**1.- SITUACIÓN ACTUAL**

Como colaboradores de la empresa hemos podido notar varios motivos que refuerzan la necesidad de realizar un estudio acerca de las vulnerabilidades informáticas en la red, entre estos motivos tenemos:

* Comportamiento anómalo en ciertos equipos de la red reportado por los usuarios internos.
* Ausencia absoluta de documentación sobre políticas y procedimientos de seguridad que describan, principalmente, la forma adecuada de uso de los recursos, las responsabilidades y derechos tanto de usuarios como administradores, que indiquen lo que se va a proteger.

Las mediciones realizadas en este estudio se efectuaron con la colaboración del administrador de red y teniendo facilidad de acceso físico a las instalaciones de la empresa.

**1.1 INVENTARIO DE HARDWARE**

A continuación presentaremos un diagrama de los componentes físicos de la red de Sudamericana de Software S.A. (SASF) en el cual visualizaremos la distribución de los diferentes equipos informáticos y de comunicación.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Equipo** | **Sistema Operativo** | **Procesador** | **RAM** | **IP** | **Disco Duro** | **Función** |
| DESA1 | Windows 2000 Professional | x86 Family 6 Model 8 Stepping 3 GenuineIntel ~647 Mhz | 130.596 KB | 192.168.0.2 | 9 GB | Estación de trabajo |
| DESA10 | Windows 2000 Professional | x86 Family 6 Model 8 Stepping 0 AuthenticAMD ~1667 Mhz | 1.048.048 KB | 192.168.0.10 | 57 GB | Servidor de Aplicaciones Desarrollo y estación de trabajo |
| DESA11 | Windows 2000 Server | x86 Family 6 Model 8 Stepping 0 AuthenticAMD ~1670 Mhz | 1.015.156 KB | 192.168.0.11 | 80 GB | Servidor de Archivos y Base de Datos y estación de trabajo |
| DESA2 (PROXY) | Linux SuSE 8.0 | Intel Pentium III 733 Mhz | 94,196 KB | 192.168.0.3 | 18 GB | Servidor PROXY |
| DESA4 | Windows 2000 Professional | x86 Family 6 Model 8 Stepping 10 GenuineIntel ~1102 Mhz | 515.636 KB | 192.168.0.4 | 37,2 GB | Estación de trabajo |
| DESA7 | Windows 2000 Professional | x86 Family 6 Model 8 Stepping 0 AuthenticAMD ~1666 Mhz | 1.048.048 KB | 192.168.0.7 | 40 GB | Estación de trabajo |
| DESA8 | Windows 2000 Professional | x86 Family 6 Model 6 Stepping 2 AuthenticAMD ~1150 Mhz | 523.760 KB | 192.168.0.8 | 38,2 GB | Estación de trabajo |
| HUB |  | Encore Modelo ENH916-NWY de 16 Puertos |  |  |  |  |
| Impresora |  | Lexmark E210 |  |  |  |  |
| Impresora |  | Epson Stylus C62 |  |  |  |  |
| Modem |  | Motorola Cable MODEM SV4100 |  |  |  |  |

# Tabla #1 Inventario de los equipos existentes



##### **Fig. # 1 Diagrama de las instalaciones Sudamericana de Software**

**1.2 INVENTARIO DE SOFTWARE EXISTENTE**

A continuación se presenta un listado de los programas instalados en cada máquina de la red, como parte del estudio de la situación actual para contar con un inventario del software existente en la red corporativa.

|  |  |  |
| --- | --- | --- |
| **Software**  | **Versión** | **Proveedor** |
| Adobe Reader  | 6.0 | Adobe Systems , Inc. |
| DJ Java Decompiler  | 3.2.2.67 | Copyright (c) Atanas Neshkov 2002 |
| Herramientas de administración de Windows 2000 | 5.0.0.0000 | Microsoft Corporation |
| Internet Explorer | 5.00.3502.1000 | Microsoft Corporation |
| Java 2 Runtime Environment SE  | 1.4.0 | Sun Microsystems, Inc. |
| Java 2 SDK Enterprise Edition  | 1.3.1 | Sun Microsystems, Inc. |
| Java Web Start | 1.0.1 | Sun Microsystems, Inc. |
| Lexmark Software Uninstall | 2.01 | Lexmark International, Inc. |
| LiveReg Symantec Corporation | 2.4.1.2056 | Symantec Corporation |
| Live Update  | 1.90.15.0 | Symantec Corporation |
| Macromedia Flash MX | 6.0 | Macromedia, Inc. |
| Macromedia Fireworks MX | 6.0 | Macromedia, Inc. |
| Macromedia Dreamweaver MX | 6.0 | Macromedia, Inc. |
| Microsoft Office 2000 Premium | 9.0.2812 | Microsoft Corporation |
| Microsoft Project 98 | - | Microsoft Corporation |
| MSN Messenger | 6.1.0211 | Microsoft Corporation |
| NVIDIA nForce APU Utilities | 3.0.1 | NVIDIA, Inc. |
| NVIDIA Windows 2000/XP Display Drivers | 3.0.1 | NVIDIA, Inc. |
| Oracle Jiniitator | 1.3.1.9 | Oracle Corporation |
| Outlook Express | 5.50.4807.1700 | Microsoft Corporation |
| Outlook Tools | 2.3.5 | Microsoft Corporation |
| PL/SQL Developer | 5.0.1.480 | Allround Automations |
| Reproductor de Windows Media | 6.4.09.1128 | Microsoft Corporation |
| Software de Impresora EPSON | 5.525 | SEIKO EPSON Corporation |
| Sophos Anti-Virus | 3.70 | Sophos Plc |
| System Soap Pro  | 3.2.-AC1 | Stanmore Media, INC. |
| Visio 2000 | 6.0.0.1 | Visio Corporation |
| Winamp | 2.91 | Nullsoft, Inc. |
| Winrar Archiver | 3.20 | Eugene Roshal |
| Winzip  | 8.1 | WinZip Computing, Inc. |
| Microsoft Windows 2000 Server | 5.0.2195 | Microsoft Corporation |
| Oracle 9i Application Server Release 2 | 9.0.2.0.1 | Oracle Corporation  |
| Oracle Developer Suite | 9.0.2 | Oracle Corporation  |
| Oracle 9i Database Release 2 | 9.2.0.1.0 | Oracle Corporation  |
| Oracle Developer 6i | Patch 2 | Oracle Corporation  |
| Oracle 9i Client Release 2 | 9.2.0.1.0 | Oracle Corporation  |

# Tabla #2 Software instalado en Desa11

|  |  |  |
| --- | --- | --- |
| **Software** | **Versión** | **Proveedor** |
| Adobe Acrobat  | 5.0 | Adobe Systems, Inc. |
| Barra de Herramientas MSN | 2.21 | Microsoft Corporation |
| DashBar Toolbar | 1.56 | Microsoft Corporation |
| Java 2 Runtime Environment SE  | 1.4.0 | Sun Microsystems, Inc. |
| Java 2 SDK, SE  | 1.4.0 | Sun Microsystems, Inc. |
| Java Web Start | 1.0.1 | Sun Microsystems, Inc. |
| LiveReg (Symantec Corporation) | 2.2.0.1621 | Symantec Corporation |
| LiveUpdate (Symantec Corporation) | 1.80.19.0 | Symantec Corporation |
| Messenger Plus 3 | 3.52 | Microsoft Corporation |
| Microsoft Office 2000 Premium | 9.00.2720 | Microsoft Corporation |
| Microsoft Project 98 | - | Microsoft Corporation |
| Microsoft Visual Studio Service Pack 3 | 6.0.0.1 | Visio Corporation |
| Microsoft Windows 2000 Professional | - | Microsoft Corporation |
| MSN Messenger  | 6.2.0137 | Microsoft Corporation |
| Norton CleanSweep | - | Symantec Corporation |
| Norton Speed Disk for Windows NT | 7.0 | Symantec Corporation |
| Norton SystemWorks 2003 | 6.0.0 | Symantec Corporation |
| Norton Utilities 2003 for Windows | - | Symantec Corporation |
| OpenOffice.org  | 1.0.3 | Sun Microsystems, Inc. |
| PowerLite S1+ | 2.03 | PowerLite, Inc. |
| QuickTime | 6.0 | Apple Computer, Inc. |
| RealOne Player | 6.0.11.853 | RealNetworks, Inc. |
| Revisión del Reproductor de Windows Media  | - | Microsoft Corporation |
| Software de impresora EPSON | 5.525 | SEIKO EPSON Corporation |
| Software de Internet de MSN | - | Microsoft Corporation |
| VBA | 6.01.00.1234 | Microsoft Corporation |
| Visio 2000 | 6.0.0.1 | Visio Corporation |
| WebFldrs | 9.00.3501 | Microsoft Corporation |
| WebSecureAlert | 1.1.0.1 | GAIN Publishing, Inc. |
| Winamp3 (remove only) | 3.0.1 | Nullsoft, Inc. |
| Windows 2000 Service Pack 3 | - | Microsoft Corporation |
| Windows Media Player 9 | - | Microsoft Corporation |
| WinZip | 8.1 (4331) | WinZip Computing, Inc. |
| Oracle 9i Client Release 2 | 9.2.0.1.0 | Oracle Corporation  |
| Oracle Developer 6i | Patch 2 | Oracle Corporation  |

# Tabla #3 Software instalado en Desa1

|  |  |  |
| --- | --- | --- |
| **Software** | **Versión** | **Proveedor** |
| Add-ons | 1.0.0.0 | Visio Corporation |
| Adobe Acrobat  | 4.0,5.0 | Adobe Systems, Inc. |
| Adobe Acrobat Writer | 5.0 | Adobe Systems, Inc. |
| Adobe Illustrator  | 9.0 | Adobe Systems, Inc. |
| Adobe Photoshop  | 6.0 | Adobe Systems, Inc. |
| Adobe Photoshop  | 7.0 | Adobe Systems, Inc. |
| Analizador y SDK de Microsoft XML | 4.10.9406 | Microsoft Corporation |
| Arc Soft Photo Impression | 5.6.3 | Adobe Systems, Inc. |
| DEKSI Secure 2 | 2.2 | 666Soft |
| Internet Explorer  | 5.00.3502.1000 | Microsoft Corporation |
| Java 2 Runtime Environment SE  | 1.4.0 | Sun Microsystems, Inc. |
| Java 2 SDK Enterprise Edition | 1.3.1 | Sun Microsystems, Inc. |
| Java 2 SDK, SE  | 1.4.0 | Sun Microsystems, Inc. |
| Java Web Start | 1.0.1 | Sun Microsystems, Inc. |
| LimeWire | 4.25.0000 | Lime Wire LLC |
| LiveReg (Symantec Corporation) | 2.2.0.1621 | Symantec Corporation |
| LiveUpdate (Symantec Corporation) | 1.80.19.0 | Symantec Corporation |
| Macromedia Dreamweaver MX | 6.0 | Macromedia, Inc. |
| Macromedia Extension Manager | 1.5 | Macromedia, Inc. |
| Macromedia Fireworks MX | 6.0 | Macromedia, Inc. |
| Macromedia Flash MX | 6.0 | Macromedia, Inc. |
| Macromedia FreeHand 10 | 10 | Macromedia, Inc. |
| Marketing Plan Pro  | 6.01.0012 | Palo Alto Software |
| Microsoft Data Access Components KB870669 | - | Microsoft Corporation |
| Microsoft Internet Explorer 6 SP1 | - | Microsoft Corporation |
| Microsoft Office 2000 Premium | 9.00.2720 | Microsoft Corporation |
| Microsoft Project 2000 | 9.00.3821 | Microsoft Corporation |
| Microsoft Visio Professional 2002 [English] | 10.0.525 | Microsoft Corporation |
| Microsoft Windows 2000 Professional | - | Microsoft Corporation |
| MSN Messenger | 6.1.0211 | Microsoft Corporation |
| Norton CleanSweep | - | Symantec Corporation |
| Norton Speed Disk for Windows NT | 7.0 | Symantec Corporation |
| Norton SystemWorks 2003 | 6.0.0 | Symantec Corporation |
| Norton Utilities 2003 for Windows | - | Symantec Corporation |
| NTI CD-Maker 2000 Plus | 5.1.17 | NewTech Infosystems, Inc. |
| NTI FileCD | - | NewTech Infosystems, Inc. |
| Oracle 9i Application Server Release 2 | 9.0.2.0.1 | Oracle Corporation  |
| Oracle 9i Client Release 2 | 9.2.0.1.0 | Oracle Corporation  |
| Oracle 9i Database Release 2 | 9.2.0.1.0 | Oracle Corporation  |
| Oracle Developer 6i | Patch 2 | Oracle Corporation  |
| Oracle Developer Suite | 9.0.2 | Oracle Corporation  |
| Oracle JInitiator  | 1.3.1.9 | Oracle Corporation  |
| Outlook Express Q837009 | 5.50.4807.1700 | Microsoft Corporation |
| PL-SQL Developer | 5.0.1.480 | Allround Automations |
| PuTTY version  | 0.53b | Simon Tatham |
| QuickTime | 6.0 | Apple Computer, Inc. |
| Rational Rose Enterprise Edition | - | IBM Corporation |
| RealPlayer | 6.0.11.853 | RealNetworks, Inc. |
| Revisión del DirectX 9 - KB839643 | - | Microsoft Corporation |
| Revisión del Reproductor de Windows Media | - | Microsoft Corporation |
| SiS 900 PCI Fast Ethernet Adapter Driver | - | SiS, Inc |
| SiS Audio Driver | - | SiS, Inc |
| Software de impresora EPSON | 5.525 | SEIKO EPSON Corporation |
| VBA | 6.01..1234 | Microsoft Corporation |
| Warez P2P Client 2.4 | 2.4 | Warez Entertainment |
| WebFldrs | 9.00.3501 | Microsoft Corporation |
| Windows Media Player system update (9 Series) | 9.0 | Microsoft Corporation |
| WinRAR archiver | 3.20 | Eugene Roshal |
| WinZip | 8.1 SR-1 (5266) | WinZip Computing, Inc. |

# Tabla #4 Software instalado en Desa4

|  |  |  |
| --- | --- | --- |
| **Software** | **Versión** | **Proveedor** |
| Ace Password Sniffer  | 1.2 | EffeTech |
| Ad-aware 6 Personal | 6.0.1.181 Personal | Lavasoft |
| Adobe Reader  | 6.0 | Adobe Systems , Inc. |
| EtherDetect Packet Sniffer  | 1.2 | EtherDetect |
| GFI LANguard Network Security Scanner  | 3.1 | GFI Software Ltd. |
| LiveReg (Symantec Corporation) | 2.1.5.1502 | Symantec Corporation |
| LiveUpdate (Symantec Corporation) | 2.5.55.0 | Symantec Corporation |
| Macromedia Dreamweaver MX | 6.0 | Macromedia, Inc. |
| Macromedia Extension Manager | 1.5 | Macromedia, Inc. |
| Macromedia Fireworks MX | 6.0 | Macromedia, Inc. |
| Macromedia Flash MX | 6.0 | Macromedia, Inc. |
| Macromedia FreeHand 10 | 6.0 | Macromedia, Inc. |
| Microsoft Office 2000 Premium | 9.00.2720 | Microsoft Corporation |
| Microsoft Project 98 | - | Microsoft Corporation |
| Microsoft Visio Professional 2002 [English] | 10.0.525 | Microsoft Corporation |
| Microsoft Windows 2000 Professional | - | Microsoft Corporation |
| Network Inventory Expert | 2.3.1 | Kviptech |
| Network Inventory Monitor | 3.0 | Kviptech |
| Norton AntiVirus 2002 | 8.00.58 | Symantec Corporation |
| Oracle JInitiator  | 1.3.1.9 | Oracle Corporation |
| PL-SQL Developer | 5.0.1.480 | Allround Automations |
| Revision de Windows 2000 - KB835732 | 20,040,323,171,849 | Microsoft Corporation |
| Skip 1.0 | 1.0 | Skip Software S.A. |
| Spy Hunter | 1.1.30 | Enigma Software Group, Inc. |
| Symantec Network Drivers Update | 5.4.3.11 | Symantec Corporation |
| WebFldrs | 9.00.3501 | Microsoft Corporation |
| Winamp (remove only) | 3.0.1 | Nullsoft, Inc. |
| Windows Key Demo | - | Microsoft Corporation |
| Windows Media Player system update (9 Series) | - | Microsoft Corporation |
| WinPcap 3.1 beta3 | - | Politecnico di Torino |
| WinZip | 9.0 SR-1 (6224) | WinZip Computing, Inc. |
| Oracle Developer Suite | 9.0.2 | Oracle Corporation  |
| Oracle 9i Database Release 2 | 9.2.0.1.0 | Oracle Corporation  |
| Oracle 9i Client Release 2 | 9.2.0.1.0 | Oracle Corporation  |

# Tabla #5 Software instalado en Desa7

|  |  |  |
| --- | --- | --- |
| **Software** | **Versión** | **Proveedor** |
| WinZip | 8.1 SR-1 (5266) | WinZip Computing, Inc. |
| Windows Media Player system update (9 Series) | - | Microsoft Corporation |
| Winamp (remove only) | 3.0.1 | Nullsoft, Inc. |
| WebFldrs | 9.00.3501 | Microsoft Corporation |
| Visio Core Files | 06.00.0000 | Visio Corporation |
| Visio 2000 | 6.0.0.1 | Visio Corporation |
| VBA | 6.01.00.1234 | Microsoft Corporation |
| RealOne Player | 6.0.11.853 | RealNetworks, Inc. |
| PL-SQL Developer | 5.0.1.480 | Allround Automations |
| PLATINUM ERwin ERX  | 3.5.2 | Computer Associates International, Inc. |
| Oracle JInitiator  | 1.3.1.9 | Oracle Corporation |
| Norton AntiVirus 2002 | 8.00.58 | Symantec Corporation |
| Network Inventory Expert | 2.3.1 | Kviptech |
| Netscape  | 6.2 | Netscape |
| MSN Messenger  | 6.1.0211 | Microsoft Corporation |
| Microsoft Windows 2000 Professional | - | Microsoft Corporation |
| Microsoft Visual Studio Service Pack 3 | 6.0.0.1 | Visio Corporation |
| Microsoft Project 98 | - | Microsoft Corporation |
| Microsoft Office 2000 Premium | 9.00.2720 | Microsoft Corporation |
| Macromedia Flash MX | 6.0 | Macromedia, Inc. |
| Macromedia Fireworks MX | 6.0 | Macromedia, Inc. |
| Macromedia Dreamweaver MX | 6.0 | Macromedia, Inc. |
| LiveUpdate 2.0 (Symantec Corporation) | 2.0.39.0 | Symantec Corporation |
| LiveReg (Symantec Corporation) | 2.2.0.1621 | Symantec Corporation |
| Jschematic | 1.0 | Abcsemiconductors |
| Java 2 SDK, SE  | 1.4.0 | Sun Microsystems, Inc. |
| Java 2 Runtime Environment SE  | 1.4.0 | Sun Microsystems, Inc. |
| Graphics Filters | 1.0.0.0 | Visio Corporation |
| GFI LANguard System Integrity Monitor 3 | 3.0.0 | GFI Software Ltd. |
| DJ Java Decompiler  | 3.2.2.67 | Copyright (c) Atanas Neshkov 2002 |
| Distinct Network Monitor | 4.21 | Distinct Corporation |
| Apache Tomcat (remove only) | 4.0 | The Apache Software Foundation |
| Adobe Acrobat  | 5.0 | Adobe Systems, Inc. |
| Oracle 9i Application Server Release 2 | 9.0.2.0.1 | Oracle Corporation  |
| Oracle Developer Suite | 9.0.2 | Oracle Corporation  |
| Oracle 9i Database Release 2 | 9.2.0.1.0 | Oracle Corporation  |
| Oracle Developer 6i | Patch 2 | Oracle Corporation  |
| Oracle 9i Client Release 2 | 9.2.0.1.0 | Oracle Corporation  |

# Tabla #6 Software instalado en Desa8

|  |  |  |
| --- | --- | --- |
| **Software** | **Versión** | **Proveedor** |
| WinZip | 8.1 SR-1 (5266) | WinZip Computing, Inc. |
| WinPcap  | 3.1 beta3 | Politecnico di Torino |
| Windows Media Player system update (9 Series) | 9.0 | Microsoft Corporation  |
| Winamp 3 (remove only) | 3.0.1 | Nullsoft, Inc. |
| WebFldrs | 9.00.3501 | Microsoft Corporation |
| Visio Core Files | 06.00.0000 | Visio Corporation |
| Visio 2000 | 6.0.0.1 | Visio Corporation |
| VBA | 6.01.00.1234 | Microsoft Corporation |
| RealOne Player | 6.0.11.853 | RealNetworks, Inc. |
| Quest Software TOAD Xpert Edition  | 7.2 | Quest Software, Inc. |
| PL-SQL Developer | 5.0.1.480 | Allround Automations |
| PLATINUM ERwin ERX  | 3.5.2 | Computer Associates International, Inc. |
| Oracle JInitiator  | 1.3.1.9 | Oracle Corporation |
| Norton AntiVirus 2002 | 8.00.58 | Symantec Corporation |
| Network Inventory Expert | 2.3.1 | Kviptech |
| Netscape  | 6.2 | Netscape |
| MSN Messenger  | 6.1.0211 | Microsoft Corporation |
| Microsoft Windows 2000 Professional | - | Microsoft Corporation |
| Microsoft Visual Studio Service Pack 3 | 6.0.0.1 | Visio Corporation |
| Microsoft Project 98 | - | Microsoft Corporation |
| Microsoft Office 2000 Premium | 9.00.2720 | Microsoft Corporation |
| Macromedia Flash MX | 6.0 | Macromedia, Inc. |
| Macromedia Fireworks MX | 6.0 | Macromedia, Inc. |
| Macromedia Dreamweaver MX | 6.0 | Macromedia, Inc. |
| LOGINventory  | 4.01.14.3 | Schmidt´s LOGIN GmbH |
| LiveUpdate (Symantec Corporation) | 2.0.39.0 | Symantec Corporation |
| LiveReg (Symantec Corporation) | 2.2.0.1621 | Symantec Corporation |
| Jschematic | 1.0 | Abcsemiconductors |
| Java 2 SDK, SE  | 1.4.0 | Sun Microsystems, Inc. |
| Java 2 Runtime Environment SE  | 1.4.0 | Sun Microsystems, Inc. |
| Graphics Filters | 1.0.0.0 | Visio Corporation |
| GFI LANguard System Integrity Monitor 3 | 3.0.0 | GFI Software Ltd. |
| DJ Java Decompiler  | 3.2.2.67 | Copyright (c) Atanas Neshkov 2002 |
| Distinct Network Monitor | 4.21 | Distinct Corporation |
| Apache Tomcat (remove only) | 4.0 | The Apache Software Foundation |
| Adobe Acrobat  | 5.0 | Adobe Systems, Inc. |
| Oracle 9i Application Server Release 2 | 9.0.2.0.1 | Oracle Corporation  |
| Oracle Developer Suite | 9.0.2 | Oracle Corporation  |
| Oracle 9i Database Release 2 | 9.2.0.1.0 | Oracle Corporation  |
| Oracle Developer 6i | Patch 2 | Oracle Corporation  |
| Oracle 9i Client Release 2 | 9.2.0.1.0 | Oracle Corporation  |

# Tabla #7 Software instalado en Desa10

#### 1.3 ESQUEMA DE ANTIVIRUS

Como parte de los métodos de protección contra virus informáticos, está la utilización de software antivirus. A continuación se muestra una tabla donde se especifica el software antivirus utilizado en cada máquina.

|  |  |  |
| --- | --- | --- |
| **Equipo** | **Software Antivirus** | Función |
| DESA1 | Norton Antivirus Versión 9.05.15 |  Estación de trabajo |
| DESA10 | Norton Antivirus Versión 8.07.17.C |  Servidor de Aplicaciones  Desarrollo y estación de trabajo |
| DESA11 |  |  Servidor de Archivos y Base de  Datos y estación de trabajo |
| DESA2 | Linux SuSE 8.0 |  Estación de trabajo |
| DESA3 | No aplica |  Servidor PROXY |
| DESA4 | Norton Antivirus Versión 9.05.15  |  Estación de trabajo |
| DESA7 | Norton Antivirus Versión 8.07.17.C |  Estación de trabajo |
| DESA8 | McAfee Virus Scan Enterprise 7.1.0 |  Estación de trabajo |

# Tabla #8 Esquema de antivirus

Cabe mencionar que las actualizaciones de las definiciones de virus y en general del antivirus no se realiza periódicamente, es decir no hay un procedimiento establecido para la ejecución y actualización de los antivirus.

Además el servidor principal de la empresa se encuentra actualmente sin antivirus, lo que representa un grave peligro frente a cualquier programa no deseado que ingrese desde la misma red o de la Internet.

**1.4 ESQUEMA DE RESPALDOS.**

El procedimiento de respaldo que actualmente se ejecuta en SASF consiste en efectuar backups cada semana, los días viernes, almacenando en CD la información importante de la empresa que reside en el servidor central DESA11. Es necesario mencionar que pese a que los respaldos se efectúan de manera constante, no se tiene un procedimiento para pruebas de los backups que constaten que la información efectivamente puede ser recuperada.

Adicionalmente, los CD’s de respaldos tienen los datos almacenados sin ninguna seguridad (encriptación), de manera que es propensa a ser obtenida fácilmente en caso de robo. Por último, estos respaldos se almacenan en el domicilio del gerente de la empresa, donde hay probabilidad de que sean dañados o robados.

#### 1.5 ANÁLISIS DE RIESGOS

Un estudio muestra que si un desastre causa que las compañías pierdan sus centros de datos por 10 o más días, 50 por ciento de esas compañías se declararán en bancarrota casi inmediatamente después de la perdida. Otro 43 por ciento lo hará dentro de un año de la perdida

El análisis de riesgos realizado supone más que el hecho de haber calculado la posibilidad de que ocurran cosas negativas. Se pudo obtener una evaluación económica del impacto de estos sucesos negativos. Este valor se podrá utilizar para justificar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir).

Fig. #2 Gráfico estadístico de riesgos en las redes de cómputo (Fuente IBM)

Recordemos una de las leyes de mayor validez en la informática, la "Ley de Murphy" que cita lo siguiente:

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

 La única solución es tener copias de seguridad, actualizarlas con frecuencia y esperar que no deban usarse.

El análisis de riesgos supone responder a preguntas del tipo:

* ¿Qué puede ir mal?
* ¿Con qué frecuencia puede ocurrir?
* ¿Cuáles serían sus consecuencias?
* ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

a) ¿Qué se intenta proteger?

Se pueden clasificar los bienes a salvaguardar de la organización en dos categorías que son:

**Bienes físicos**

* CDs de instalación
* Manuales
* Archivador
* Equipos informáticos.
* Equipos y muebles de oficina
* Libros
* Útiles de oficina.

**Bienes lógicos**

* Código fuente de aplicaciones desarrolladas.
* Base de datos de las aplicaciones.
* Manuales de las aplicaciones (almacenados en medios magnéticos)
* Base de datos de clientes.
* Documentos electrónicos de la empresa.
* Base de datos de empleados.
* Base de datos de conocimientos.

b) ¿Cuál es su valor para la organización?

Frente a esta interrogante, se obtuvo esta información del área gerencial de la empresa, especificando lo siguiente:

* Valor de la información almacenada en el servidor central: $80.000,00
* Valor de los activos de la empresa: $12.000,00
* Valor aproximado de costo por día de inactividad: $2.250,00

c) ¿A qué riesgos en la seguridad informática se enfrenta la institución?

A continuación se muestra una lista de riesgos a los que esta expuesta la red de SASF.

* Al fuego, que puede destruir los equipos y archivos.
* Al robo común, llevándose los equipos y archivos. **
* Al vandalismo, que dañen los equipos y archivos. **
* A fallas en los equipos, que dañen los archivos. **
* A equivocaciones, que dañen los archivos.
* A la acción de virus, que dañen los equipos y archivos.
* A terremotos, que destruyen el equipo y los archivos.
* A accesos no autorizados, filtrándose datos no autorizados.
* Al robo de datos, difundiéndose los datos sin desearlo.
* A averías por fallas eléctricas.

d) ¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados?

Para contestar a esta interrogante se realizó un sondeo donde participaron los jefes de área y la gerencia de la empresa, contestando a las preguntas especificadas en el anexo A, referentes a cada riesgo potencial que amenaza a la red corporativa.

**1.5.1 CLASIFICACIÓN DE LOS FACTORES DE RIESGOS**

* Factor de riesgo muy bajo
* Factor de riesgo bajo
* Factor de riesgo medio
* Factor de riesgo alto
* Factor de riesgo muy alto

A continuación se muestra una tabla con el resumen de los riesgos ordenados por el factor de riesgo de cada uno, de acuerdo al sondeo realizado.

# Fig. #3 Porcentajes por riesgos

a: Fuego f: Virus

b: Robo g: Terremotos

c: Vandalismo h: Accesos no autorizados

d: Fallas de equipos i: Robo de datos

e: Fallas humanas j: Fraude

|  |  |
| --- | --- |
| **TIPO DE RIESGOS** | **FACTOR DE RIESGO** |
| Fuego  | Muy alto |
| Acción de virus | Alto |
| Vandalismo | Alto |
| Fallas en los equipos | Medio |
| Terremotos | Medio |
| Accesos no autorizados | Medio |
| Robo de datos | Medio |
| Robo físico | Medio |
| Fallas humanas | Muy bajo |
| Fraude | Muy bajo |

# Tabla #9 Calificación de riesgos

#### 1.5.2 PROTECCIONES ACTUALES

* Respaldos: se hace una copia semanal de los archivos que son vitales

para la institución.

* Robo común: se cierran las puertas de entrada y ventanas*.*
* Vandalismo: se cierra la puerta de entrada.
* Falla de los equipos: se operan con cuidado, además de mantener los

CDs de instalación con que vinieron al momento de comprarlos y se tiene un registro de los equipos que aun tienen garantía válida.

* Daño por virus: la mayoría de los equipos tiene instalado software

antivirus. Los programas de dominio público y de uso compartido (shareware), sólo se usan si proceden de una fuente fiable. Los usuarios normales no tienen privilegios para hacer instalaciones de nuevo software, para esto deben solicitar ayuda del administrador de la red.

* Equivocaciones: los colaboradores tienen buena formación en el

manejo de equipos informáticos.

* Terremoto: no existen protecciones actuales frente a este riesgo.
* Acceso no autorizado: se tiene un servidor proxy con firewall sobre

Linux para separar la red interna de la nube de Internet, aunque no están configuradas políticas que restrinjan el acceso*.*

* Robo de datos: se cierra la puerta principal. Los datos críticos solo

pueden ser accesados por usuarios autorizados.

* Fuego: en la actualidad no se toman precauciones frente a este riesgo.

**1.5.3 REVISIÓN DE SEGURIDADES**

De acuerdo a los resultados obtenidos en el análisis de riesgos, se hizo una revisión para constatar el estado actual de la seguridad en la red de SASF.

Esta revisión consistió en verificar los controles llevados en la empresa a nivel físico y lógico. También se verificó el esquema existente de conectividad a Internet.

**1.5.4 VERIFICACIÓN DE CONTROLES FÍSICOS**

Los controles de acceso físico son los más importantes dentro de una empresa, debido a que éstos tienen la finalidad de salvaguardar los activos de la empresa, además el considerar los controles de acceso a las instalaciones, por citar un ejemplo.

Como parte de la evaluación de los controles físicos de la red, se procedió a evaluar los siguientes puntos:

#### Nivel de protección de los equipos de cómputo y comunicaciones

Como parte de esta evaluación se procedió a verificar las conexiones de los cables del HUB, los cables del servidor de base de datos y del servidor proxy, quedó en evidencia el libre acceso físico que existe hacia el hardware de comunicaciones, puesto que el HUB esta almacenado en un armario donde también se guarda documentación física de la empresa , los cables de red y tomas de alimentación eléctrica no tienen protección, se encuentran en el paso, lo cual podría ocasionar que estos se desconecten de forma premeditada o no,.

Otra de las observaciones realizadas fue en cuanto a la seguridad de los servidores, puesto que son utilizados también como estaciones de trabajo, y debido a esto son propensos a interrumpir su funcionamiento por la impericia de quien lo este operando, por ejemplo, accidentalmente reiniciando el equipo.

#### Acceso físico a las instalaciones

Entre las falencias encontradas en el control de acceso físico a las instalaciones tenemos:

* Ausencia de un área de recepción donde se solicite una identificación a los empleados como a los visitantes que deseen ingresar al área de cómputo.
* Los colaboradores de la empresa carecen de una medio de identificación, llámese tarjeta de Id o alguna otro forma de identificación.
* La empresa no cuenta con personal para el resguardo del área física. Además no existe una bitácora donde todas las personas que entren a las instalaciones firmen un registro que indique la hora de entrada, el motivo por el que entran, la persona a la que visitan y la hora de salida.
* El ingreso se lo hace por medio de puertas con chapas de control manual para el acceso a las oficinas, sin que exista una persona específica para la labor de abrir y cerrar las mismas.

###### Control de incendios

Entre las debilidades encontradas en el control de incendios que se lleva en SASF tenemos:

* Ausencia de extintores de incendios.
* No se ha adquirido un seguro contra incendios.
* Las instalaciones no han sido revisadas por la persona del cuerpo de bomberos.
* No se realizan simulacros de incendio para capacitar al personal en caso de presentarse una emergencia.
* No hay instalados detectores de humo.
* No existen sistemas automáticos de rocío.
* Se conectan múltiples dispositivos a un mismo tomacorriente.

###### Control de fluido eléctrico

Entre las debilidades encontradas en el control del fluido eléctrico de SASF tenemos:

* La caja de los medidores de energía eléctrica se encuentra sin ningún tipo de protección, estando a la intemperie y a simple vista del público en general.
* No hay instalado un equipo de suministro de energía de emergencia (UPS) en caso de presentarse un corte abrupto del fluido eléctrico, pudiendo ocasionar severos daños a los equipos e información almacenada en estos.
* Existe una falta de equipos reguladores de voltaje, en caso de presentarse fluctuaciones considerables del fluido de electricidad que pueda averiar los equipos de cómputo.

**1.5.5 VERIFICACIÓN DE CONTROLES LÓGICOS**

Los controles de acceso lógico son el método primario de gestionar y proteger los activos de información para reducir a un nivel aceptable el riesgo de ataque en una organización. Para el estudio se hicieron revisiones de diferentes aspectos concernientes a la seguridad lógica de la empresa, entre estos tenemos:

###### Vulnerabilidades de sistemas operativos y puertos

Se realizó un análisis de las vulnerabilidades de los sistemas operativos de los diferentes equipos de cómputo que conforman la red de SASF, así como de los puertos y servicios que se ejecutan en los mismos. Este análisis de realizó con la ayuda de la herramienta GFI LANguard Network Security Scanner 5.0, que es un analizador de seguridades en redes LAN.

Luego de realizar este análisis, quedó en evidencia que los parches de seguridad en los equipos no se encuentran actualizados, y hay varios servicios y puertos que están funcionando innecesariamente. El resultado de estos análisis al detalle se puede encontrar en el anexo B.

**Seguridad frente a virus informáticos**

Los virus de ordenador son una amenaza para cualquier tipo de equipo de computación, mientras se realizaba al análisis de las seguridades se evidenció la presencia de virus informáticos en ciertos computadores, los virus encontrados fueron los siguientes:

W32.Sasser.B.Worm: Tipo: [Worm] - Programa que se replica copiándose entero (sin infectar otros ficheros) en la máquina infectada, y a través de redes de ordenadores. Este es un gusano que explota la vulnerabilidad en el servicio LSASS de la cual e habla más al detalle en el boletín de seguridad Microsoft Security Bulletin MS04-011.

Este gusano busca máquinas a las que infectar realizando chequeos de direcciones IP generadas semi-aleatoriamente, intentando conectarse al puerto TCP/445 de cada una de ellas (puerto donde se encuentra por defecto el servicio LSSAS vulnerable).

Este gusano fue detectado en dos de los equipos de la red, DESA10 y DESA7 presentando como síntoma el apagado no deseado de la máquina mostrando el siguiente mensaje:



Fig. #4 Mensaje de error del lsass.exe

Se sugirió que para corregir este problema se proceda a descargar el utilitario FxSasser para la eliminación de este gusano desde la página de Symantec. Además que se instale el parche de seguridad Windows2000-KB835732-x86-ESN que se puede descargar de la página de Microsoft.

Frente a este problema quedó en evidencia que estos equipos no tenían instalados los últimos parches de seguridad para prevenir el ataque de este gusano.

W32.HLLW.Habrack: Tipo: [Worm] - Programa que se replica copiándose entero (sin infectar otros ficheros) en la máquina infectada, y a través de redes de ordenadores.

W32.HLLW.Habrack es un gusano que se esparce a través de redes con archivos compartidos. El gusano además tiene funcionalidades de “puerta trasera” que permiten al creador controlar el sistema comprometido.

La máquina infectada con este virus fue DESA10, presentando el siguiente comportamiento anómalo:

* Despliega el siguiente mensaje:



**Fig. #5 Falso mensaje de download de parche**


**Fig. #6 Falso mensaje de petición de clave de Hotmail**



Fig. #7 Falso mensaje de petición de deshabilitación de antivirus

* Crea los siguientes archivos:

C:\Windows\WinSys.Dll

C:\Windows\Rundlls.exe

C:\Windows\Wscript.exe

C:\My Shared Folder\Linux Mandrake.Zip

C:\My Shared Folder\Microsoft® Visual Basic 7.exe

C:\My Shared Folder\Microsoft ® Windows Xp + Gen.exe

C:\My Shared Folder\Norton AntiVirus 2003 + Crack.exe

C:\My Shared Folder\Norton Ghost KeyGen.exe

C:\My Shared Folder\Msn 8 Cracked.exe

C:\My Shared Folder\Msn6Plus.exe

C:\Program Files\Panda AntiVirus Trial\Core files\Panda.exe

C:\Windows\\*.dll

C:\Winnt\\*.dll

C:\Windows\Desktop\\*.ink

* Crea la carpeta C:\Windows\System32\Norton\Defenitions\File\Break,

y dentro de la misma crea los siguientes archivos:

WinSys.Dll

WinSys.exe

Crea los siguientes archivos:

C:\Home.Vbs (142 bytes)

C:\Me.Html (52 bytes)

C:\hello.bat (51 bytes)

C:\Windows\Wscript.bat (80 bytes)

* Agrega 8,640 bytes al archivo:

C:\Program Files\Norton AntiVirus\Ccimscan.exe, cada vez que el virus se ejecuta.

* Agrega 4,320 bytes al archivo:

C:\Program Files\Norton AntiVirus\Qconsole.exe, cada vez que el virus se ejecuta.

* Borra los siguientes archivos:

C:\Program Files\Yahoo!\Messenger\res\_msgr.dll

C:\Program Files\MSN Messenger\msgslang.dll

* Trata de conectarse a la página web de Windows Update.
* Despliega el siguiente mensaje:, "Happy Birthday ...:::Hackers:::... "
* Trata de conectarse a Internet a través de un puerto de red aleatorio.

Se sugirió que para eliminar este virus se haga una actualización del antivirus y un rastreo total al computador.

**Seguridad de datos en la red local**

La seguridad de los datos conlleva a la identificación y autentificación de los usuarios con la finalidad de mantener los datos protegidos de intrusos.

La identificación es el proceso de probar la identidad de alguien y la autentificación el medio por el cual el usuario da una información (algo que solamente él conoce o tiene) que garantiza que realmente es quien dice ser pudiendo así acceder a la información que le corresponde. La técnica más conocida es la utilización de usuarios y contraseñas.

### Usuario y contraseña

En Sudamericana de Software existen definiciones de usuarios y roles, estos son los brindados por el sistema operativo del servidor de dominio, el mismo que esta utilizando Windows 2000 Server. Los roles existentes son los siguientes:

* Administrador del dominio: Control total de todas las maquinas, sus

aplicativos y acceso total a carpetas dentro de la red.

* Usuario Corporativos: Acceso a carpetas con información de la

Empresa. Rol principalmente utilizado por la parte Gerencial y Administrativa de la organización.

* Usuarios de Desarrollo: Solo se les permite el acceso a carpetas en

donde se encuentran los archivos fuentes de las aplicaciones.

Cabe mencionar que el periodo de validez de una contraseña en Sudamericana de Software actualmente esta fijada con de un lapso de 60 días, dentro del cual el usuario es forzado a cambiar la clave.

Actualmente no existen reglas que determinen el formato de las claves, lo cual no garantiza que estas no sean propensas a ataques de fuerza bruta.

Como parte de las verificaciones en este aspecto de la seguridad se revisó lo siguiente:

Instalaciones no autorizadas

Como se pudo observar en el inventario de software instalado, hay una diversa cantidad de programas en las estaciones de trabajo, muchos de estos que no tienen relación directa con la actividad de la empresa. Esto se debe a que los colaboradores suelen instalar software usando el usuario administrador de la máquina, el cual es el mismo en todas las estaciones. Esta situación suele acarrear problemas debido que ciertos programas cambian configuraciones en el sistema operativo o bloquean puertos, afectando el correcto desempeño de la estación de trabajo en las actividades para las que originalmente fue usada.

Ataques de fuerza bruta y diccionario

Desde los sistemas más simples hasta algunos increíblemente sofisticados, en su mayoría dependen de algo tan vulnerable como es el ingreso de un password o clave secreta.

¿Pero en que consisten los ataques de Fuerza Bruta? Estos consisten en generar e ir probando con todas las combinaciones de letras posibles hasta dar con el password.

Para dar un ejemplo de esto, se utilizó un utilitario llamado Brutus para realizar este tipo de ataque a la red de SASF, haciéndolo con las claves de los usuarios del proxy.



Fig. #8 GUI de Brutus

Por medio de esta herramienta se logró obtener en poco tiempo el password de varios usuarios registrados en el sistema operativo del servidor proxy. Este ataque fue fácilmente realizado debido a la poca complejidad de las claves utilizadas para los diferentes usuarios en la red.

Sniffers

EtherDetect: es una herramienta sniffing, se utilizó el EtherDetect Packet Sniffer Versión 1.2, instalándolo en DESA7, y haciendo accesos remotos al servidor Proxy vía telnet, obteniendo los siguientes resultados:

****

**Fig. #9 GUI del Etherdetect**

Como se puede observar, el password del usuario “awong” fue capturado por el sniffer, dejando en evidencia el peligro que conlleva el manejo poco seguro de esta información.

Accesos no permitidos como administrador de dominio

Este control puede ser considerado tanto a nivel de seguridad lógica como física.

Puede ser físico desde el punto de vista de que existe libre acceso a las instalaciones de SASF y una vez dentro de ellas encontrarnos con los servidores vulnerables y lógico, por no existir limitantes a nivel de software para acceder a los computadores.

Se realizó el acceso como usuario Administrador de dominio por parte de un usuario “x” no autorizado. Este acceso se lo hizo mediante la utilización del Offline NT Password & Registry Editor boot disk, que es una utilidad que consiste en un CD booteable que permite cambiar las claves de los usuarios locales de la máquina sin arrancar el sistema operativo. El procedimiento seguido fue el siguiente:

* Usando el Offline NT Password & Registry Editor disk reconfigurar la

clave de administrador de la máquina con "no password". Reiniciar,

presionar F8, y entrar a "Directory Service Recovery Mode". La

máquina iniciará como un servidor independiente sin soporte para

Active Directory.



# Fig. #10 Pantalla de configuración de Directory Service

* Cuando la página de acceso aparezca, presionar CTRL-ALT-DEL e

iniciar como "Administrador" sin password. Esta es la cuenta del

Administrador de la máquina, y no tiene la capacidad de modificar

cualquier cosa específica referente a la información del Active

Directory. Sin embargo puede cambiar y restaurar los archivos físicos

que contienen la base de datos de AD.

* Ejecutar "REGEDIT.EXE". Navegar a

*HKEY\_USERS\.Default\Control Panel\Desktop*

Cambiar los siguientes valores:

*SCRNSAVE.EXE* - change from *logon.scr* to *cmd.exe*

*ScreenSaveTimeout* - change from *900* to *15*

*ScreenSaveActive* - change to 1 (if it wasn't 1 already)

* Reiniciar normalmente. Cuando el cuadro de inicio aparezca no se

debe presionar nada y esperar.



# Fig. #11 Pantalla de login de Windows

* Después de 15 a 30 segundos se observará una ventana de DOS (ya

que es el screensaver). En la línea de comandos, escribir el siguiente comando: *MMC DSA.MSC.* Este es en realidad el nombre del ejecutable para los Usuarios y Equipos de Active Directory, que es la herramienta principal para administrar usuarios, grupos y equipos en el Active Directory de Windows 2000.

# Fig. #12 Línea de comando de activación Active Directory

Esto debe traer la consola de administración donde se puede editar claves de usuarios, incluyendo la clave del Administrador del dominio.

****

#

# Fig. #13 Pantalla consola de administración



# Fig. #14 Pantalla de configuración de nuevo password



# Fig. #15 Pantalla de confirmación de cambio de password

* Después de cambiar la clave del Administrador, salir de la consola de

administración y de la ventana de DOS, luego presionar CTRL-ALT-

DEL e ingresar como Administrador del dominio con el nuevo

password.

Para llevar a cabo este procedimiento es necesario tener acceso físico al equipo para insertar el CD de arranque. Por esto se demuestra que el no almacenar el servidor en un área restringida es un peligro inminente frente a cualquier individuo que realice un acceso no permitido con el usuario Administrador.

###### Controles de acceso a Internet

El Internet es hoy en día un recurso necesario para el desempeño de las organizaciones, y Sudamericana de Software no es la excepción, es por esto que incluimos como parte del estudio, un análisis de la arquitectura utilizada en SASF para conectarse al Internet.

A continuación se presenta un gráfico que muestra el esquema de conectividad a Internet:



# Fig. #16 Controles de acceso a Internet

Como se puede observar en el gráfico, el esquema de conectividad es muy simple, ya que no interviene un router sino que la conexión con el ISP es directa a través de cable MODEM y un servidor PROXY sobre Linux para distribuir el servicio en la LAN. Las características más al detalle de los equipos se dan a continuación:

Modem: Se utiliza un "cable modem" Motorola SurfBoard SB4100 que conecta directamente la línea de cable del proveedor ISP.

Proxy Server: Como Servidor Proxy se esta utilizando un equipo "Clon" con las siguientes características:

* 253M de Ram
* Procesador x86 Family 6 Model 8 Stepping 10 GenuineIntel ~1002

Mhz

* Disco Duro 28 G
* Sistema Operativo Linux SuSE 8.0
* SuSEFirewall habilitado.

Cabe anotar que pese a que el firewall que viene incluido en el SuSE está habilitado, no se encuentra configurado para hacer ningún tipo de bloqueo de tráfico en la red, ya que no existen políticas definidas frente a ese tema.

Controles administrativos de Procesamiento de Datos (PAD)

La máxima autoridad del área de Informática de una empresa debe implantar los siguientes controles que se agruparan de la siguiente forma:

* Controles de preinstalación
* Controles de organización y planificación
* Controles de sistemas en desarrollo y producción
* Controles de operación
* Controles de uso de microcomputadores

Los controles de preinstalación hacen referencia a procesos y actividades previas a la adquisición e instalación de un equipo de computación y obviamente a la automatización de los sistemas existentes.

Actualmente no existe un informe técnico en el que se justifique la adquisición de un equipo, software con su respectivo estudio costo-beneficio, el cual sirva para la toma de decisión con el fin de adquirirlo o no.

Los controles de organización y planificación se refieren a la definición clara de funciones, línea de autoridad y responsabilidad de las diferentes unidades del área PAD, en labores tales como:

* Acceso a la información
* Diseñar un sistema
* Elaborar los programas
* Operar el sistema
* Control de calidad

Las funciones y responsabilidades de los colaboradores en SASF no están definidos claramente, ya que no existe documentación que especifique a cada persona sus tareas y obligaciones en la empresa. Se debe evitar que una misma persona tenga el control de toda una operación.

Los controles de sistema en desarrollo y producción indican si los sistemas han sido la mejor opción para la empresa, bajo una relación costo-beneficio que proporcionen oportuna y efectiva información, además, que los sistemas se han desarrollado bajo un proceso planificado y se encuentren debidamente documentados. En Sudamericana de Software no existen personas que lleven un control de auditoria interna que sugieran y soliciten la implantación de rutinas de control.

Los controles de operación abarcan todo el ambiente de la operación del equipo central de computación y dispositivos de almacenamiento (DESA11), la administración y la operación de equipos de comunicación.

Los controles tienen como fin:

* Garantizar la integridad de los recursos informáticos.
* Asegurar la utilización adecuada de equipos acorde a planes y

objetivos.

No existe un registro permanente (bitácora) de todos los procesos de mantenimiento realizados en el equipo central de computación (DESA11) y pruebas de verificación de los equipos de comunicación.

Los controles en el uso del microcomputador son la tarea más difícil pues son equipos más vulnerables, de fácil acceso, de fácil explotación, pero los controles que se implanten ayudaran a garantizar la integridad y confidencialidad de la información.

No existen establecidos procedimientos de backups de la información, ni revisiones periódicas y sorpresivas del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa.

Además no existe un mantenimiento de programas y procedimientos de detección e inmunización de virus.