA**
Dominio **SBDOMAIN**

SERVICIOS:

- Computer Browser
- Microsoft TCP/IP
- Servidor Isa (PROXI)
- Agente Panda Antivirus
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Intel PrO/1000 Mt Network Connection UTP

Direccion IP : 192.168.10.6
Mascara : 255.255.252.0

Adaptador 2 : Intel PrO/1000 Mt Network Connection UTP

IP WEB – INTERNET

Dirección IP Web	:	200.60.102.34
Mascara	:	255.255.255.240
Puerta de Enlace	:	200.60.102.33

DNS ISA:

DNS Primario	:	200.37.10.34
DNS Secundario	:	200.37.10.35

IP EXCHANGE:

Dirección IP Correo	:	200.60.102.35

Datos MX para el nombre del dominio sanbartolome.gob.pe

```
sanbartolome.gob.pe     mail exchanger = 10 mail.sanbartolome.gob.pe.
```

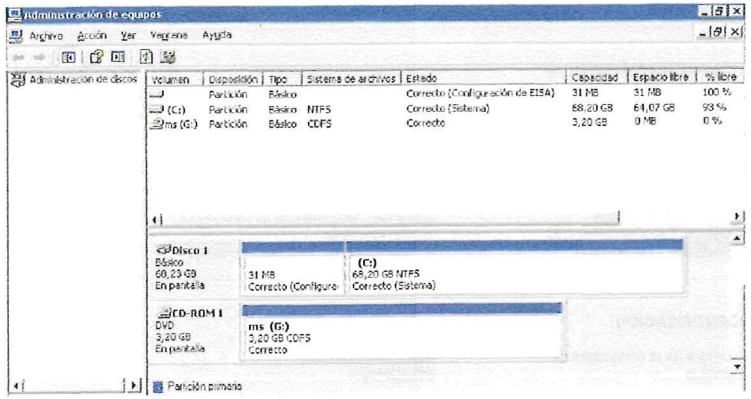
Datos NS para el nombre del dominio sanbartolome.gob.pe

```
sanbartolome.gob.pe     nameserver = DNS1.UNIRED.NET.pe.
sanbartolome.gob.pe     nameserver = DNS2.UNIRED.NET.pe.
DNS1.UNIRED.NET.pe      internet address = 200.37.10.34
DNS2.UNIRED.NET.pe      internet address = 200.37.10.35
```


CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Física.

Estos discos se han divido en:
Disco 1 (Capacidad 68.20 GB) : (01 Discos) volumen C NTFS
RAID 1



INFORMACIÓN ALMACENADA EN DISCOS:

Disco (1) Volumen C:

- Sistema Operativo Windows Server 2003
- Programas y Aplicaciones.
- Firewall Server (PROXI)
- Programa Agente Antivirus
- Papelera de Reciclaje

ANEXO 06

CONFIGURACION DE SERVICIOS EN SERVER SBDESARROLLO

Sistema Operativo instalado Windows Server 2003 R2 Enterprise Edition SP1

FUNCION:
Servidor de Desarrollo de Sistemas y Pruebas

CONFIGURACIÓN FÍSICA:

COMPONENTE	CARACTERISTICAS
PROCESADOR	Intel Pentium Xeon II de 448 Mhz
MEMORIA RAM	1.25 GB
DISCO DURO	4 discos de 8GB y 1 disco de 34 GB
ALMACENAMIENTO	Lector CD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 450 Watts
CONTROLADOR GRAFICO	8 MB Integrada
CONEXIÓN DE REDES	1 Fast Ethernet, 1 Gigabit Ethernet 03 Slot PCI

IDENTIFICACIÓN:

Nombre de la computadora **SBDESARROLLO**
Dominio **SBDOMAIN**

SERVICIOS:

- Computer Browser
- Microsoft TCP/IP
- Servidor de pruebas de Sistemas
- Servidor de pruebas de Base de Datos SQL
- Pruebas para la Publicación del Portal Web
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Tarjeta de Red Server Gigabit 3C996B UTP

Dirección IP : Automático
Mascara : Automático

Adaptador 2 : IBM Netfinity

Dirección IP : Deshabilitado
Mascara : Deshabilitado

Adaptador 3 : Nic TX PCI 10/100 3com

Dirección IP : Deshabilitado
Mascara : Deshabilitado

Adaptador 4 : Nic TX PCI 10/100 3com

Dirección IP : Deshabilitado
Mascara : Deshabilitado

CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Física.

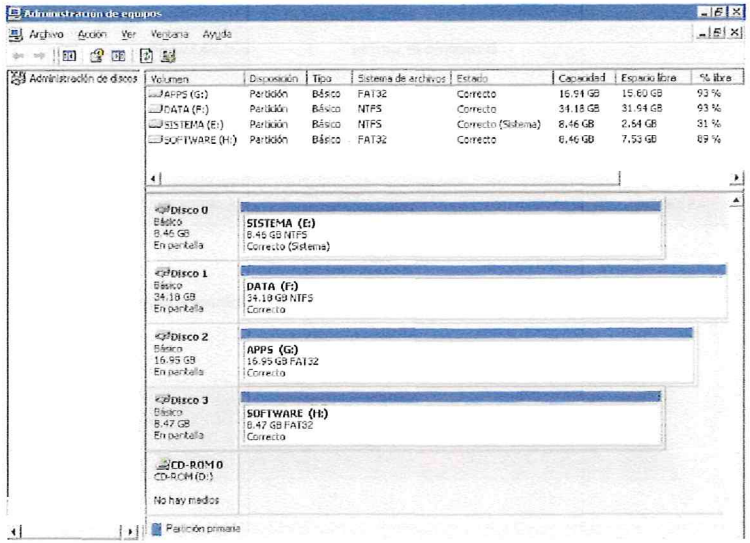
Estos discos se han divido en:

Disco 1 (Capacidad 8.46 GB) : (01 Discos) volumen E NTFS
RAID 1

Disco 2 (Capacidad 34.18 GB) : (01 Discos) volumen F NTFS
RAID 1

Disco 3 (Capacidad 16.95 GB) : (02 Discos) volumen G NTFS
RAID 1

Disco 4 (Capacidad 8.46 GB) : (01 Discos) volumen H NTFS
RAID 1



INFORMACIÓN ALMACENADA EN DISCOS:

Disco (1) Volumen E:

- Sistema Operativo Windows Server 2003
- Programas y Aplicaciones.
- SQL Server
- Programa Agente Antivirus
- Papelera de Reciclaje

Disco (1) Volumen F:
- Base de Datos de Sistemas.
- Documentación de Sistemas

Disco (1) Volumen G:
- Portal Web
- Fuentes de Sistemas

Disco (1) Volumen H:
- Backup de Sistemas

ANEXO 07

CONFIGURACION DE SERVICIOS EN SERVER NOVELL

Sistema Operativo Instalado Novell Netware 5.1

FUNCION:
Servidor Novell Netware 5.1

CONFIGURACIÓN FÍSICA:

COMPONENTE	CARACTERISTICAS
PROCESADOR	Pentium III 1.0 Ghz
CARACTERISTICAS PRINCIPALES DEL PROCESADOR	PENTIUM XEON
MEMORIA CACHE	1 MB
MEMORIA RAM	1260 GB
DISCO DURO	2 discos de 36. 0 Gb
ALMACENAMIENTO	Lector CD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 550 Watts
CONTROLADOR GRAFICO	16 MB Integrada
CONEXIÓN DE REDES SLOTS	1 Fast Ethernet, 1 Gigabit Ethernet 03 Slot PCI

IDENTIFICACIÓN:

Nombre de la computadora **NOVELL**
Dominio **SBDOMAIN**

SERVICIOS:

- Computer Browser
- Servicios IPX
- Administracion Consola Novell Netware
- Administracion de Usuarios Novell
- Administracion de Sistemas Asistenciales Xbase
- Administracion de Sistemas Administrativos Xbase
- Administracion de Directorios y Archivos
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Tarjeta de Red Server Gigabit 3C996B UTP

Dirección IP : Automático
Mascara : Automático

Adaptador 2 : Nic TX PCI 10/100 3com

Dirección IP : Deshabilitado
Mascara : Deshabilitado

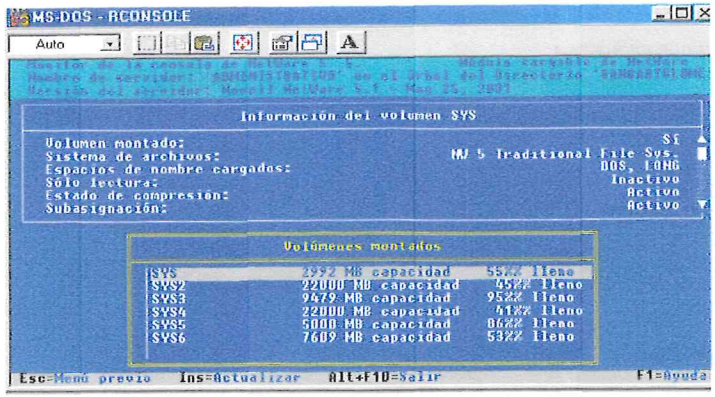
Adaptador 3 : Nic TX PCI 10/100 3com

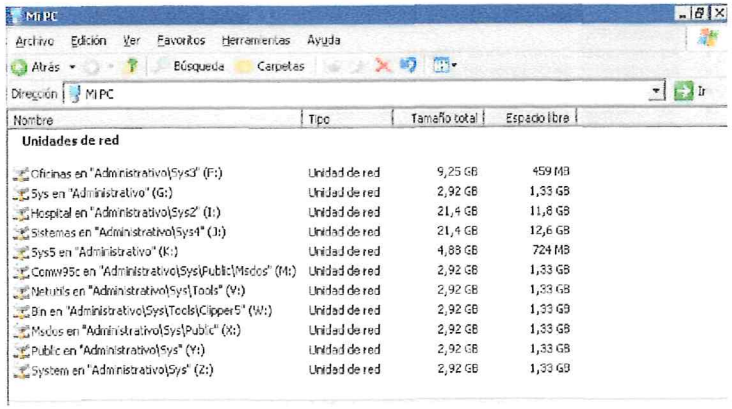
Dirección IP : Deshabilitado
Mascara : Deshabilitado

CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Física.

Estos discos se han divido en:
Disco 1 (Capacidad 72 GB) : (02 Discos) volumen C NTFS
RAID 1





INFORMACIÓN ALMACENADA EN DISCOS

Disco (1) Volumen F:
- File Server
  - Archivos de Usuarios Institucionales

Disco (1) Volumen G:
- Archivos del Sistema - Clipper

Disco (1) Volumen I:
- Archivos del Sistema Asistencial - Clipper
- Base de Datos de los Sistemas Asistenciales - Clipper

Disco (1) Volumen J:
- Archivos del Sistema Administrativo - Clipper
- Base de Datos de los Sistemas Administrativos - Clipper

Disco (1) Volumen K:
- Archivos de Drivers de Soporte Tecnico

Disco (1) Volumen M:
- Archivos de D.O.S.

Disco (1) Volumen V:
- Archivos de D.O.S. Novell 5.1

Disco (1) Volumen W:
- Archivos de D.O.S. Novell 5.1

Disco (1) Volumen X:
- Archivos de D.O.S. Novell 5.1

Disco (1) Volumen Y:
- Consola Administrativa de Novell 5.1
- Administración de Cliente Novell 5.1
- Administración de Usuarios Novell

Disco (1) Volumen Z:
- Sistema Operativo Novell 5.1
- Directorios
- Agente Panda Antivirus

ANEXO 08

CONFIGURACION DE SERVICIOS VIRTUAL EN SERVER SBPANDA

Sistema Operativo instalado Windows Server 2003 R2 Enterprise Edition SP1

FUNCION:
Servidor Virtual Panda Antivirus

CONFIGURACIÓN FÍSICA:

COMPONENTE	CARACTERISTICAS
FACTOR DE FORMA	RACK-2U
PROCESADOR	2x Intel Xeon de 3.4Ghz
CARACTERISTICAS PRINCIPALES DEL PROCESADOR	Hyper-Threading Technology Bus 800 MHz EM64T
MEMORIA CACHE	2MB L2
MEMORIA RAM	3GB(instalados)Hasta 16 GB(maximo) – DDR II SDRAM - ECC 400 Mhz – PC2-3200
CONTROL DE ALMACENAMIENTO	PERC 4 RAIS 0, 1, 5, 10 con memoria de 256MB (ULTRA 320 SCSI)integrada
BAHIA DE DISCOS	6 x 1" Hot Swap SCSI
DISCO DURO	5 discos de 72GB RPM de 15 KRPM
ALMACENAMIENTO	Lector DVD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 700 Watts
CONTROLADOR GRAFICO	16 MB Integrada
CONEXIÓN DE REDES SLOTS	1 Fast Ethernet, 1 Gigabit Ethenet Cobre 03 Slot PCI-x de 64 bit/100 Mhz como Mínimo Cumple

IDENTIFICACIÓN:

Nombre de la computadora **SBPANDA**
Dominio **SBDOMAIN**

SERVICIOS:

- Computer Browser
- Microsoft TCP/IP
- Servicios de Consola Administradora Panda Antivirus
- Servicios de Cliente Novell
- Console Remote
- Agente Panada Antivirus
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Intel PrO/1000 Mt Network Connection UTP

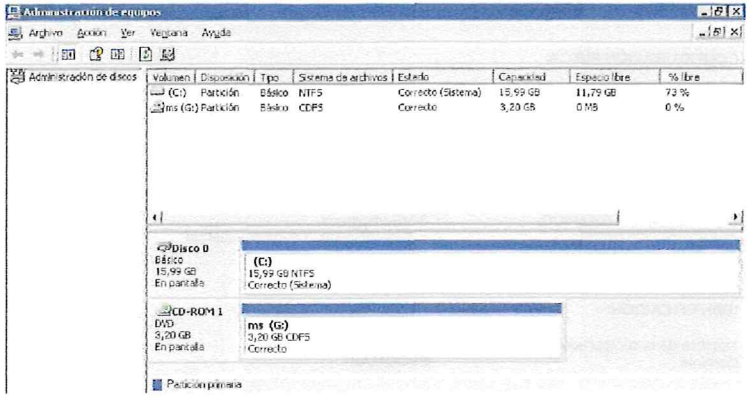
Direccion IP : 192.161.10.7
Mascara : 255.255.255.0

CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Física.

Estos discos se han divido en:

Disco 1 (Capacidad 15 GB) : (01 Discos) volumen C NTFS
RAID 5 (Configuración de la Unida D del Servidor Web).



INFORMACIÓN ALMACENADA EN DISCOS:

Disco (1) Volumen C:

- Sistema Operativo Windows Server 2003
- Programas y Aplicaciones.
- Consola Administradora Panda Antivirus
- Cliente Novell 5.1
- Agente Panda Antivirus
- Directorios
- Papelera de Reciclaje

ANEXO 09

CONFIGURACION DE SERVICIOS EN SERVER SBESPEJO

Sistema Operativo instalado Windows Server 2003 R2 Enterprise Edition SP1

FUNCION:
Servidor Espejo de Base de Datos SQL

CONFIGURACIÓN FÍSICA:

COMPONENTE	CARACTERISTICAS
PROCESADOR	Intel Pentium Xeon II de 448 Mhz
MEMORIA RAM	1.25 GB
DISCO DURO	2 discos de 32 GB
ALMACENAMIENTO	Lector CD interno
UNIDAD DE DISQUETTE	Lector de Disquette de 3.5" de 1.44MB
FUENTE DE PODER	2 fuentes redundantes de 450 Watts
CONTROLADOR GRAFICO	8 MB Integrada
CONEXIÓN DE REDES	1 Fast Ethernet, 1 Gigabit Ethernet 03 Slot PCI

IDENTIFICACIÓN:

Nombre de la computadora **SBBACKUP**
Dominio **SBDOMAIN**

SERVICIOS:

- Computer Browser
- Microsoft TCP/IP
- Servidor Espejo de la Base de Daros SQL Server
- Workstation

CONFIGURACIÓN TCP/IP DEL SERVIDOR:

Adaptador 1 : Tarjeta de Red Server Gigabit 3C996B UTP

Dirección IP : Automático
Mascara : Automático

Adaptador 2 : IBM Netfinity

Dirección IP : Deshabilitado
Mascara : Deshabilitado

Adaptador 3 : Nic TX PCI 10/100 3com

Dirección IP : Deshabilitado
Mascara : Deshabilitado

Adaptador 4 : Nic TX PCI 10/100 3com

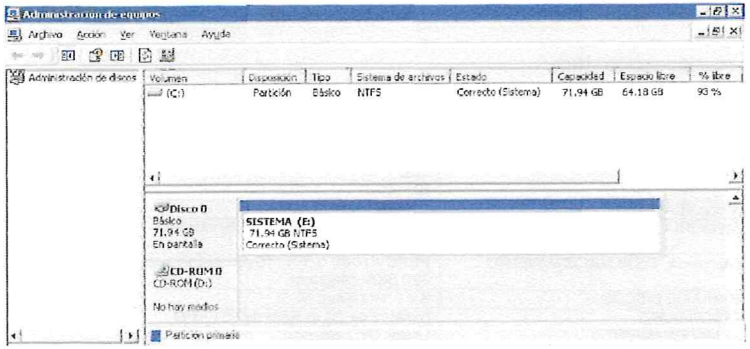
Dirección IP : Deshabilitado
Mascara : Deshabilitado

CONFIGURACIÓN DE DISCOS:

Este servidor cuenta con seis discos cuyas especificaciones técnicas son descritas en la parte inferior para su identificación Física.

Estos discos se han divido en:

Disco 1 (Capacidad 71.94 GB) : (02 Discos) volumen C NTFS
RAID 1



INFORMACIÓN ALMACENADA EN DISCOS:

Disco (1) Volumen C:

- Sistema Operativo Windows Server 2003
- Programas y Aplicaciones.
- Servidor SQL Server
- Base de Datos SQL
- Programa Agente Antivirus
- Papelera de Reciclaje

ANEXO 10

CONFIGURACION DE LOS SISTEMAS DE INFORMACION

1. **Configuración del Cliente SQL Server 2005**

   La versión del cliente de usuario de aplicaciones de SQL Server es la versión Client-2005.
   Los Instaladores del cliente se ubican:

   SERVIDOR: SBCORREO
   CARPETA COMPARTIDA: \\Soporte\SQL_Client_2005

2. **Configuración del Cliente SQL Server 2000**

   La versión del cliente de usuario de aplicaciones de SQL Server es la versión Client-2000.
   Los Instaladores del cliente se ubican:

   SERVIDOR: SBCORREO
   CARPETA COMPARTIDA: \\Soporte\SQL_Client_2000

3. **Ruta de los Archivos ejecutables de los Sistemas Visuales de Información**

   Los archivos ejecutables se encuentran en el servidor SBWEB\Ejecutables, dentro de este directorio se encuentran los subdirectorios por cada modulo.

4. **Ruta de los Archivos ejecutables de los Sistemas XBase de Información :**

   Los archivos ejecutables se encuentran en el servidor NOVELL NETWARE:
   Volúmenes: SYS2:\ , SYS4:\
   En estos volúmenes encontramos los archivos ejecutables por cada aplicación.